

# CYBER POLICY RECOMMENDATIONS FOR THE NEW ADMINISTRATION

STANFORD CYBER POLICY CENTER

Edited by Kelly Born

# CONTENTS

<b>Introduction</b> Kelly Born	<b>2</b>
<b>Reforming Section 230 And Platform Liability</b> Dr. Mary Anne Franks <i>Professor of Law and Dean's Distinguished Scholar, University of Miami School of Law, President and Legislative &amp; Tech Policy Director, Cyber Civil Rights Initiative</i>	<b>6</b>
<b>Middleware for Dominant Digital Platforms: A Technological Solution to a Threat to Democracy</b> Francis Fukuyama, Barak Richman, Ashish Goel, Roberta R. Katz, A. Douglas Melamed, Marietje Schaake	<b>24</b>
<b>Opening a Window into Tech: The Challenge And Opportunity for Data Transparency</b> Nathaniel Persily	<b>38</b>
<b>Democracy First: The Need for a Transatlantic Agenda to Govern Technology</b> Marietje Schaake	<b>55</b>
<b>How the Biden-Harris Administration Can (Begin To) Save The Internet</b> Gaurav Laroia, Matt Wood <i>Free Press</i>	<b>65</b>
<b>The Next Cyber Strategy: Playing a Better Game of Whack-A-Mole</b> Jacquelyn Schneider, PhD <i>Hoover Fellow, Stanford University</i>	<b>83</b>
<b>Top Technology Policy Priorities for the New Administration</b> Eileen Donahoe	<b>96</b>
<b>Conclusion</b> Kelly Born	<b>111</b>

# INTRODUCTION

**D**igital technologies have influenced all sectors of political and economic life in the 21st century. They have provided unprecedented benefits, but have also provoked massive power disruptions. These technologies are transforming governments, up-ending legal and political norms, reconfiguring economies and societies, and shifting geopolitical balances.

A new administration and Congress provide an opportunity to improve the governance of digital communication technologies. The problems posed by these technologies appear daunting: foreign-sponsored election interference, viral disinformation, online radicalization spilling into street violence, privacy violations, as well as the emergence of platform monopolies with unprecedented power over speech. Additionally, competition among governance regimes, specifically between the United States, Europe and China, has raised the stakes over whether democracies or authoritarian governments will set the rules for the internet. The policy choices made by the new administration will play a pivotal role in shaping our global future.

The following articles highlight technology policy priorities from a diverse array of leading experts. Some of the policy changes they recommend can be accomplished quickly; others may take years. Some must be implemented by government; others could be more quickly implemented by technology companies themselves. The explosion of research and expertise in these areas in recent years in academia, civil society, and the private sector can help guide the White House and Congress as they wrestle with the difficult trade-offs, and potential unintended consequences, inherent in governing the digital future.

This volume of essays is not intended as a comprehensive policy agenda for a new administration. Instead, it represents a compilation of priorities identified by a select group of experts. Some essays focus on one or two very specific recommendations, while other authors take a broader approach, identifying a larger set of priorities essential to the improvement of the digital technology ecosystem.

Despite this variation, several common themes emerge:

- The need to form an alliance between global democracies focused on technology governance in order to counter the rising threat posed by digital authoritarianism. Additional multilateral diplomatic efforts should ensure democratic principles guide the development of the new standards, protocols and norms governing digital technologies and cyberspace writ large.
- The need for the United States government to create dedicated leadership positions responsible for oversight of technology companies, including a potential “Commissioner on Cyber Abuse and Extremism”, an “Ambassador for Global Digital Affairs,” a “Czar” to coordinate agency action on privacy and algorithmic decision-making. Existing government agencies responsible for various aspects of technology oversight should be reorganized and new agencies may be needed to dramatically improve capacity and coordination amongst all relevant government bodies.
- The need for increased US investment in cybersecurity related R&D, and in ensuring universal broadband access, particularly for the most underserved populations.
- The need for greater algorithmic transparency from leading internet platforms, as a necessary precondition for both any meaningful oversight of platform activities, and sensible regulations moving forward.

Specifically, contributors suggest:

- Amending CDA 230 to deny immunity to platforms with respect to illegal and harmful content, that is disproportionately targeted at vulnerable communities, as Mary Anne Franks, professor of First Amendment Law at the University of Miami School of Law suggests.
- Laying the foundations for greater “content competition” by enabling a market for “middleware providers” that would hand editorial control to a diverse group of competitive actors, thereby enabling users to

tailor their own online experiences, as Frank Fukuyama, Co-Director of the Cyber Policy Center’s Program on Democracy and the Internet, and co-authors Barak Richman, Ashish Goel, Douglas Melamed, Roberta Katz, and Marietje Schaake, suggest.

- Drafting of a new Platform Transparency and Accountability Act that would enable scholarly research on the impact of technology companies by: providing immunity from civil and criminal liability when big tech platforms share data with vetted academics and immunizing qualified researchers who scrape publicly available data for research purposes, as Nate Persily, faculty Co-Director of the Cyber Policy Center suggests.
- Prioritizing the renewal of transatlantic cooperation in the governance of technology, to serve as the backbone for a global democratic alliance in tech governance, as Cyber Policy Center Director of International Policy Marietje Schaake argues in “Democracy first: the need for a transatlantic agenda to govern technology.”

Other contributors take a broader look, suggesting multiple priorities for reform, including:

- Gaurav Laroia and Matt Wood of media advocacy nonprofit Free Press, who argue that to fix the information ecosystem the Biden Administration must simultaneously work to fix the digital divide, address algorithmic discrimination, address conflicts between Section 230 and the First Amendment, and build non-commercial media to combat misinformation.
- Jackie Schneider of Stanford’s Hoover Institute, who looks at lessons from both the Obama and Trump administrations to recommend strategic priorities of an open, free, secure internet that safeguards genuine information by focusing on resilience first, bolstered by strategic deterrence, and complemented by ongoing investments in defense, intelligence, and information sharing while conducting counter-cyber operations.

- Finally, Eileen Donahoe of the Cyber Policy Center’s Global Digital Policy Incubator argues that the U.S. must rally the world around a democratic, human rights-based vision of digital society, and she recommends a range of early concrete actions that can be taken by the new administration to combat the competing digital authoritarianism model.

Finally, because these chapters reflect the priorities of only this select group of authors, a range of critical topics remain unaddressed. The concluding section on Additional Priorities, therefore, highlights other areas requiring urgent attention from federal policymakers. Some priorities are thoughtfully covered in other, related publications, including the Aspen Cybersecurity Group’s [A National Cybersecurity Agenda for Resilient Digital Infrastructure](#), the German Marshall Fund’s [#Tech2021 - Ideas for Digital Democracy](#), and the [Cyberspace Solarium Commission’s](#) 2020 Report.

In the coming months, the thought leaders included here, alongside many other experts from across the field, look forward to working with the next administration and Congress to address the impact that emerging technologies are having on global democracy, national security, society, markets and economies, and racial and economic inequality — alongside other impacts we have yet to imagine. The Cyber Policy Center welcomes feedback and collaboration towards informing the new administration, and to ensure facts and research guide technology policies.

# REFORMING SECTION 230 AND PLATFORM LIABILITY

STANFORD CYBER POLICY CENTER

Dr. Mary Anne Franks

*Professor of Law and Dean's Distinguished Scholar, University of Miami School of Law  
President and Legislative & Tech Policy Director, Cyber Civil Rights Initiative*

# REFORMING SECTION 230 AND PLATFORM LIABILITY

*Insulating the tech industry from liability for online extremism, abuse, and misinformation has threatened free expression, worsened existing inequalities of gender, race, and class, and gravely undermined democracy. The tech industry can no longer be exempted from the principle of collective responsibility for harm.*

---

## THE PROBLEM

On Jan. 8, 2021, two days after a violent mob attacked the United States Capitol in an attempt to prevent Congress’s certification of the 2020 presidential election, the social media platform Twitter permanently [banned](#) President Donald Trump’s personal account. Twitter had temporarily locked the @realDonaldTrump account on Jan. 6 after Trump posted a video and a statement repeating false claims about the election and expressing his “[love](#)” for the rioters, requiring Trump to delete the tweets before being able to post again. At the time of the [lockout](#), the Twitter Safety team noted that if Trump violated Twitter’s policies again his account would be banned. In a [blog post](#) on Jan. 8, the company explained that it had determined that two of Trump’s tweets following the riots, one referencing “American Patriots” and another stating that Trump would not be attending President-Elect Joseph R. Biden’s inauguration, were “likely to inspire others to replicate the violent acts that took place on Jan. 6, 2021, and that there are multiple indicators that they are being received and understood as encouragement to do so.”

The rioters who [attacked](#) the Capitol on Jan. 6 bludgeoned a police officer to death with a fire extinguisher; dragged another officer down several steps and beat him with an American flag; attempted to locate and assassinate Speaker of the House Nancy Pelosi; constructed a gallows on Capitol grounds and called for the hanging of Vice President Mike Pence; ransacked Congressional offices; looted federal property; and forced terrified elected



officials and their staff into hiding for several hours. The rioters [organized](#) their efforts on sites such as Facebook, Twitter, and Parler, where false claims about election fraud and increasingly unhinged conspiracy theories like QAnon had proliferated for months.

Twitter's decision to ban Trump came after Facebook's announcement that it would be suspending Trump's account [indefinitely](#); more [social media bans](#) – not just of Trump, but of other individuals who promoted lies about the election, endorsed white supremacist rhetoric and violence, or encouraged further insurrection efforts – quickly followed. On Jan. 9, Google and Apple removed the rightwing-dominated social media site [Parler](#) from their app stores after the site refused to moderate violent content, and Amazon removed the site from its web hosting services later that same day, citing the platform's multiple violations of Amazon's terms of service.

While many praised the social media crackdown, several prominent Republican figures [characterized](#) it as an attack on free speech and the First Amendment – often taking to social media to do so. Secretary of State Mike Pompeo tweeted, “Silencing speech is dangerous. It’s un-American. Sadly, this isn’t a new tactic of the Left. They’ve worked to silence opposing voices for years.” Trump’s son, Donald Trump Jr., tweeted, “Free Speech Is Under Attack! Censorship is happening like NEVER before! Don’t let them silence us.” Congressman Matt Gaetz [proclaimed](#), on Twitter, “We cannot live in a world where Twitter’s terms of service are more important than the terms in our Constitution and Bill of Rights.”

Many conservatives also complained about how many [followers they were losing](#) as Twitter purged accounts violating their terms of service. Pompeo tweeted a graphic purporting to show how many thousands of followers he and other high-profile right-wing individuals had lost. Scott Atlas, who served as a Trump advisor on COVID-19 policy, bemoaned on Jan.11, “I have lost 12k followers in the past few days.” Sarah Huckabee Sanders, the former White House press secretary, tweeted on Jan. 9, “I’ve lost 50k+ followers this week. The radical left and their big tech allies cannot marginalize, censor, or silence the American people. This is not China, this is United States of America, and we are a free country.”

But it was not only conservatives who raised concerns about social media platforms banning Trump and cracking down on election disinformation and violent propaganda. Following Facebook’s indefinite suspension of Trump’s account, National Security Agency whistleblower Edward Snowden [tweeted](#), “Facebook officially silences the President of the United States. For better or worse, this will be remembered as a turning point in the battle for control over digital speech.” The Electronic Frontier Foundation (EFF) somberly [observed](#) that “we are always concerned when platforms take on the role of censors.” A senior legislative counsel for the American Civil Liberties Union (ACLU) [wrote](#) “it should concern everyone when companies like Facebook and Twitter wield the unchecked power to remove people from platforms that have become indispensable for the speech of billions.” ACLU attorney Ben Wizner criticized Amazon’s decision to cut off Parler, [telling](#) the New York Times that “[t]here will be times when large majorities of people want to repel speech that is genuinely important... I think we should encourage, in a broad sense, companies like Amazon to embrace neutrality principles so that there can be a diversity of voices online.”

The swift social media crackdown on harmful online content following the events of Jan. 6 demonstrated that technology companies have long had the capacity to address online extremism and abuse – they have only lacked the will. And the cries of censorship that these belated and modest moves have triggered from influential figures across the political spectrum helps explain why that will has been lacking for so long. The telecommunications industry has actively encouraged the public to think of online platforms as natural, essential, and unmediated outlets for free speech. Society has become so dependent on social media for communication, news, commerce, education, and entertainment that any restriction of access feels like a violation of [constitutional significance](#). The outsized influence of the internet over daily life leads users to think of online platforms and tech companies not as the premises and products of private businesses, but as public forums controlled by quasi-governmental actors.

The tech industry’s invocation of “free speech” as a core value contributes greatly to the American public’s confusion between state action restricting

---

***Powerful tech companies have for decades been invoking the laissez-faire principles of the First Amendment to absolve themselves of responsibility for abuse and extremism that flourish on their platforms and services, undermining the concept of collective responsibility that is central to a functioning society, both online and off.***

---

speech, which implicates the First Amendment, and private action, which does not. It also contributes to the erasure of the distinction between speech and conduct, and the distinction between speech protected by the First Amendment and speech that is not. Powerful tech companies have for decades been invoking the laissez-faire principles of the First Amendment to absolve themselves of responsibility for abuse and extremism that flourish on their platforms and services, undermining the concept of [collective responsibility](#) that is central to a functioning society, both online and off.

The most powerful tool for this destructive agenda has been Section 230 of the Communications Decency Act, which courts have interpreted as broadly insulating online intermediaries from liability even when they knowingly benefit from harmful content and conduct on their platforms and services. Courts have interpreted Section 230 to protect online classifieds sites from responsibility for advertising sex trafficking, online firearms sellers from responsibility for facilitating unlawful gun sales, online marketplaces from responsibility for putting defective products into the stream of commerce, and social media platforms from responsibility for the organization and encouragement of terrorist acts.

Section 230 has, without a doubt, produced a wealth of expressive, economic, and informational benefits. But both the benefits and the harms

flowing from the exceptional immunity granted to the tech industry are unequally distributed. For while the anti-regulatory, pro-corporation, techno-utopian system made possible by courts' expansive interpretation of Section 230 immunity generates enormous capital, both literal and symbolic, the vast majority of that capital stays firmly in the hands of those who have always had more of it than everyone else: the wealthy, the white, the male. While Section 230 does indeed amplify free speech, increase profits, and enable informational dominance for the powerful and the privileged, it also enables the silencing, bankrupting, and subordination of the vulnerable.

The concept of “[cyber civil rights](#)” (a phrase [coined](#) by Professor Danielle Keats Citron in 2009), highlights how the internet has rolled back many recent gains in racial and gender equality. The anonymity, amplification, and aggregation possibilities offered by the internet have allowed private actors to discriminate, harass, and threaten vulnerable groups on a massive,

---

***While Section 230 does indeed amplify free speech, increase profits, and enable informational dominance for the powerful and the privileged, it also enables the silencing, bankrupting, and subordination of the vulnerable.***

---

unprecedented scale. Abundant [empirical evidence demonstrates](#) that online abuse further chills the intimate, artistic, and professional expression of individuals whose rights were already under assault offline. As the internet has multiplied the possibilities of expression, it has also multiplied the possibilities of repression, facilitating a censorious backlash against women and minorities. The internet lowers the costs of abuse by providing abusers with anonymity and social validation, while providing new ways to increase

---

***We are all living in the world Section 230 built: where expressive, economic, and information inequalities divide our society; where a President can use social media platforms to incite violence against his own citizens; where domestic terrorists can coordinate bloody attacks on the Capitol; where global corporations can extract astronomical profits from exploiting private data, where women and minorities are silenced by online mobs, and where massive disinformation and misinformation campaigns can micro-target populations to create public health crises, foment armed rebellions, and undermine democracy itself.***

---

the range and impact of that abuse. The online abuse of women in particular amplifies sexist stereotyping and discrimination, compromising gender equality online and off.

We are all living in the world Section 230 built: where expressive, economic, and information inequalities divide our society; where a President can use social media platforms to incite violence against his own citizens; where domestic terrorists can coordinate bloody attacks on the Capitol; where global corporations can extract astronomical profits from exploiting private data, where women and minorities are silenced by online mobs, and where massive disinformation and misinformation campaigns can micro-target populations to create public health crises, foment armed rebellions, and undermine democracy itself.

## RECOMMENDATIONS

In light of the foregoing, the Biden-Harris Administration should take the following three steps.

**1. Instruct Congress to pass legislation that amends Section 230 to protect online intermediaries against liability only for the speech of third parties and to deny immunity to platforms that demonstrate deliberate indifference to harmful content.**

### **A. Explicitly limiting Section 230’s protections to speech.**

Both critics and defenders of Section 230 agree that the statute provides online intermediaries broad immunity from liability for a wide range of internet activity. While critics of Section 230 point to the extensive range of harmful activity that the law’s deregulatory stance effectively allows to flourish, Section 230 defenders argue that an unfettered internet is vital to a robust online marketplace of ideas. The marketplace of ideas is a familiar and powerful concept in First Amendment doctrine, serving as a justification for a laissez-faire approach to speech. Its central claim is that the best approach to bad or harmful speech is to let it circulate freely, because letting ideas compete in the market is the best way to sort truth from falsity and good speech from bad speech.

The internet-as-marketplace-of-ideas presumes, first of all, that the internet is primarily, if not exclusively, a medium of speech. The text of Section 230 reinforces this characterization through the use of the terms “publish,” “publishers,” “speech,” and “speakers” in 230(c), as well as the finding that the “Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.”

When Section 230 was passed, it may have made sense to think of the internet as a speech machine. In 1996, the internet was text-based and predominantly noncommercial. Only 20 million American adults had internet access, and these users spent less than half an hour a month online. But by 2019, 293 million Americans were using the internet, and they were using it not only to communicate, but also to buy and sell merchandise, find dates, make restaurant reservations, watch television, read books, stream music, and look for jobs. According to Section 230 [enthusiast](#),

the entire suite of products we think of as the internet—search engines, social media, online publications with comments sections, Wikis, private message boards, matchmaking apps, job search sites, consumer

review tools, digital marketplaces, Airbnb, cloud storage companies, podcast distributors, app stores, GIF clearinghouses, crowdsourced funding platforms, chat tools, email newsletters, online classifieds, video sharing venues, and the vast majority of what makes up our day-to-day digital experience—have benefited from the protections offered by Section 230.

But many of these “products” have very little to do with speech and, indeed, many of their offline cognates would not be considered speech for First Amendment purposes. If, as many defenders of Section 230 as currently written would have it, the broad immunity afforded online intermediaries is justified on First Amendment principles, then it should apply only with regard to online activity that can plausibly be characterized as speech. What is more, it should only apply to third-party speech for which platforms serve as true intermediaries, not speech that the platform itself creates, controls, or profits from.

Section 230 should be amended to make explicitly clear that the statute’s protections only apply to speech by replacing the word “information” in (c) (1) with the word “speech.” This revision would put all parties in a Section 230 case on notice that the classification of content as speech is not a given, but a fact to be demonstrated. If a platform cannot make a showing that the content or information at issue is speech, then it should not be able to take advantage of Section 230 immunity.

## **B. Explicitly committing to the principle of collective responsibility and incentivizing intervention.**

Many harmful acts are only possible with the participation of multiple actors with various motivations. The doctrines of aiding and abetting, complicity, and conspiracy all reflect the insight that third parties who assist, encourage, ignore, or contribute to the illegal actions of another person can and should be held responsible for their contributions to the harms that result, particularly if those third parties benefited in some material way from that



contribution. While U.S. law, unlike the law of some countries, does not impose a general duty to aid, it does recognize the concept of collective responsibility. Third parties can be held both criminally and civilly liable for the actions of other people for harmful acts they did not cause but did not do enough to prevent.

Among the justifications for third-party liability in criminal and civil law is that this liability incentivizes responsible behavior. Bartenders who serve alcohol to obviously inebriated patrons can be sued if those patrons go on to cause car accidents; grocery stores can be held accountable for failing to clean up spills that lead to slip and falls; employers can be liable for failing to respond to reports of sexual harassment. Such entities are often said to have breached a “duty of care,” and imposing liability is intended to give them incentive to be more careful in the future. It is a central tenet of tort law that the possibility of such liability incentivizes individuals and industries to act responsibly and reasonably.

Conversely, grants of immunity from such liability risk encouraging negligent and reckless behavior. The immunity granted by Section 230 does just that, despite the evocative title of its operative clause, “Protection for ‘Good Samaritan’ blocking and screening of offensive material.” This title suggests that Section 230 is meant to provide “Good Samaritan” immunity in much the same sense as “Good Samaritan” laws in physical space. Such laws do not create a duty to aid, but instead provide immunity to those who attempt in good faith and without legal obligation to aid others in distress. While Good Samaritan laws generally do not require people to offer assistance, they encourage people to assist others in need by removing the threat of liability for doing so.

Subsection (c)(2) of Section 230 is a Good Samaritan law in a straightforward sense: it assures providers and users of interactive computer services that they will not be held liable with regard to any action “voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable” or “taken to enable or make available



to information content providers or others the technical means to restrict access” to such material. Importantly, because most interactive computer service providers are private entities, their right to choose whether to carry, promote, or associate themselves with speech is not created by Section 230, but by the First Amendment. Subsection (c)(2) merely reinforces this right by making it procedurally easier to avoid specious lawsuits.

On the other hand, Subsection 230(c)(1)’s broad statement that “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,” has been interpreted in ways directly at odds with Good Samaritan laws, as well as with a host of other legal principles and settled law. Where (c)(2) offers immunity to interactive computer service providers in exchange for intervening in situations where they have no duty of care, (c)(1) has been read to provide the same immunity to providers who do nothing at all to stop harmful conduct – and, even more perversely, extends that same immunity to providers who actively profit from or solicit harmful conduct. Section 230(c)(1) has been invoked to protect message boards like [8chan](#) (now 8kun), which provide a platform for mass shooters to spread terrorist propaganda, online firearms marketplaces such as [Armslist](#), which facilitate the illegal sale of weapons used to murder domestic violence victims, and to classifieds sites like [Backpage](#) (now defunct), which was routinely used by sex traffickers to advertise underage girls for sex.

In subsidizing platforms that directly benefit from illegal and harmful conduct, Section 230(c)(1) creates a classic “[moral hazard](#),” ensuring that the multibillion-dollar corporations that exert near-monopoly control of the Internet are protected from the costs of their risky ventures even as they reap the benefits. Given that the dominant business model of websites and social media services is based on advertising revenue, they have no natural incentive to discourage abusive or harmful conduct: “[abusive posts still bring in considerable ad revenue... the more content that is posted, good or bad, the more ad money goes into their coffers.](#)”

Online intermediaries who do not voluntarily intervene to prevent or alleviate harm inflicted by another person are in no sense “Good Samaritans.” They are at best passive bystanders who do nothing to intervene against harm,

and at worst, they are accomplices who encourage and profit from harm. Providing them with immunity flies in the face of the longstanding legal principle of collective responsibility that governs conduct in the physical world. In physical spaces, individuals or businesses that fail to “take care” that their products, services or premises are not used to commit wrongdoing can be held accountable for that failure. There is no justification for abandoning this principle simply because the conduct occurs online.

Creating a two-track system of liability for offline and online conduct not only encourages illegality to move online, but also [erodes](#) the rule of law offline. Offline entities can plausibly complain that the differential treatment afforded by broad interpretations of Section 230 violates principles of fairness and equal protection, or to put it more bluntly: if they can do it, why can’t we? There is a real risk that Section 230’s abandonment of the concept of collective responsibility will become the law offline as well as on.

To undo this, Section 230 (c)1 should be further amended to clarify that the prohibition against treating providers or users of interactive computer services as a publisher or speaker should only apply to speech *wholly provided by another information content provider, unless such provider or user intentionally encourages, solicits, or generates revenue from this speech.* In addition, a new subsection should be added to Section 230 to explicitly exclude from immunity intermediaries who exhibit deliberate indifference to unlawful content or conduct.

The revised version of Section 230(c) would read:

**(1) Treatment of publisher or speaker**

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any ~~information~~ **speech wholly** provided by another information content provider, **unless such provider or user intentionally encourages, solicits, or generates revenue from this speech.**

**(2) Civil liability**

No provider or user of an interactive computer service shall be held liable on account of-

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1);<sup>1</sup>

(3) **Limitations.** The protections of this section shall not be available to a provider or user who manifests deliberate indifference to unlawful material or conduct.

## **2. Instruct Congress to pass clear and effective legislation addressing severe online harms disproportionately targeted at women and minorities, including nonconsensual pornography, sextortion, doxing, and deep fakes.**

The new administration should call for the passage of federal legislation addressing new and highly destructive forms of technology-facilitated abuse. Doing so will ensure that victims of these abuses will have a path to justice with or without Section 230 reform, as Section 230 does not apply to violations of federal criminal law.

Victims of online abuse are not safe on or offline. They suffer anxiety, severe emotional distress, and damage to their reputations, intimate relationships, and employment and educational opportunities. Some victims are forced to relocate, change jobs, or change their names. Some have committed suicide.

In addition to inflicting economic, physical, and psychological harms on victims, unchecked online abuse also inflicts free speech harms. Online abuse, especially online sexual abuse, silences victims. To avoid further harassment and threats to themselves and their families, targeted individuals delete their social media accounts, cancel speaking engagements, and refrain from engaging in public discourse. Many alter their professional

choices, including [journalists](#) who feel compelled to refrain from reporting on controversial topics and politicians forced to [leave office](#) due to intimidation.

In other words, the failure to regulate online abuse chills speech. The corollary of this observation is that regulation is sometimes necessary to encourage speech. According to a [2017 study](#) by Jonathon Penney, regulating online abuse “may actually facilitate and encourage more speech, expression, and sharing by those who are most often the targets of online harassment: women.” Penney suggests that when women “feel less likely to be attacked or harassed,” they become more “willing to share, speak, and engage online.” Knowing that there are laws criminalizing online harassment and stalking “may actually lead to more speech, expression, and sharing online among adult women, not less.” As expressed in the title of a [recent article](#) co-authored by Penney and Danielle Keats Citron, sometimes “law frees us to speak.”

Technology-facilitated abuses that have proven particularly destructive include nonconsensual pornography (also known as “revenge porn”), sextortion (a form of blackmail in which sexual information or images are used to extort sexual acts and/or money from the victim), doxing (the publication of private or personally identifying information, often with malicious intent), and so-called “deep fakes” (the use of technology to create false visual and audio material indistinguishable from authentic visual and audio representations of individuals). Fortunately, strong federal legislation has already been drafted on the first three issues, and there are strong efforts in process to address the fourth.

The administration should direct Congress to pass the Stopping Harmful Image Exploitation and Limiting Distribution (SHIELD) Act of 2019 (S.2111/H.R.2896), sponsored by Senator Kamala Harris and Congresswoman Jackie Speier, which would make it a crime to knowingly distribute or threaten to distribute private, sexually explicit visual material of an individual, when the distributor knows or recklessly disregards whether the depicted individual has a reasonable expectation of privacy and has not consented

to the distribution, and has no reasonable belief that distribution touches a matter of public concern.

The administration should also call upon Congress to pass the Online Safety Modernization Act of 2017 (H.R.3067), sponsored by Congresswoman Katherine Clark, which would prohibit multiple forms of online abuse, which the bill refers to as “cybercrimes against individuals.” These include coercion of sexual acts, sexual contact, and the production of sexually explicit visual depictions; coercion or extortion involving threats to publish sexually explicit visual depictions; the reporting of false or misleading information to initiate an emergency law enforcement response; and the publication of personally identifiable information of another person to threaten, intimidate, harass, or cause other harm. The Act also requires the Department of Justice to develop a national strategy to reduce, investigate, track, and prosecute cybercrimes against individuals, as well as providing personnel, training, state and local grants towards this goal, and requires the Federal Bureau of Investigation to create a category, in the Uniform Crime Reports, for an offense that constitutes a cybercrime against individuals.

The administration should additionally direct Congress to draft and enact a statute criminalizing so-called “deep fakes.” The statute should target a narrow category of digital forgeries, defined as audiovisual material that has been created or materially altered to falsely appear to a reasonable observer to be an actual record of actual speech, conduct, appearance, or absence of an individual, that is created, distributed, or reproduced with the intent to cause serious harm or with reckless disregard for whether serious harm would result.

**3. Appoint a Commissioner on Cyber Abuse and Extremism to work with the National Task Force on Online Harassment and Abuse and to lead research and policy efforts to combat technology-facilitated abuse, with particular focus on the impact on the privacy, free expression, and democratic participation of women, minorities, and other marginalized groups.**

The Biden-Harris administration's announcement that it will convene a [National Task Force on Online Harassment and Abuse](#) to study the connections between sexual harassment and abuse, mass shootings, extremism and violence against women signals that it recognizes how technology-facilitated abuse jeopardizes not only women's physical safety, but also their rights to expression, privacy, education, professional achievement, and civic participation. The administration should appoint a Commissioner on Cyber Abuse and Extremism to work in coordination with this Task Force and to spearhead research and policy efforts to combat technology-facilitated abuses, including sexual harassment and exploitation, radicalization, and mis/disinformation. These efforts should be particularly focused on safeguarding and promoting the privacy, free expression, and democratic participation of women, minorities, and other marginalized groups.

Among the Commissioner's primary areas of focus should be the often-overlooked role that misogyny plays in violent extremism, given that the abuse of women is one of the most common characteristics of mass shooters and other terrorists who are increasingly radicalized in online spaces. Understanding the interplay of technology, firearms, and misogyny is vital for combating not only violence against women, but violence against society as a whole. The Commissioner should also make recommendations regarding the responsibility that social media and other internet platforms share in the encouragement and amplification of abuse.

## OBJECTIONS AND CHALLENGES

### *A. Danger to Free Speech.*

Some claim that any reform of Section 230 jeopardizes free speech in a larger sense, even if not strictly in the sense of violating the First Amendment. Of course, free speech is a cultural as well as a constitutional matter. It is shaped by non-legal as well as legal norms, and tech companies play an outsized role in establishing those norms. There is indeed good reason to be concerned

about the influence of tech companies and other powerful private actors over the ability of individuals to express themselves. This is an observation scholars and advocates who work on online abuse issues have been making for years—that some of the most serious threats to free speech come not from the government, but from non-state actors. Marginalized groups in particular, including women and racial minorities, have long battled with private censorial forces as well as governmental ones.

But the unregulated internet—or rather, the selectively regulated internet—is exacerbating, not ameliorating, this problem. The current model shielding platforms from liability may ensure free speech for the privileged few; protecting free speech for all will require legal reform.

### ***B. Piecemeal Approach.***

Some reformers maintain that the best way to reform Section 230 is to create explicit exceptions from its legal shield for certain types of particularly egregious behavior. This was the approach taken in the controversial 2016 Stop Enabling Sex Traffickers Act (SESTA), which amended Section 230 by rendering websites liable for knowingly hosting sex trafficking content. But Section 230's problems are structural, and its flaws [cannot be cured](#) through a piecemeal approach. The exceptions approach is inevitably underinclusive, establishing an arbitrary hierarchy of harms that creates troubling normative and fairness implications. Such an approach also requires Section 230's exceptions to be regularly updated, an impractical option given the glacial pace of congressional efforts and partisan deadlock.

## CONCLUSION

The problem of platform liability brings to mind a popular expression often attributed to the 18th-century statesman Edmund Burke: “The only thing necessary for the triumph of evil is for good men to do nothing.” While Burke did not author those words, he did offer a similarly wise sentiment that can help guide efforts to fix what the law of cyberspace has broken: “When bad men combine, the good must associate; else they will fall one by one, an unpitied sacrifice in a contemptible struggle.”

### ABOUT THE AUTHOR

**Dr. Mary Anne Franks** is Professor of Law and Dean’s Distinguished Scholar at the University of Miami School of Law, where she teaches First Amendment law, Second Amendment law, criminal law and procedure, and law and technology. She serves as the President and Legislative and Tech Policy Director of the nonprofit organization Cyber Civil Rights Initiative and is the author of the award-winning book *The Cult of the Constitution: Our Deadly Devotion to Guns and Free Speech* (2019). Twitter handle: @ma\_franks



# MIDDLEWARE FOR DOMINANT DIGITAL PLATFORMS: A TECHNOLOGICAL SOLUTION TO A THREAT TO DEMOCRACY

STANFORD CYBER POLICY CENTER

Francis Fukuyama, Barak Richman, Ashish Goel,  
Roberta R. Katz, A. Douglas Melamed, Marietje Schaake

# MIDDLEWARE FOR DOMINANT DIGITAL PLATFORMS: A TECHNOLOGICAL SOLUTION TO A THREAT TO DEMOCRACY

*Although most critics emphasize the economic dangers that digital monopolists pose, at least equally if not more significant are their threats to democratic politics. We offer a technology-based solution: requiring the dominant platforms to allow users to install “middleware.” This would take editorial power away from a small number of technology platforms and hand it to a diverse group of competitive firms that would allow users to tailor their online experiences.*

---

## INTRODUCTION

**T**he internet economy has produced digital platforms of enormous economic and social significance. They have created a variety of enormous benefits for consumers, workers, producers, voters and other participants in civic life around the world. These platforms—specifically, Google, Facebook, Amazon, Twitter, and Apple—now play central roles in how millions of Americans obtain information, spend their money, communicate with fellow citizens, and earn their livelihoods. Their reach is also felt globally, extending to many countries around the world. They have amassed the economic, social, and political influence that very few private entities have ever obtained previously. Accordingly, they demand careful consideration from American policymakers, who should soberly assess whether the nation’s current laws and regulatory institutions are adequately equipped to protect people against potential abuses by platform companies.

Although most critics emphasize the economic dangers that these digital monopolists pose, at least equally if not more significant are their threats to democratic politics. Since 2016 there has been substantial discussion about fake news, filter bubbles, targeted political advertising, propagation of conspiracy theories, and the power of platforms to vastly amplify (or bury)

particular voices in democratic political debate. The ultimate fear is that the platforms themselves have amassed sufficient power that they could potentially sway an election, either as a matter of deliberate choice or as a result of being unwittingly manipulated by other political actors. These political harms have not yet been given sufficient attention in policy circles, especially with respect to possible remedies. We discuss those harms and potential remedies at considerable length in this report and conclude with policy recommendations.

In this regard, scale matters acutely. We expect democratic debate and politics to be pluralistic and to protect freedom of speech. But the scale of today's platforms gives them extraordinary power to reach broad audiences, much like the network television oligopoly of the 1950s and '60s, and their control over what appears and is disseminated on their platforms can shape both beliefs and behavior.

Consider also that the platforms—Facebook, Amazon, and Google in particular—possess information about our individual lives that empower them to engage in potentially damaging conduct that prior monopolists never had. They know what we buy, where we work, where we live, where we go, with whom we communicate, and what we value. They know our friends and family, our income and our possessions, and many of the most intimate details of our lives. What if a platform executive with corrupt intentions were to exploit embarrassing information to force the hand of a public official? Alternatively, imagine a misuse of private information in conjunction with the powers of the government, perhaps if Facebook were to team up with a politicized Department of Justice, or Twitter to be bought by an investor in an adversarial state. How can we ensure that the platforms' amassing of personal information will not corrupt government powers and the political process?

The platforms' ability to gather data and information and to curate content would not be as problematic if they were less dominant in their role as information filters—if, for example, there were a large number of important digital intermediaries for news and other information providers. In a more

competitive platform environment, such curation would be a unique selling point. Indeed, curation remains highly desirable in the aggregate, since a totally uncensored internet quickly becomes a miasma of disinformation, spam, pornography, and incivility.

We therefore introduce the concept of middleware to stem the control of dominant platforms over communication and political discourse. Middleware is software, provided by a third party and integrated into the dominant platforms, that would curate and order the content that users see. Users would choose among competing middleware algorithms, selecting providers that reflect their interests and have earned their trust, and thereby would dilute the platforms' editorial control over political communication. We urge the Biden Administration to explore the potential of middleware solutions with technology sector leaders and to develop the regulatory capacity within a specialized regulatory agency to make middleware possible.

---

***No liberal democracy is content to entrust concentrated political power to individuals based on assumptions about their good intentions or on the merits of their business models, which is why we place checks and balances on that power.***

---

The growing political power of the current major digital platforms is like a loaded weapon sitting on the table in front of us. At the moment, we are reasonably confident that the people sitting on the other side won't deliberately pick up the gun and shoot us with it. The question for American democracy is whether it is safe to leave the gun on the table, where others with less good intentions—whether the owners of the platforms or outsiders

who figure out how to manipulate them for their purposes—could come along and pick it up. No liberal democracy is content to entrust concentrated political power to individuals based on assumptions about their good intentions or on the merits of their business models, which is why we place checks and balances on that power.

## MIDDLEWARE AS A SOLUTION

A variety of policy interventions have been proposed to combat the outsized power of these digital giants. Because much of the platforms' influence is connected to their monopoly positions, many have turned to antitrust laws to curtail the dominance of these digital platforms. Antitrust law, however, is designed to redress economic harms, and though antitrust enforcement actions might fruitfully bring economic benefits where competition is currently lacking, they would be ineffective in directly confronting the political harms that the platforms now pose. Some have consequently proposed expanding antitrust's domain beyond economic concerns to include a variety of political values, so as to retool the Sherman Act to confront a wider set of policy challenges in the platform age. However, we are concerned that reforming antitrust's consumer welfare standard would cause damaging policy incoherence, invite politically motivated and unprincipled actions, and erode support for procompetitive policies. Some alternatively have proposed requiring data interoperability, data portability, or privacy protections to curtail the political influence of the dominant platforms. Even if these proposed remedies have their respective merits, they overlook technical difficulties specific to individual platforms and might inadvertently undermine other policy objectives.

Very few policymakers have considered pursuing structural interventions to stem platform dominance over information content, but such technological interventions do offer very promising remedies. Specifically, we propose stimulating the creation of a competitive layer of companies offering middleware products. Although middleware is traditionally defined as computer software that provides services beyond those available from an operating system, including the software that connects operating systems

with applications, we use the term to include software and services that would add an editorial layer between the dominant internet platforms and internet users.

We view middleware as an opportunity to introduce competition and innovation into markets currently dominated by the principal internet platforms. A competitive middleware sector would help solve this problem by outsourcing content curation to organizations that enable consumers to tailor their feeds to their own explicit preferences. At the same time, middleware could be a superior alternative to structural remedies imposed by either courts or regulators because, among other things, it would directly respond to consumer preferences and market actors.

### ***The nature and function of middleware***

By “middleware,” we refer to software products that can be appended to the major internet platforms. These products would interconnect with Facebook, Amazon, Apple, Twitter, and Google APIs and allow consumers to shape their feeds and influence the algorithms that those dominant platforms currently employ. Middleware would offer a third-party service chosen by the consumer and would make editorial judgments that are currently provided (usually without transparency) by the platform. Middleware could be integrated into a platform without disintermediating the platform from the user, or it could offer an independent entry point into the platform (though the platforms would likely oppose losing the point of service to the customer). In either case, middleware can tailor the functionality of those websites to the preferences of their users.

We imagine a diversity of middleware products, designed to accommodate the individual platforms and meet specific demands of interested consumers, with transparent offerings and technical features so that users can make informed choices. Middleware can offer fact-checking services, news rankings, relevance priorities, information filters, or other services that supplement those currently supplied by the major platforms. Similarly, middleware could adjust news results from Google searches and Facebook pages. Middleware can also give users more control over commercial content

and privacy settings. For example, consumers could select middleware providers that adjust their Amazon search results to favor domestic production and eco-friendly products, or that make fine-grained choices on Facebook’s privacy settings dashboard. Trusted community organizations or preferred media outlets could offer, sponsor, or endorse middleware providers. Platforms could also offer their own middleware, on the condition that they do not favor their own product over those provided by third parties or make their own middleware a default choice. To learn more about the variety of interventions that middleware can offer, read our white paper [here](#).

### ***The benefits of employing middleware***

Middleware’s primary benefit is that it dilutes the enormous control that dominant platforms have in organizing the news and opinion that consumers see. Decisions over whether to institute fact-checking, remove hate speech, filter misinformation, and monitor political interference will not be made by a single company but will instead be controlled by a variety of informed and diverse intermediaries. For this reason, technology companies—who have expressed an eagerness to outsource some of these decisions—may be willing to embrace controlled offerings of middleware, since it will afford them the space to focus on their core mission, rather than having to determine (and defend) decisions that so significantly affect the information that millions of users consume. And since middleware should increase the value of the platform to consumers by more closely hewing to user preferences, it might generate economic rewards for the platform as well.

Additionally, middleware facilitates competition. It offers a new and distinct layer of potential competition for consumer loyalties and opens a pathway for innovations in managing information, including commercial information that might benefit firms otherwise disadvantaged by the platforms’ business models. It could also open lucrative markets both for technology companies that can improve platform functionality and for civic organizations that want to participate in political and social discourse.

Finally, a middleware system could offer services that many in our society deem to be urgently needed, such as a robust system of fact-checking and

hate-speech moderation. Current platforms hesitate to provide these services because they know their decisions are so consequential and that various people do not trust the motives of the fact-checker. When these services are instead offered by a diversity of providers, no one player exercises outsized power in making fine-grained decisions over content, and users can select providers they trust. Allowing users to choose from multiple middleware providers offers a blueprint for bringing transparency and flexibility to privacy settings, terms of service, and other services that users care about.

Although many platforms already tailor algorithms and customize feeds to meet users' interests and past practices, our middleware proposal is far more transparent than these current practices. Middleware enables users to avoid being dependent on the platforms' currently enormous editorial control over organizing political content and labeling or censoring speech, and it enables new providers to offer and innovate in services that are currently dominated by the platforms.

### ***Questions to be answered for middleware markets***

Although we are enthusiastic about middleware solutions, we explicitly acknowledge that we offer here only a conceptual outline of a middleware approach and that much thinking remains to be done. To start, we highlight three aspects of a new middleware architecture that will require careful elaboration.

First, the role and function of middleware must be determined. We emphasize that, whether by statutory authority or by some other lawful regulation, we consider it necessary to mandate that dominant search engines and social media companies allow users to choose among third-party filters. Moreover, the platforms might be compelled to alert users to the option of installing middleware and to require users to explicitly opt out of middleware use. Middleware can serve its intended purpose only if it is used widely, and a default option that allows users to never consider installing middleware would severely limit its uptake.



Even under these mandatory rules to encourage middleware adoption, the division of responsibility between the dominant platforms and the middleware filters could vary. At one extreme, the middleware performs all of the essential functions—such as procuring content, sequencing results, and distributing feeds—and the underlying platform serves as little more than a neutral pipe. At the other extreme, the platform continues to curate and rank the content with its standard algorithms, and the middleware could do no more than serve as a supplemental filter to the platform’s output, such as by tagging specific pieces of content with labels or warnings. It is unlikely that either of these extreme arrangements would be satisfactory; the former would likely prompt aggressive resistance from the current platforms because it would undermine their business and revenue models (and perhaps future innovation), while the latter would likely be inadequate to curb the dominant platforms’ power in curating and disseminating content. An intermediate role would probably be preferable, perhaps one in which middleware is able both to provide filters for specific news stories and to develop ranking and labeling algorithms selected by the users. Developing this intermediate role would require further reflection, both from a regulatory point of view and in terms of technical architecture.

Second, a business model for middleware providers must be sufficiently attractive to induce an adequate supply. The most logical approach would be to establish revenue sharing arrangements between the dominant platforms and the third-party providers of middleware. If a middleware product enhances the value of the platforms to users, the platforms might be able to generate increased advertising (or maybe, in the future, user fee) revenues that could be shared with the middleware provider. Alternatively, the middleware provider might be able to charge user fees or sell advertising directly.

If a middleware product reduces the value of the platform by, for example, making it harder for the platform to optimize the targeted advertising or by diverting advertising revenues to middleware providers, the platforms will predictably resist a middleware requirement. Middleware might have to be offered as an alternative to more onerous regulatory requirements or

legal risk related to the platforms' role as providers of political or otherwise offensive information. If middleware providers are themselves able to obtain advertising revenues or user fees, they might be expected to share their revenues with the platforms. If the parties are unable to agree on a fee sharing arrangement, the terms of such revenue sharing might have to be established by regulators. The fee sharing must navigate a balance between encouraging the development of a robust supply of trustworthy middleware while also inducing the cooperation of (or avoiding hostile refusals from) dominant platforms and preserving their rewards for investment in and innovation on the platforms.

Third, a technical framework must be developed that would invite a diversity of middleware products. The technological requirements for a vibrant middleware market might be demanding. Middleware developers must be able to easily deploy their products to work with the various dominant platforms, each of which exhibits different architectures, as well as with other closely related platforms. At the same time, the specifications for middleware access to the platforms should be sufficiently simple that a diversity of technologists and nonprofits can sponsor offerings. Moreover, middleware must be prepared to assess at least three different kinds of content: widely accessible public content, including news stories with RSS feeds and tweets from public officials, that already have an identification system for searches and aggregators; public content generated by users of social media networks and search engines that is curated on those platforms, which the platforms must make available and cognizable to third-party providers; and content that is not public but nonetheless might attract the attention of either middleware or platform monitors, such as WhatsApp messages that promote hate speech or individual Facebook posts that encourage violence. Third-party providers will have to identify these different kinds of content and then offer their assessments of, for example, veracity, relevance, or centrality to whatever metric the middleware provider is applying. Because the middleware provider will not have access to private content, middleware services may have to provide labeling algorithms on top of features provided by the platform. Navigating these categories of content and providing consistent services will pose a challenge to third-party providers.

It is critical to get these technical elements right. The middleware intervention would be appropriately questioned if it generated an inadequate supply and diversity of third-party providers, became another tool to capture control over public discourse, or introduced more technological bottlenecks. We believe that a middleware solution has the potential to reduce informational and economic concentration, as long as the technical solutions offer an intuitive and open architecture that fosters a diversity of middleware suppliers and products.

### ***A Specialized Agency***

Our middleware proposal, if adopted, heightens the need for additional agency expertise. Prior calls for a specialized agency—for example, by the Stigler Center, the Shorenstein Center, and a high-profile report submitted to the United Kingdom’s Competition and Markets Authority—have identified the need for greater regulatory proficiency in understanding the economics

---

***We expect that Congress would have to pass new legislation that authorizes an existing agency, or establishes a new specialized agency, to exercise the regulatory functions to foster a middleware market.***

---

of digital markets, appreciating the many uses of personal data and associated threats to privacy intrusions, anticipating the pace and direction of technological change, and recognizing the industry-and economy-wide benefits of establishing common technological and consumer protection standards. In addition to these needs, our middleware proposal would also demand of regulators the capacity to ensure, or if necessary, mandate, the availability of platform APIs to middleware providers, platform compliance

with other conditions necessary to allow middleware providers to offer their products, and fair revenue sharing and adherence to rules that allow middleware business models to thrive. Even more challenging, administrators of our middleware proposal will need to work with industry leaders to chart out the assorted responsibilities and prerogatives for both middleware providers and the platforms and to design the technical framework that will allow middleware offerings to thrive.

It is unlikely that there is authority under any existing statute or court-ordered remedy under existing law to establish the kind of regulation we envision, even if the regulation were housed in an existing administrative body like the FTC or FCC. We expect that Congress would have to pass new legislation that authorizes an existing agency, or establishes a new specialized agency, to exercise the regulatory functions to foster a middleware market. The new statutory authority does not need to be expansive, nor would it be necessary to disrupt or reorganize the operations of other parts of government. An advantage to the middleware proposal is that it leaves most other policy instruments unchanged.

## CONCLUSION

The public should be alarmed by the growth and power of dominant internet platforms, and particularly by their control over political speech. The First Amendment envisioned a marketplace of ideas where competition, rather than regulation, protected public discourse. Yet in a world where large platforms amplify, suppress, and target political messaging, that marketplace breaks down.

Today, governments are launching actions against Big Tech platforms under existing antitrust law in both the United States and Europe, and the resulting cases are likely to be litigated for years to come. But while antitrust law may be effective in mitigating certain economic abuses, it is not likely to fundamentally reduce the size of the major platforms or to require material changes in their business models. Antitrust enforcement is therefore unlikely

---

***Middleware is another potential solution to this problem, and one that has not been adequately explored. It can take editorial power away from a small number of technology platforms and hand it not to a single government regulator, but to a diverse group of competitive firms that would allow users to tailor their online experiences.***

---

to provide an effective remedy for unique political threats to democracy created by platform scale. Straightforward state regulation, data portability, and privacy law have all been advanced as alternative tools to deal with platform scale.

Middleware is another potential solution to this problem, and one that has not been adequately explored. It can take editorial power away from a small number of technology platforms and hand it not to a single government regulator, but to a diverse group of competitive firms that would allow users to tailor their online experiences. This approach would not prevent hate speech or conspiracy theories from circulating, but it would ensure that no single harmful idea will receive the amplification of a dominant information platform. It also ensures, in a way that aligns with the original intent of the First Amendment, that no one idea, whether disseminated by a platform or by those who manipulate them, will drown out all other speech. Today, the content that the platforms offer is determined by murky algorithms generated by artificial intelligence programs. With middleware, platform users would be handed the controls over what they see. They—and not some invisible artificial intelligence program—would determine their ultimate online experience. We believe that this approach deserves further elaboration and testing and should ultimately become the basis for new public policies.

## ABOUT THE AUTHOR

**Francis Fukuyama** is the Olivier Nomellini Senior Fellow at Stanford University's Freeman Spogli Institute for International Studies (FSI), Mosbacher Director of FSI's Center on Democracy, Development, and the Rule of Law (CDDRL), and Director of Stanford's Masters in International Policy Program. Dr. Fukuyama has written widely on issues in development and international politics.

@FukuyamaFrancis

**Barak Richman** is the Katharine T. Bartlett Professor of Law and Business Administration at Duke University. His primary research interests include the economics of contracting, new institutional economics, antitrust, and healthcare policy.

@BarakRichman

**Ashish Goel** is a Professor of Management Science and Engineering and (by courtesy) Computer Science at Stanford University. His research interests lie in the design, analysis, and applications of algorithms.

@ashishgoel

**Douglas Melamed** practiced law for 43 years before spending the 2014-15 academic year at the Stanford Law School as the Herman Phleger Visiting Professor of Law. He was appointed Professor of the Practice of Law in 2015. From 1996 to 2001, Professor Melamed served in the US Department of Justice as Acting Assistant Attorney General in charge of the Antitrust Division and, before that, as Principal Deputy Assistant Attorney General.

**Roberta Reiff Katz**, lawyer and cultural anthropologist, is a Senior Research Scholar at the Center for Advanced Study in the Behavioral Sciences (CASBS) at Stanford University. Ms. Katz was Special Advisor to the Assistant Attorney General for Antitrust, U.S. Department of Justice, in 2009-10.

**Marietje Schaake** is the International Policy Director at Stanford University's Cyber Policy Center and International Policy Fellow at Stanford's Institute for Human-Centered Artificial Intelligence. Between 2009 and 2019, Marietje served as a Member of European Parliament for the Dutch liberal democratic party where she focused on trade, foreign affairs, and technology policies.

@MarietjeSchaake

# OPENING A WINDOW INTO TECH: THE CHALLENGE AND OPPORTUNITY FOR DATA TRANSPARENCY

STANFORD CYBER POLICY CENTER

Nathaniel Persily

# OPENING A WINDOW INTO TECH: THE CHALLENGE AND OPPORTUNITY FOR DATA TRANSPARENCY

In the first year of the Biden administration, we should expect several new initiatives to be proposed relating to technology regulation. Content moderation, privacy, antitrust, and cybersecurity exist on a crowded agenda, although many devils exist in the details of any policy proposals in these areas. Moreover, as anyone who has engaged honestly with these issues recognizes, the impulses that drive policies in these domains often conflict with each other. Navigating the inescapable tradeoffs presents a real challenge to those with authority willing to jump into this political thicket.

Data transparency, however, represents a condition precedent to effective regulation in all of these areas. At present, we do not know even what we do not know concerning a host of pathologies attributed to social media and digital communication technologies. Pundits and policy makers think they have a handle on phenomena as varied as disinformation, hate speech, political bias in content regulation, and microtargeted advertising, but the publicly available data relevant to these problems represents a tiny share of what the platforms possess. The first step toward regulation of these platforms is to grant access to outsiders to bring to light the prevalence and character of the problems that are the target of regulation.

When critics describe Facebook and Google as “data monopolies”, they usually mean it in the antitrust sense. That is, the anticompetition “problem” with those companies is that they have amassed an enormous amount of data, which puts them in a privileged position to deliver targeted advertising as well as tweak their algorithms to maximize engagement. Of course, this amassing of data is also the source of their privacy and surveillance problems, but what sets them apart in the marketplace is the economic chokehold they have on would-be competitors, none of whom can ever



---

***The research that drips out from the companies represents a tiny share of the potential insights that could be gained from their data were access more broadly available.***

---

achieve parity given the years of data these companies have on billions of users.

In a different sense from their economic dominance, though, their status as data monopolies poses a distinct threat to democracy arising from their exclusive access to insights from the mass of data they have collected. Unfortunately, the insights of most value to them often concern how to keep people on the platform and how to target them better with advertising. To be sure, sometimes, after serious vetting from multiple authorities within the companies, internal researchers publish research that has great value to society, on issues such as polarization, news consumption, or even on the effect of certain platform interventions on the health of the information ecosystem. But the research that drips out from the companies represents a tiny share of the potential insights that could be gained from their data were access more broadly available. (These arguments are given fuller treatment in Chapter 13 of Nathaniel Persily & Joshua Tucker, eds., [Social Media and Democracy: The State of the Field and Prospects for Reform](#) (Cambridge Press, 2020).)

Researcher access is not a luxury good for academics; it is a precondition for sound policy concerning the information ecosystem and economy. The U.S. government, like its counterparts around the world, is rushing headstrong and blind toward regulation without a complete understanding of the problems they wish to solve. Legislators need better information about what

---

***Researcher access is not a luxury good for academics;  
it is a precondition for sound policy concerning the  
information ecosystem and economy.***

---

is happening on the major internet platforms and what is happening behind the scenes. For both legal and commercial reasons, the platforms are not going to provide that information willingly.

Of course, the platforms cannot make public all the sensitive data they have on their users. Doing so would be against the law and would be a fundamental violation of user privacy even if it were not. Nor should the platforms (or society) simply trust the government to hold onto the data for its purposes, which likely would include surveillance and criminal investigation. The policy challenge, therefore, involves creating a regime that respects user privacy, keeps user data out of the hands of government, and allows for public facing research that could lead to policy-relevant insights concerning the nature of the online information ecosystem.

Doing so requires legislation. The beginning of such an effort — and it is only a beginning — should include three components. The first concerns immunity from civil and criminal liability when platforms share data with vetted academics under prescribed circumstances. The second involves compulsion of the largest platforms, namely Facebook and Google, to share their data under the circumstances for which they would receive immunity. The third would immunize qualified researchers who scrape publicly available data for research purposes. A new “Platform Transparency and Accountability Act” with these three components could help turbocharge research on the harms and benefits of new communication technologies with a goal of producing well-informed public policy.

---

***The policy challenge, therefore, involves creating a regime that respects user privacy, keeps user data out of the hands of government, and allows for public facing research that could lead to policy-relevant insights concerning the nature of the online information ecosystem.***

---

## **I. SCOPING THE CHALLENGE AND POLICY RESPONSE**

Enacting a compulsory data sharing regime is easier said than done. It is all well and good to say that platforms should share data with researchers, but legally defining which platforms, which data, which researchers, and under what circumstances proves especially challenging. Some models can provide clues, such as the protocols in place for the sharing of census, IRS, or sensitive health data, but none of them quite capture the breadth of the potential data available or the unique position and character of the relevant platforms.

### ***A. Which Platforms?***

Google and Facebook are first among (un)equals when it comes to the sheer volume of social media and digital trace data the firms possess. Any regulatory regime aimed at researcher access should be reverse engineered to capture those two firms in particular. Twitter, which already provides more data than any other firm for researcher access, could also be added to the list, if the focus of the regulation is social media, per se.

But what about Amazon, Apple, and Microsoft? Researchers could gain enormous insight from access to those firms' data. Amazon, in particular, represents a monopoly of a different sort with data on users that could

be extremely helpful to understanding the digital economy. Moreover, if the communications ecosystem is the target for research, what about the cable and cell phone companies, such as Comcast and Verizon? Surely, they possess data farther down the stack that could be helpful in assessing some relevant problems. A similar argument could be made for traditional media companies, e.g., Fox, or “new media” companies, such as Netflix.

To some extent, the universe of firms to which a data access regime would be applicable depends on the range of phenomena one considers worthy of study and the inability of researchers to gain insights from the outside. For those (like me) for whom the principal concern is the health of the information ecosystem and its impact on democracy, Google, Facebook, and Twitter reign supreme. The identification of the relevant firms, then, would include a definition of social media or search firms meeting some threshold of daily or monthly active users.

The [Honest Ads Act](#) took a stab at such a definition in its attempt to force a disclosure regime on online political advertising. That bill defined an “online platform” as “any public-facing website, web application, or digital application (including a social network, ad network, or search engine) which . . . has 50,000,000 or more unique monthly United States visitors or users for a majority of months during the preceding 12 months.” That law might capture more than just the “big three” social media platforms, but the form of the definition could be instructive in refining it further for purposes of researcher access.

It may be that different firms should be compelled to provide data than should be given immunity for voluntarily providing data. In other words, we should encourage a large number of firms to cooperate with approved researchers and be immune from liability for doing so. But when it comes to compelling certain firms to grant researcher access, that extreme measure should be reserved for Google, Facebook, and Twitter. Compelling smaller firms, such as Gab and Parler, let alone traditional or “new” media companies, to grant outside researcher access would raise constitutional concerns as to the First Amendment rights of these companies. (Indeed, as discussed later, such constitutional concerns will also be present for

compulsion of the large companies, but at least their monopoly status might augur toward greater access in the public interest.)

## ***B. Which Researchers?***

One of the most difficult questions in considering researcher access concerns the selection and vetting process for researchers who will be granted access. “Researchers” come in many forms and a wide variety of civil society actors have an interest in the data held by internet platforms. However, some quality control must exist lest political operatives and propagandists repurpose themselves as “researchers” to gain access to platform data. It may also be that a separate regime for platform data access could be erected for think tanks or journalists, many of whom (such as Pew, ProPublica, the Markup, BuzzFeed or the Guardian) have done foundational research on these types of topics. But categories such as journalists or think tanks are not amenable to any limiting principle.

Focusing a data access regime on university-affiliated researchers has several advantages. First, a university is an identifiable “thing,” and while low quality academic institutions exist, regulations can more easily specify the type of institutions that house the academics that should be granted access. Second, universities can be signatories to data access agreements with the platforms so as to add another layer of security (and retribution) against researcher malfeasance. Third, universities have Institutional Review Boards that can provide ethics and Human Subjects review for research proposals. Fourth, in the wake of the Cambridge Analytica scandal, which involved an academic operating outside of his academic capacity, involving universities directly in the process of vetting and vouching for their researchers will make clear to the platforms which researchers are nested in a larger regulatory framework.

Assuming universities are the universe from which to draw the researchers to be granted access, how should the researchers be selected and vetted? The platforms, the government, or some academic association, in theory, could be in the position of deciding which researchers get access. The law should

prescribe a process for designating “qualified researchers” and qualified research projects, which could involve familiar procedures initiated by the National Science Foundation (NSF). The precise body doing the vetting is not critical, so long as the process is transparent and is one step removed from influences from both the platforms and the government.

### ***C. Which data?***

In some settings, it is quite easy to define the data that should be made available for research. For instance, when drug trial data are made available for outside review, there are settled and familiar expectations for what kind of information the pharmaceutical company will provide. For Google and Facebook, though, the volume and variety of data they possess are so vast that any legally defined data access regime cannot simply say “turn over all available data to researchers.” Some kind of principle should specify the range of data that should be available for research, or at least a process for deciding what data should be made available.

As a threshold matter, any available dataset should be anonymized and stripped of personally identifiable information. To be sure, social media data are so rich that enterprising analysts might be able to reidentify people if they were hell-bent on doing so. But the datasets must be delivered in a format with protections that make it extremely difficult to do so. Moreover, as described below, monitoring of the research and researchers should be in place to prevent any reidentification.

At a minimum, researchers should be allowed to analyze any data that is otherwise for sale to commercial entities or advertisers. If the datasets are available for a price, then they can be made available for academic analysis. Similarly, any data that goes into the preparation of government or other reports, such as those relating to enforcement of community standards (e.g., how many pieces of content were designated as hate speech and taken down) should be made available.

However, to get a handle on the prevalence of the most notorious problems on these platforms, information about user exposure, engagement, and other behaviors will be essential, as will data about the producers of content and the policies of the platforms. It would be difficult for the law to specify in advance the range of data that platforms must make available or for which their disclosure to academics would not incur liability. Here too, an outside party, such as the NSF, could be in a better position to evaluate which datasets can reasonably be provided by platforms to answer the most important research questions.

Such was the vision for Social Science One, the outside academic research initiative that I co-chaired until last year and that was established to serve as a broker between firms, such as Facebook, and the research community. In its original vision, the academics affiliated with Social Science One would pose questions to firms like Facebook and the firm would generate datasets that independent researchers could use to answer those questions. For various reasons, including those related to privacy, that model did not succeed. Instead, we moved to a model in which Facebook would provide a privacy-protected dataset and then researchers would apply, through the Social Science Research Council, to have access to it. This, too, proved suboptimal, because, in the end, Facebook said it could not find a way to provide broad access to the data it possessed while complying with its obligations under the FTC consent decree and applicable privacy laws around the world. The growing pangs of Social Science One, however, can be instructive for federal legislation that might compel platforms to provide researcher access and for the development of an agency with the power to define the datasets that might be made available for outside analysis. The experience has demonstrated that the necessary researcher access will not emerge voluntarily from the platforms. Their economic incentives counsel against it, and the applicable privacy laws (and consent decrees) create liability risks that far exceed the benefits – PR, public-spirited, or otherwise – of giving access to data to a bunch of academics.

---

***the purpose of academic access is to combat the privileged monopoly position that insiders at the firms have over socially meaningful insights derived from the data in their possession. Private data has been and will continue to be analyzed by employees of the internet companies. The question is whether anyone else detached from the profit-making motives of the firms will have access to those same data to produce research in the public interest.***

---

## **II. A THREE-PRONGED APPROACH TO REGULATION**

Regulation to promote transparency through academic access to platform data must reckon with the serious privacy concerns that surround release of any social media data. Indeed, a transparency bill, such as that proposed here, should be adopted as part of a larger comprehensive privacy bill that makes clear how the balance shall be struck in limited, protected circumstances between privacy and other competing values. However, the purpose of academic access is to combat the privileged monopoly position that insiders at the firms have over socially meaningful insights derived from the data in their possession. Private data has been and will continue to be analyzed by employees of the internet companies. The question is whether anyone else detached from the profit-making motives of the firms will have access to those same data to produce research in the public interest.

### ***A. Platform Immunity for Granting Researcher Access***

Unless platforms are given immunity from suit, the data they willingly provide, if any, will not be amenable to the kind of detailed analysis that will produce the necessary public benefits. It is all well and good for academics



to preach the value of public facing research, but the platforms are staring down multi-billion dollar fines if they leak user data. Moreover, the general counsels at the platforms tend to adopt the maximalist and most risk-averse interpretation of applicable privacy laws, sometimes dismissing research or public interest exceptions in such laws as vague and insufficiently shielding the company from liability. In short, if platforms are going to share their data, they need to know they will not be sued as a result.

At the same time, these privacy protections exist for a reason. The major platforms have a sorry history of protecting user privacy, and their business models depend on massive surveillance of users to gather information that enables targeted advertising. They possess data on some of the most private aspects of people's lives, and in some respects, they understand user psychology and behavior better than users themselves. Any pathway for research must ensure, to the extent possible, that an individual user's data will not be leaked to the public or even to the researcher.

To be clear, though, if researchers have data access akin to that of firm insiders, there is a risk that they will abuse their position. The task of policy, therefore, is to make sure that does not happen. This can be done at every stage of the research process. The law needs to specify, in detail, the privacy-protecting prerequisites for a platform to receive legal immunity when it shares data.

First, the law must identify a process for selecting/vetting researchers, research questions, and research designs. As noted above, this can be done by the NSF or a comparable institution. Similar methods related to IRS data, although not terribly routinized, have allowed researchers to do [pathbreaking work](#) on social mobility.

Second, the law must specify the environment in which the research will be conducted. Three options warrant consideration for where the data will be contained and the research conducted: (1) at the firm itself; (2) in a government supervised depository; or (3) at a university or other data hub, akin to the [Federal Statistical Research Data Centers](#). Depending on the nature of the data, it may make the most sense for the data to remain at the firm under its control. Delivering private social media data to a government

facility runs the risk of actual or perceived government surveillance of users. Depositing the data with secure, government-approved university facilities would make the data more broadly accessible and keep the data one step removed from the government. But at least in the short term, if for no other reason than to build confidence, the firms themselves could be made responsible for the secure facilities for the data environments for research.

What should those data environments look like? Again, analogies from similar secure facilities related to health, financial, or even national defense data will prove helpful. Among the key features of the environment, apart from all the expected cybersecurity measures, would be real time observation and recording of the researchers. Researchers need to know that they are being observed and that every key stroke is recorded. Doing so sends a signal to the researchers and the public alike that any attempt to misuse data will set off early alarms and that safety measures are built in to preserve evidence of the actions taken by the researchers as they analyze the data.

For similar reasons of privacy protection, all results garnered from the research should be evaluated before submission for publication. The firm should only be able to “object” to public release if the research will necessarily leak private data or otherwise violate the law. Any objections must be made in writing and explanations sent to the appropriate body (e.g., the NSF) overseeing the research.

Finally, the researchers, themselves, must be under threat of criminal punishment if they misuse data and attempt to invade the privacy of individual users. This may seem extreme, but researchers need to understand how seriously they must consider user privacy in their research. Any replay of Cambridge Analytica needs to be met with the strongest sanction. The public also needs to know that malfeasance will lead to fine and imprisonment.

If these conditions are met by the platform, however, then they should be immune from liability for the release of data to the researchers. To be clear, this immunity would not extend to the lessons learned from the data itself. For example, if the researcher discovers or publishes information pointing

toward criminal or civil liability on the part of the platform, then such information could be used in a lawsuit or prosecution. The immunity for the platform should extend only to potential liability arising from the mere fact of releasing data to the researchers. In other words, they cannot be punished (under privacy laws or otherwise) for giving researchers data so long as the stringent privacy-protecting conditions are met.

### ***B. Compelled Data Access for Major Platforms***

Even if the law spells out a clear safe harbor for research, some platforms (perhaps even most) will still resist giving researchers access. As described above, even apart from potential legal liability, platforms worry about the PR or financial risk of what research might reveal. For data monopolies, though, such as Google and Facebook, this compelled access should be seen as a price they need to pay as the quasi-public utilities they have come to resemble.

Forcing any platform, big or small, to grant access to its data poses potential constitutional problems. The government could not, for example, require every website to reveal to government-approved researchers information about individuals who use its service. Indeed, doing so might not only raise privacy concerns but also First Amendment issues for both the platforms and their users.

For the largest platforms, though, this kind of law should be viewed as regulation designed to protect First Amendment rights, rather than threaten them. Because Facebook and Google exert unprecedented control over the speech marketplace, understanding what is happening on those platforms is critical to ensuring that users' speech rights are respected. This is not to say that the companies have the same responsibilities as the government. In fact, their First Amendment rights include the right to deplatform speakers and ban speech in ways that governments cannot. As with other corporate disclosure regulations in the public interest, however, requiring limited academic access to proprietary data should be viewed as a necessary step in preventing potential harms caused by the products themselves.

This kind of regulation could be seen as part of antitrust enforcement or as a condition for receiving the legal immunity platforms receive under Section 230 of the Communications Decency Act. In other words, for platforms that have achieved a status comparable to regulators of the public square, their scale comes with certain obligations, including allowing independent access to researchers who will gauge the effect of such platforms on democracy. If direct regulation is seen as legally precarious for one reason or another, then the large platforms could be given a choice. If they wish to enjoy the legal immunity for user-generated speech provided by CDA 230, then they must also agree to the academic access conditions detailed above. On the other hand, if protecting their data from outside analysis is sufficiently important to the firm, then they will be liable for the content on the platform. To be sure, such a “choice” raises questions of “unconstitutional conditions,” but that is a court fight worth fighting, especially with respect to the largest data monopolies.

### ***C. Immunity for qualified researchers who use publicly available data from the largest platforms***

In addition to compelling the largest platforms to make their data available for research and shielding other platforms from legal liability were they to voluntarily make data available under restrictive circumstances, the law should protect researchers who amass publicly available data from the largest platforms. “Web scraping” and similar methods have been used by researchers when authorized research pathways, such as APIs, have been shut down. Often, these methods violate platform terms of service and in an extreme case, could lead to criminal liability on the part of the researcher. Applicable law, including the Computer Fraud and Abuse Act (CFAA), should be amended to carve out immunity, at least for approved researchers on the major platforms.

A similar impulse underlies “[Aaron’s Law](#)” introduced by Representative Zoe Lofgren and Senator Ron Wyden. In a now famous and tragic episode, Aaron Swartz downloaded a large number of articles from the digital repository,

JSTOR. In doing so, he breached the applicable terms of service for the website. Swartz was later arrested and prosecuted under the CFAA, which could have led to a penalty of 35 years in prison and up to \$1 million in fines. However, he committed suicide before he was brought to trial. Aaron's Law would remove the threat of a felony prosecution for breaching terms of service in actions like this, if they do not cause significant economic or physical damage.

A similarly aggressive move occurred this summer when Facebook sought to shut down the NYU Ad Observatory. The project of NYU's engineering school scraped Facebook's political ad archive with a browser plug-in to perform research on political ads and to evaluate whether Facebook was following its declared disclosure policies. Facebook sent the researchers a warning letter threatening additional "enforcement action." It did so, it said, because these terms of service protect user privacy and comply with the terms of Facebook's consent decree with the FTC.

The rules against scraping and unauthorized accessing of available data derive from real concerns about hacking, cyber security, and privacy protection. For their products to function, for example, platforms may need to limit the numbers of queries per user or the degree to which users can download all the content on the service. By placing content on the web, companies are not consenting to hacking the entire back end of their systems by clever users or the reproduction of all of their content on someone else's server.

However well intentioned, the applicable laws should include a carve-out for legitimate research performed by university researchers. Congress should pass Aaron's law, but it should also do much more. It should make clear that researchers cannot be prosecuted for breaking the terms of service of the largest platforms—Facebook, Google and Twitter—in the course of their research. Any university researcher with a project that has been approved by the university's institutional review board should not be subject to any criminal or civil liability for scraping Facebook, Google or Twitter. The platforms could still shut down the accounts of the researchers who break the terms of service, but they cannot appeal to the courts or the U.S.

---

***Legitimate privacy concerns exist, for example, related to researchers (or any outsiders) gaining access to platform data. But policy should address those concerns directly, rather than assume that a zero-sum game exists between privacy and transparency.***

---

Attorneys to follow suit. Moreover, the platforms too, for reasons similar to those expressed above, should be immunized for actions taken by legitimate university researchers who scrape their sites in the course of their research.

## CONCLUSION

As with Section 31 of the new Digital Services Act proposed in Europe, the kinds of proposal presented here should be bundled together in a larger package of technology reforms, including privacy protection, competition rules, cybersecurity, and content moderation regulation. Researcher access to platform data undergirds all of these policies, however, as it results in the kind of knowledge production that will inform good tech regulation. If the other values are maximized, however, transparency by way of researcher data access may be unfortunate collateral damage. Legitimate privacy concerns exist, for example, related to researchers (or any outsiders) gaining access to platform data. But policy should address those concerns directly, rather than assume that a zero-sum game exists between privacy and transparency. A first step in doing so requires a recognition that the biggest platforms, particularly Facebook and Google, are qualitatively different types of monopolies than preexisting firms. If they are going to continue to enjoy unrivaled market power, they also must take on additional responsibilities. One of the most important responsibilities in that vein is the obligation to share their data with qualified researchers seeking to answer some of the most important questions as to the impact of new digital communications on society.

## ABOUT THE AUTHOR

**Nathaniel Persily** is the James B. McClatchy Professor of Law at Stanford Law School, with appointments in the departments of Political Science, Communication, and FSI. Prior to joining Stanford, Professor Persily taught at Columbia and the University of Pennsylvania Law School, and as a visiting professor at Harvard, NYU, Princeton, the University of Amsterdam, and the University of Melbourne. Professor Persily's scholarship and legal practice focus on American election law or what is sometimes called the "law of democracy," which addresses issues such as voting rights, political parties, campaign finance, redistricting, and election administration. He has served as a special master or court-appointed expert to craft congressional or legislative districting plans for Georgia, Maryland, Connecticut, New York, North Carolina, and Pennsylvania. He also served as the Senior Research Director for the Presidential Commission on Election Administration. In addition to dozens of articles (many of which have been cited by the Supreme Court) on the legal regulation of political parties, issues surrounding the census and redistricting process, voting rights, and campaign finance reform, Professor Persily is coauthor of the leading election law casebook, *The Law of Democracy* (Foundation Press, 5th ed., 2016), with Samuel Issacharoff, Pamela Karlan, and Richard Pildes. His current work, for which he has been honored as a Guggenheim Fellow, Andrew Carnegie Fellow, and a Fellow at the Center for Advanced Study in the Behavioral Sciences, examines the impact of changing technology on political communication, campaigns, and election administration. He is codirector of the Stanford [Cyber Policy Center](#), Stanford [Program on Democracy and the Internet](#), and [Social Science One](#), a project to make available to the world's research community privacy-protected Facebook data to study the impact of social media on democracy. He is also a member of the American Academy of Arts and Sciences, and a commissioner on the [Kofi Annan Commission on Elections and Democracy in the Digital Age](#). Along with Professor Charles Stewart III, he recently founded HealthyElections.Org (the Stanford-MIT Healthy Elections Project) which aims to support local election officials in taking the necessary steps during the COVID-19 pandemic to provide safe voting options for the 2020 election. He received a B.A. and M.A. in political science from Yale (1992); a J.D. from Stanford (1998) where he was President of the Stanford Law Review, and a Ph.D. in political science from U.C. Berkeley in 2002.



# DEMOCRACY FIRST: THE NEED FOR A TRANSATLANTIC AGENDA TO GOVERN TECHNOLOGY

STANFORD CYBER POLICY CENTER

Marietje Schaake



# DEMOCRACY FIRST: THE NEED FOR A TRANSATLANTIC AGENDA TO GOVERN TECHNOLOGY

*In “Democracy first: the need for a transatlantic agenda to govern technology” Marietje Schaake articulates the importance of renewed transatlantic cooperation in the governance of technology, which can serve as the backbone for a global democratic alliance in tech governance aiming to advance human dignity, individual and collective rights, economic fairness, security and democratic principles.*

---

With the Jan. 6 attack on the United States Capitol, the Biden Administration had its agenda carved out for it even before being sworn in. While it is necessary and urgent to focus on healing the wounds of division in the United States and to strengthen the integrity and resiliency of American democracy, too much of an inward focus would deny the shared challenges that are experienced not only within but also between democratic nations collectively. Of the many threats, ensuring technology companies do not disrupt the rule of law and are aligned with democratic principles is a priority that requires cooperation between like-minded countries. A joint effort between the United States and the European Union would create a combined force that will kickstart more democracy-focused coordination, in particular on technology governance.

The lively debate following Jan. 6, on the appropriateness of ad hoc responses by social media giants, but also on the proportionality of power that technology companies have amassed, should not overshadow how democratic governments themselves abdicated their responsibility. These governments should have done more to ensure technology companies would develop services and business models without disrupting democracy or the rule of law. This task far exceeds the immediate impact of incidents that are visible and controversial. Corporate power reaches deeply into digital infrastructure, currencies, identity, offensive and defensive capabilities in cyberspace, and other aspects directly touching the role of the state.

---

***The lively debate following Jan. 6, on the appropriateness of ad hoc responses by social media giants, but also on the proportionality of power that technology companies have amassed, should not overshadow how democratic governments themselves abdicated their responsibility.***

---

Even if in Europe more legislative initiatives have been taken, both the EU and the U.S. are behind in ensuring clear rules to safeguard the public interest. The United States' hands-off approach towards intervening in the business models of social media companies has now come back like a boomerang, with the attack on the Capitol as indisputable evidence that amplified disinformation fuels fascism. Online hate speech does not remain confined in some virtual, parallel universe, but leads to violence in the streets. For Americans, it has finally been revealed how a powerful technology sector becomes a weakness in equal force, if fairness, safety and rights are not protected with laws and regulations. This is a challenge that reaches beyond the governing of social media giants. Europeans look with hope and anticipation in the direction of Biden's Washington to develop a joint, democratic technology governance agenda. This is how the political and policy dynamics may play out.

## **JOINING FORCES ACROSS THE ATLANTIC**

Given the raw reality of the United States' loss of democratic credibility and standing after four years of President Trump with his anti-democratic agenda, the country needs partnerships and an explicit display of commitment to a democratic alliance. A democracy first agenda. Transatlantic cooperation can function as the backbone for such a global agenda while an inclusive, global alliance is necessary. When the economic and political power of the EU and

---

***After four years of President Trump and his anti-democratic agenda, the country needs partnerships and an explicit display of commitment to a democratic alliance.***

---

the U.S. are combined, an engine spanning 42 percent of the world's Gross Domestic Product (GDP), 60 percent of the world's Foreign Direct Investment (FDI) and a combined 800 million people of the world's population living in democracies is created. If the U.S. manages to reignite its legacy of supporting multilateralism, the transatlantic partners will be able to set the agendas of international organizations and fora such as the Organization for Economic Co-operation and Development, the World Trade Organization and the UN. Synchronizing regulatory efforts and building a critical mass should be the core ambition if they are to set democratic standards and policies together. In both the EU and the U.S. this will require a willingness to compromise in overcoming differences between the two blocks, in order to better address the most significant competition: that from authoritarian regimes or from privatized technology governance. A common technology policy agenda that advances human dignity, individual and collective rights, economic fairness, security and democratic principles has been neglected even as the geopolitical stakes have risen and China has emerged as an ambitious global player.

The global competition for economic power and the ability to set standards is now a battle between companies and countries. Major power benefits are gained for those who manage to come out in the dominant position: owning a market, as China does with the production of semi-conductors; setting global standards like Europe has done with the Global System for Mobile Communications and the General Data Protection Regulation; or outpacing others in the amounts of data harvested to build artificial intelligence as we see done by companies and countries alike. Governance models in the

---

***If the U.S. manages to reignite its legacy of supporting multilateralism, the transatlantic partners will be able to set the agendas of international organizations and fora such as the OECD, the WTO and the UN.***

---

digital world have become battlegrounds in a systems competition because technology is now a layer of all sectors in the economy and impacts almost all aspects of people's lives.

At present, the emphasis on specific aspects of governing in the digital world diverge between the U.S. and the EU. The United States is strong with its economic power coming from technology giants, and if it intervenes, this tends to be for national security purposes. The European Union, meanwhile, has sought to build on values it wishes to protect, with regulations that safeguard rights. Its growth of a digital economy is lagging behind, and despite ambitions of the European Commission to build a 'geopolitical Europe', meaning the EU should strengthen its role on the global stage. This remains too much of a paper reality, especially when it comes to the intersection of technology and geopolitics. Thus far, a political commitment to acting in an EU-U.S. tandem in the space of technology governance has not in fact manifested.

Eyebrows and question marks were raised for example, when the EU signed an investment deal with China in the month before Biden's inauguration. While it is perfectly legitimate for the EU to go after its own interests, the ability to act together vis-a-vis the most significant challengers of democracies and open markets was seen as a low hanging fruit to approach jointly.

A new transatlantic policy agenda on technology governance should at least include the buckets of trade, peace and security as well as democracy and human rights. In all areas existing rules should be updated or new rules

drawn up to ensure they cover the changing realities and new domains that emerge as a result of technological innovation. While negotiations on a Transatlantic Trade and Investment Partnership (TTIP) were met with resistance on both sides of the Atlantic, aligning trade and investment rules should help to create a level playing field and set agreed standards ranging from dataflows to the cybersecurity of services and the integrity of supply chains. Likewise, building on similar approaches to antitrust with aligned rules should ensure fairness in the digital economy.

Cybersecurity and trust in supply chains is a growing concern globally. The SolarWinds hack, which enabled the stealthy intrusion into U.S. government departments, NATO, the European Parliament and AstraZenica alike, has confronted political leaders with their dependence on technology companies without proper security guarantees once more. The combined market and political power of the U.S. and the EU will prove a powerful leverage to ensure shared standards apply to global suppliers. Accountability and attribution processes will similarly be more effective if they are coordinated. Additionally, determining how to translate laws of armed conflict and responsible behavior in peace time should lead to new accountability mechanisms after criminal acts or escalations into cyberwar.

A shared approach towards safeguarding electoral and democratic integrity should lead to a blueprint of how cyberattacks and disinformation can be stopped before they succeed in eroding trust in the foundations of the liberal democratic system. Agreed resiliency measures as well as protections of human rights and fundamental freedoms in the digital context should help to set democracies apart from authoritarian regimes while keeping abuse of power by corporations in check.

## WHERE POLICY MEETS POLITICS

Policy agendas never play out in a vacuum. Political positions already taken, as well as the legacy of existing policies, will have to be navigated. The EU has set the tone by elevating the digital agenda to the highest political level and making it part of the pandemic recovery spending along with a green

economy agenda. The U.S. should do the same. Too often, digital policies are left to industry leaders, or are treated as a second-tier priority on diplomatic and policy agendas. Addressing technology policy at the highest political level should lead to a whole-of-government approach to ensure that different entities that are part of the same government do not act in opposite directions.

The EU has been making headways in a number of governance areas. In particular, the role of large platforms is being scrutinized with regulatory initiatives seeking to spell out clear responsibilities in the fields of fair competition, free speech and content moderation, risk and liability, data protection and privacy, democratic integrity and digital taxation. Slowly but surely, American sentiment seems to be moving closer towards that of the EU, but just because the U.S. is moving in a similar direction, does not mean the choice to cooperate has been made. Implementation and enforcement continue to require improvements on both sides. Convergence can be spotted in the antitrust realm, where Google and Facebook, but also Amazon and Apple, have come under investigation for abuse of market power, mergers and acquisitions and illegitimate data use. In both the EU and the U.S. critics are looking for ways to address harms to the public interest and society stemming from monopolistic actors, beyond the necessary mitigation of harms to the market.

The EU, while relatively weak on homegrown digital giants, has declared the ambition to become digitally sovereign. With investments in research, advancing 5G, the combined use of industrial data as well as the creation of a European cloud, the EU hopes to rely less on imports and standards set by others. Still, European sovereignty is unrealistic and doomed to fail without allies, even if it makes for an attractive political rallying cry. To strive towards self-determination and the ability to advance common values and interests with allies makes more sense in a connected world that creates interdependence for everyone. The fact that the notion of ‘sovereignty’ is frequently invoked by authoritarian regimes to justify strong state interventions in the context of technology governance does not help the EU either.

The European commission president, Ursula von der Leyen, has extended a hand to the Biden Administration with a proposed EU-U.S. Agenda for Global Change including proposed cooperation through a Trade and Technology Council, a dialogue on the responsibility of Big Tech, protecting critical technologies and developing 5G and rules for data flows and artificial intelligence. The EU embraced Biden's proposal of a Summit for Democracy, and further hopes to cooperate on a long list of geopolitical challenges. With likeminded countries including Canada, Japan, Australia, the United Kingdom and hopefully India, shared technology governance questions such as surveillance, transparency and accountability of AI, algorithmic bias and use of facial recognition technologies might be addressed. Sanctions and other accountability mechanisms for the development and use of repressive technologies to silence dissent or hack and track human rights defenders should be aligned. The EU, U.S. and other powerful development donor states should tie investments in digital infrastructure, development programs, security assistance and a rights agenda in a way that offers a democratic answer to China's Belt and Road agenda. This should also help prevent developing countries from becoming launchpads of cyberattacks elsewhere.

For the EU to fully embrace its role at home or as a partner, there needs to be better coordination between different policy areas. Over and over again, the treatment of economic, geopolitical and security issues happen in isolation or even friction. To assess whether Huawei and other network technologies could safely enter the common European single market, 27 countries had to find a common, ad hoc 'toolbox' to assess national security concerns in coordination. The EU's potential will only fully come to fruition when economic, geopolitical and security aspects of governing technology are integrated into its existing values-based efforts. In technological systems, it is increasingly difficult to separate these multiple aspects, as they impact each other. In terms of governance, the question of which political model will prevail in setting rules for the digital world should be answered on the systems level. This integrated nature is one of the arguments to address several policy aspects at once. Additionally, such coordination may lead to a comprehensive transatlantic negotiation, whereas a topical approach would not. Negotiations on data protection have been politically challenging and the



European Court of Justice struck down the Privacy Shield in the Schrems II case. The decision struck down the existing adequacy decision, which implied that data protection standards in the U.S. were sufficient to allow for the frictionless exchange of data. Negotiations for a new arrangement continue and the Biden Administration is well advised to meet Europeans halfway on their data protection and privacy concerns just as the EU has moved in the United States' direction on the 5G debate.

President Biden has appointed a team with a legacy of respect for multilateralism, that can hopefully shepherd America's return to constructive collaboration with allies. He announced a Summit of Democracies with technology policy high on the agenda. The Biden administration will need allies in this effort. An alliance for democratic technology governance offers a solid starting point. Taxation of technology companies would be an area where Americans need to show a willingness to address EU concerns. It may not be long before Americans, while needing to address the fallout from the Covid-19 pandemic, also look to their main profiteers to contribute their fair share. The pandemic has laid bare the backlog in safeguarding the public interest vis-a-vis that of technology firms. While the latter have become wealthier and more powerful than ever before, unprecedented pressure on public health, public education and unemployment benefits will lead to public spending of historic proportions.

As the United States resurfaces from a tense campaign year, and arguably one of the most divisive phases in the history of transatlantic relations, the European Union has been presenting a jigsaw of technology policy proposals. It seeks to address the abuse of market power, democratic resiliency, cybersecurity as well as governance of artificial intelligence. On both sides of the Atlantic, growing numbers of citizens are concerned about surveillance capitalism as well as the rise of technology-powered authoritarianism. A lot is at stake, and a failure to cooperate more effectively along democratic lines will undoubtedly result in the further privatization of the governance of technologies, while handing authoritarian regimes additional space to instrumentalize technologies for their control driven political agendas. Digital ecosystems therefore need principled and systematic governance approaches



to have the desired effect of protecting the rule of law and democracy, even as new iterations and innovations are expected to emerge. The U.S. and the EU can create a critical mass together to do so at scale.

It is tempting for the Biden Administration to focus all attention on addressing the urgent erosion of democracy at home. However, joining forces with the EU to build a transatlantic technology governance alliance would support that cause. Addressing both domestic harms and the geopolitical aspects of technology's disruption supports a democracy first agenda.

#### ABOUT THE AUTHOR

**Marietje Schaake** is the international policy director at Stanford University's Cyber Policy Center and international policy fellow at Stanford's Institute for Human-Centered Artificial Intelligence. She was named President of the Cyber Peace Institute.

Between 2009 and 2019, Marietje served as a Member of European Parliament for the Dutch liberal democratic party where she focused on trade, foreign affairs and technology policies. Marietje is affiliated with a number of non-profits including the European Council on Foreign Relations and the Observer Research Foundation in India and writes a monthly column for the *Financial Times* and a bi-monthly column for the Dutch *NRC* newspaper. She can be found on Twitter @MarietjeSchaake.

# HOW THE BIDEN-HARRIS ADMINISTRATION CAN (BEGIN TO) SAVE THE INTERNET

STANFORD CYBER POLICY CENTER

Gaurav Laroia, Matt Wood

*Free Press*

# HOW THE BIDEN-HARRIS ADMINISTRATION CAN (BEGIN TO) SAVE THE INTERNET

*To fix our information ecosystem the Biden Administration must simultaneously work to bridge the digital divide, address algorithmic discrimination, be honest about Section 230 and the First Amendment, and build non-commercial media to combat misinformation.*

---

**T**he [cynical machinations](#) surrounding Congress's last COVID relief bill showcase the dismal state of tech policy at the end of the Trump era. Activists and advocates worked for nine months to get funding for broadband affordability in the law, winning a \$3.2 billion allocation to support internet access for people affected by the pandemic and economic crisis. That's both a landmark achievement and an insufficient endpoint, as it is roughly enough to keep just five million households connected for a year in the absence of additional steps.

Meanwhile, a Republican-led Section 230 repeal made a surprise last-minute appearance as the wrench used to sink \$2,000 stimulus payments in that December relief bill. That law was the subject of Trump's incoherent wrath long before Twitter started [labeling his tweets](#) last spring, and will only continue to anger misguided GOP politicians now that so many platforms have [banned Trump](#) for stoking violence and insurrection.

The relative invisibility of broadband adoption and affordability as a policy issue, especially when compared to the near-endless, high-profile wrangling over the future of Section 230 and its purported role in alleged online "anti-conservative bias" shows just how badly the Trump administration and its fellow travelers lost the plot on tech policy.

The centrality of the internet to our lives was already a cliché before the pandemic. But the crisis has underlined the importance of getting these policies right. Turning the page on the Trump administration and preparing for the crises to come means moving past the tech utopianism that

---

***Successful reimagination of the status quo is possible and within reach. The internet and our information and media ecosystem must work in the public interest. Charting a better path forward stands on these four pillars: connecting people that aren't connected; centering civil rights and privacy in the data economy; having a clear-headed and honest conversation about Section 230, content moderation and intermediary liability; and encouraging and publicly supporting noncommercial sources of information.***

---

characterized much of the early internet but also putting aside the cynicism and defeatism that has emerged in recent years. “Just turn it off” can’t be the solution to any of tech policy’s major issues, especially when even mass user defections and advertiser boycotts have not and could not curb all the excesses and abuses of social media, the data economy, and disinformation.

Successful reimagination of the status quo is possible and within reach. The internet and our information and media ecosystem must work in the public interest. Charting a better path forward stands on these four pillars: connecting people that aren’t connected; centering civil rights and privacy in the data economy; having a clear-headed and honest conversation about Section 230, content moderation and intermediary liability; and encouraging and publicly supporting noncommercial sources of information.

Congress should be a willing and eager partner on these issues. But the close partisan divide in both chambers may mean an uphill climb on many of the nation’s most pressing issues. This document emphasizes executive action where possible, so the Biden administration can act immediately.

## **BROADBAND: TITLE II, ACCESS, AND AFFORDABILITY**

It has been more than three years now since Trump's Federal Communications Commission Chairman Ajit Pai abdicated the agency's regulatory oversight of broadband providers in the egregiously misnamed *Restoring Internet Freedom Order*. While commonly conceived of as the order that reversed the Obama FCC's 2015 Net Neutrality order, it also uprooted the same order's proper classification of broadband as a "telecommunications service" under Title II of the Communications Act, and that classification has always been about much more than Net Neutrality nondiscrimination rules alone.

Treating broadband as an essential service or a utility in common parlance, and as a telecom service and common carrier in more precise terms under Title II, is integral to promoting equitable, universal and affordable internet

---

***Treating broadband as an essential service or a utility in common parlance, and as a telecom service and common carrier in more precise terms under Title II, is integral to promoting equitable, universal and affordable internet access for everyone in the United States.***

---

access for everyone in the United States. It provides the FCC with the best and in some cases only authority the agency has to make broadband more ubiquitously available, reliable, reasonably priced and competitive. It would let the FCC prohibit broadband disconnections during the pandemic. It would allow the agency to protect public-safety communications from unreasonable internet service provider (ISP) practices, and to require the rapid restoration and improvement of communications infrastructure wiped out by increasingly severe disasters like the [hurricanes that devastated](#)

[Puerto Rico](#) and the wildfires in so many western states. And Title II supplies [the only good authority](#) the FCC has to support discounted broadband on a permanent basis with its Lifeline program.

Some ISP lobbyists, and the pundits and politicians that listen to them, are eager for the “reclassification wars” to end; but Title II just makes sense. It is only contentious in D.C. because a few powerful lobbies and lawmakers keep fighting against what [people across the political spectrum](#) overwhelmingly and obviously [want and need](#).

As [Free Press has written](#), Title II is the proper framework for broadband from both [a legal and engineering](#) standpoint. It comes with [none of the harms](#) to broadband investment and deployment that Pai and others so often and so falsely claimed. Its repeal did not result in the broadband investment, speeds, and coverage increase that [Pai claims](#), and in fact investment did nothing but decline on his watch. Sustained attacks by the industry to avoid proper oversight and scrutiny should not deter the Biden administration from doing the right thing.

The end of the Trump presidency leaves us with this sobering legacy, even as the outgoing administration and FCC leadership falsely claim to have made real progress in closing the digital divide: Nearly 80 million people, or almost a quarter of the U.S. population, lack an adequate home-broadband connection. Economic and [racial gaps](#) in broadband adoption persist. Only 48 percent of low-income households have a fixed broadband connection. Some 13 million Black people, 18 million Latinx people, and 13 million Indigenous people lack this type of adequate home connectivity.

The FCC’s failure here would be wrong under any circumstance. But the pandemic has made that failure even more visible, poignant and tangible. Universal, affordable and open internet connectivity is necessary for jobs, education, civic engagement, and staying connected to one another — especially during a time of social distancing.

To protect the internet and ensure a resilient, affordable, and accessible telecommunications infrastructure, the FCC must put broadband back under Title II of the Communications Act.

The Biden administration should:

1. Appoint FCC commissioners who support returning to a proper interpretation of Title II of the Communications Act, which provides the legal foundation for a wide range of FCC initiatives to increase broadband deployment, affordability, reliability, resiliency and competition, as well as the foundation for strong Net Neutrality protections.
2. Support legislative efforts to clarify, reaffirm or restate this proper legal classification for broadband, and the FCC jurisdiction and mandates that come with it. The Save the Internet Act has already passed the House of Representatives once in 2019, and was modeled on the Congressional Review Act vote in the Senate in 2018 to overturn the Pai repeal. That kind of legislation would fully restore Net Neutrality rules along with the necessary Title II legal foundation, but Congress could also take up this task in more straightforward ways not tied back to reversing the Pai repeal.
3. Oppose any legislation that would restore only a few of the “bright-line rules” in the Net Neutrality context without restoring other necessary protections against unreasonable ISP discrimination or reinstating the necessary authority for the FCC to achieve all of these other broadband equity and affordability goals.

When it comes to affordability, the incoming administration should do everything it can to improve adoption, especially by people of color, on tribal lands, and in low-income communities more generally. This means it must:

1. Nominate or elevate an FCC chair and/or new commissioner (joining Democrats Jessica Rosenworcel and Geoffrey Starks) who wholeheartedly supports the Lifeline program, which subsidizes critical communication services for low-income households. The new FCC leadership must stop the attacks on that program launched by the outgoing chairman and his Republican colleagues, and also must protect broadband affordability by ensuring that businesses contribute their fair share to the Universal Service Fund that pays for Lifeline and other initiatives.

2. Support legislation mandating FCC collection of data on the actual prices people pay for broadband, to provide a comprehensive picture of cost-based barriers to adoption and formulate policies to address them.
3. Explore more progressive ways to fund broadband support mechanisms, not only for people already eligible for Lifeline but those above the poverty line too, with a mix of direct congressional appropriations and tax-credits to reduce the prices that working families and others pay for broadband today. The ink is barely dry on the December stimulus package, and the FCC has just begun work to administer the \$3.2 billion emergency broadband benefit described at the outset of this article. But more economic recovery and pandemic relief spending is necessary, and both the new administration and new Congress should look to build upon the broadband affordability support in the December bill.
4. Encourage the FCC 's use of its authority under Title II to investigate and stop unjust and reasonable practices and penalties, and at least oversee the prices charged and fees imposed by internet service providers. This is the crux of the argument over Title II: While it is possible to debate the need and capacity of the FCC to actually set rates for broadband, the FCC must have oversight of the prices and fees imposed on internet users by monopoly and duopoly providers of this essential service.
5. Support FCC action, and new legislation if necessary, to allow for broadband wholesaling and then resale competition from providers that do not own their own networks. That kind of competition is present in the wireless market to some degree but has almost disappeared in the wired broadband market after two decades of bad FCC decisions.
6. Support legislation that removes barriers to municipal broadband projects, and other cooperative and competitive initiatives, while using federal broadband-deployment subsidies to support local decision-making on construction and maintenance of these kinds of networks.



## CIVIL RIGHTS AND PRIVACY

There is an urgent need to address the failings, damaging business models, and privacy and civil rights abuses of the data economy. The large tech companies, already wildly wealthy and integrated into our lives before the pandemic, have seen [their profits soar](#) in recent months as the online world supplanted so much of the brick-and-mortar world for jobs, [commerce](#), education and social interaction. The obvious vehicle for addressing these issues is comprehensive federal privacy legislation — which is perennially at a standstill in Congress, as the political parties and other stakeholders continue trying to hammer out a compromise. The Biden administration should support that legislative effort. But federal action on data collection and security, and on algorithmic discrimination, cannot wait forever for Congress to break that logjam.

How data is collected, shared and processed affects all economic opportunities and implicates the pandemic recovery. The way that data collection supports targeted propaganda has imperiled the right to vote, the peaceful transition of power, and perhaps the foundations of democracy. These companies have used data to enable and sometimes even participate in discrimination against people of color, women, members of the LGBTQIA+ community, religious minorities, people with disabilities, and other marginalized groups. Importantly, even when they are not expressly designed to do so, algorithms that profile users and target content to them can also facilitate age, racial, and sex discrimination in [employment](#), [housing](#), lending, commerce, and [voting](#).

[These violations are well documented.](#) And they can force the poor and most vulnerable into increasing levels and cycles of precarity, which like everything else have been exacerbated during the pandemic. People that have experienced acute economic hardship because of the pandemic, like losing a job or facing an eviction, are having those hardships logged into credit-reporting databases that will make it harder for them to avail themselves of economic growth when it returns.

Free Press and the Lawyers' Committee for Civil Rights Under Law [have written draft privacy legislation](#) with these problems in mind. Our model bill has strong civil rights provisions that fill in the gaps where existing civil rights laws sometimes do not reach, and that address the disparate impacts of this new kind of data and algorithmic based decision-making.

Members of Congress have taken up this same civil rights and privacy fight. At least half a dozen Democratic privacy bills have addressed civil rights issues, and leaders of key committees have committed to addressing privacy in a way that [strengthens consumer and civil rights](#) alike. These efforts should be supported by the Biden administration, and any privacy bill that comes across his desk ought to advance the cause of civil rights.

But the Biden administration should not wait for Congress to act. Civil rights laws already on the books remain woefully under-enforced with regards to algorithmic decision-making and data use. For instance, the Equal Employment Opportunity Commission (EEOC) has [yet to issue guidance](#) on how it intends to apply its authorities to regulate hiring algorithms and facial-recognition software (though it has made moves in that [direction this month](#)). The Department of Housing and Urban Development (HUD) promulgated a rule making it [nearly impossible to substantiate](#) a disparate-impact claim with regards to housing discrimination, in effect allowing landlords to hide behind algorithmic models that perpetuate segregation. Machine-learning bias in credit denial can have lasting impacts on a family's wealth that lasts generations, and the Equal Credit Opportunity Act (ECOA) is meant to [guard against that kind of discrimination](#). And so on. Some existing authorities, though limited, wielded artfully could still have material impacts on combating this kind of discrimination.

Dedicated and systematic attention from the new administration is a must. Executive-branch agencies need strong direction and leaders ready to tackle these problems, and they should not just be left to their own devices. Leadership across the Biden administration and government must be consistent and coherent, not just attempt to address these issues that fall under different agencies' jurisdictions in a scattershot way.

The Biden administration should show its commitment to these civil rights issues, and should:

1. Commit to tasking all of its agencies with any civil rights authorities and responsibilities to regulate data collection and algorithmic decision-making within their scope of authority and competence. This must be done in a coordinated fashion across the government.
2. Appoint a “czar” to coordinate agency action on privacy and algorithmic decision-making, or at minimum direct the Department of Justice to spearhead the effort.
3. Reorganize agencies to place civil rights at the top of their agendas. Every agency/commission that does not have an Office of Civil Rights reporting directly to its political leadership should create one. If the agency/commission already has an OCR but it does not report directly to the Secretary/Commissioners, it should reorganize to raise the profile of the OCR.
4. Direct or suggest that every agency or commission hire senior officials dedicated to technology policy within their Office of Civil Rights. These various Offices of Civil Rights should hire additional technology policy professionals and attorneys as appropriate given the scope of the agency or commission’s activities. A single official cannot be expected to handle the civil rights portfolio of an entire large agency or commission.

Nominate or elevate an Federal Trade Commission Chair who will breathe new life into the Commission’s “unfairness” authority to address algorithmic discrimination and injustice. Using this authority is an idea that current Democratic FTC Commissioners [Rebecca Kelly Slaughter](#) and [Rohit Chopra](#) have already endorsed. The Commission should use this authority to address civil rights and privacy harms and increase the scope of its oversight of practices beyond just policing companies’ adherence to their own (often poorly crafted and poorly enforced) privacy policies.

One drawback of a full-throated commitment by the administration to tackle privacy and data abuses through existing authorities is the potential to take the wind out of the sails of federal privacy legislation, which is already mired in wrangling over issues like preemption of state laws and enforcement. But this needn't be the case. The executive branch effort should complement, not conflict with the legislative effort, bootstrapping attempts to address all of these problems without waiting indefinitely for Congress.

A commitment by the Biden administration to seriously investigate and regulate the data economy, with the goal of ensuring that real-world biases and disparate impacts from superficially “neutral” inputs don't unfairly disadvantage vulnerable populations, would begin to rework the data economy. It would set the stage for a less exploitative system and flex regulatory muscles that will be needed once legislation is finally passed. Not only worrying about but also working against discriminatory outcomes in data collection and algorithmic decisions will necessarily begin to tame some of the most exploitative aspects of the internet economy. It will teach valuable lessons both to Congress, as it continues to craft privacy legislation, and to the federal government too in building the expertise and institutional power necessary to manage and counter the adverse effects of the data ecosystem.

## INTERMEDIARY LIABILITY AND SECTION 230

Newly notorious and widely misunderstood, [Section 230](#) has been thrust into the public's consciousness due to repeated attempts by the Trump administration (and its congressional allies) to twist the law, suggesting that its repeal is deserved to punish social media companies for fact-checking the president and for other sins both real and imagined. Repeated grandstanding and mischaracterizations of this law [by Senators Ted Cruz, Josh Hawley,](#) and other less seditious lawmakers, in congressional hearings with tech CEOs and other settings, has made the debate over Section 230 eclipse almost every other issue in tech policy. President-elect Biden also took a rather [un-nuanced view](#) of Section 230 a year ago on the campaign trail, but must take the opportunity to recenter the debate on the facts, the law, and the Constitution.

We [have written about](#) President Trump’s persistent, but incoherent, [cynical](#) and [unconstitutional attempts](#) to use Section 230 to subvert the First Amendment in pursuit of remedying the nonexistent “anti-conservative bias” of social media companies. Trump and Senator Mitch McConnell’s final actions on Section 230 at the close of 2020 tied its proposed repeal to passage of increased covid stimulus payments for people in need. Whether that was a confused but earnest attempt by Trump to accomplish both goals, or a poison pill in McConnell’s mind to further dampen prospects for \$2,000 checks, the move characterized the lack of rigor and seriousness they took toward the legitimate policy questions surrounding intermediary liability.

As long as prominent members of the House and Senate continue to create or at least to take advantage of the confusion over Section 230, and continue to mischaracterize the law themselves, technology policymaking in Congress will remain distracted and confused. And as long as the debate is confused, it will not move forward.

Free Press is unconvinced that any of the changes thus far proposed to Section 230 are both necessary and good — and many of them are [just outright harmful](#) — but we’re certainly listening and engaging in the conversation on good-faith proposals seeking a positive impact.

Any changes to Section 230 must retain a balance: keeping low barriers to people posting their own content, ideas, and expression on platforms, websites, apps and other online fora they don’t own; but also preserving the principle that interactive computer services are legally liable for their own bad acts, not for everything their users say and share in real time and at scale. It’s worth emphasizing that the [balance the law currently strikes](#), immunizing platforms for third-party speech but also immunizing platforms for their content-moderation decisions, is what has facilitated the swift and wide-ranging [deplatforming of insurrectionists](#) — and most recently [the President](#) who incited them — and all manner of [their enablers](#) on services across the internet, both before and especially in the wake of the deadly attack on Congress on January 6th.

---

***Yet even if interactive computer services were suddenly (in theory) liable for everything their users posted, many of those posts containing clearly awful racism, bigotry, homophobia, sexism and other ills, such as COVID disinformation and conspiracy theories, can't readily be addressed by changes to Section 230.***

---

Remember also that repealing Section 230 would lead to far more preemptive takedowns and refusals to host any user-generated content at all, if social media, online exchanges, and comments sections could even withstand such a drastic change. Yet even if interactive computer services were suddenly (in theory) liable for everything their users posted, many of those posts containing clearly awful racism, bigotry, homophobia, sexism and other ills, such as COVID disinformation and conspiracy theories, can't readily be addressed by changes to Section 230. The First Amendment generally protects that speech, and tort law doesn't readily provide for civil suits against it either. Repealing or otherwise gutting the statute wouldn't suddenly make speech unlawful or tortious for a platform to host if it weren't already unlawful or tortious for the original speaker in the first place.

The Biden administration has a responsibility to speak honestly about where it understands the scope and the limits of the First Amendment to be, and how within that context it sees the roles of websites and other intermediaries in hosting any such lawful but disfavored speech.

The Biden administration should:

1. Rescind and disavow the [Trump Section 230 executive order](#), and make it clear that the government cannot enforce a principle of “political neutrality” on private websites, not only because it's a bad and unworkable policy but also because of the limitations the First Amendment rightly places on the government in this context.

2. Rescind and revisit the [Department of Justice’s Section 230 recommendations](#). Provide an accounting of actual instances where the Department of Justice, the FTC, or other agencies have felt they couldn’t bring enforcement actions against internet platforms because of the provision. Include a civil rights review of the section and make it clear that the government believes Section 230 does not provide a shield for civil rights violations committed by or facilitated by the platforms themselves.
3. Don’t be skittish about bringing cases against the actual creators of unlawful content or against platforms that actively support illegal activity. Much of the ire Section 230 has drawn is misdirected anger at government inaction in the face of clear wrongdoing. Section 230’s co-author, former Rep. Chris Cox, [recently wrote that](#) the provision is premised on the idea “of imposing liability on criminals and tort-feasors for their own wrongful conduct.” This is still true. The underenforcement of civil and criminal law is not reason to reject the shield.
3. Encourage more transparency, as campaigns like [Change the Terms](#) (where Free Press is a founding member) and others have called for, in terms of how content moderation actually happens on large social media platforms. The Europeans are moving to compel this kind of transparency. The new administration here can encourage the FTC to use its 6(b) authority or other routes to get a full accounting of social media content-moderation practices.

We need to turn the page on the prevailing but unhelpful discussion of Section 230 in too many public and congressional debates, where its reform or repeal are posited wrongly as simple and obviously beneficial steps. This single statute is crucial, but contrary to popular misperception it is not an all-encompassing liability shield for all harmful content online. It’s also not a special benefit to large social media and Silicon Valley giants, but is instead a protection for every online service that allows any user interaction. And its



removal would not allow lawmakers, regulators or enforcers to skirt the First Amendment or hold platforms liable for speech to which no legal liability attaches now.

The Biden administration should make it clear that platforms are indeed already liable for their own conduct, products, or speech. They should expand on and clarify precedents set in the 9th Circuit ([Malwarebytes](#) and [Roommates](#)) and the 3rd Circuit ([Oberdorf](#)), ruling that the shield is in fact limited. The government should not be afraid to bring more enforcement actions like the HUD Facebook settlement.

There are persistent harms caused by things like harassment, revenge porn, child sexual abuse material, and increasingly visible insurrectionist and white-supremacist violence organized online. The administration should be clear that [enhancing existing laws and enforcement capabilities](#) against such heinous conduct — rather than wholesale rejection of Section 230 — can best provide relief.

There have been [suggestions](#) too that the Biden administration should support Senator Brian Schatz and Senator John Thune’s [PACT Act](#) that seeks to codify the principles of “distributor liability” rather than publisher liability for platforms. Free Press agrees that kind of approach would properly keep the focus on the original content creators’ harmful and criminal conduct, yet could clarify interactive computer services’ obligations to take down content already adjudged to violate the law rather than purporting to make services pre-screen everything users post. Of course, the notice and enforcement provisions for any such distributor liability scheme matter greatly, even if the idea is sound in principle.

But the invocation of Section 230 as a boon to big tech alone, and one that must be taken away to somehow punish the largest platforms, is not helpful and will not lead to good results. The Biden administration having an honest accounting of Section 230, the First Amendment, and where it believes it can push on aggressive litigation to punish platforms’ own bad conduct, would help immensely.



## SAVING JOURNALISM

The misinformation crisis, along with the low trust Americans have in institutions, each other, and politics in general, can't be untangled from the crisis in journalism. Producing high-quality information has to be part of the tech-policy conversation. Yet no amount of new privacy laws, antitrust actions, or other suits against the largest platforms will be enough to bring America back together if we keep swimming in a pit of lies. These falsehoods take root not only on the largest and most popular platforms, but on all manner of websites and various broadcast and [cable channels](#) too. The inability to access high quality local information doesn't just affect low-information voters. The collapse of local news is having a material affect on our democracy. Commercial media sources, both online and traditional, have failed to provide local communities with the news they need. We don't believe government should ever influence news content and coverage, but it must do more to fund public-interest journalism.

In 2019, Free Press published [“Beyond Fixing Facebook,”](#) which included a legislative plan to fund local news media through a tax on targeted internet advertising. In 2020, we followed up with [comprehensive plans](#) to put [journalism funding into pandemic relief bills](#). That should be a priority because truly local news outlets were among the businesses hurt by the massive economic disruptions; but also because the only way to build back better from the pandemic is to [acknowledge and repair](#) the media's historical and present role in propping up systemic racism, economic injustices, and the toxic mixture of purposeful disinformation and negligence in newsrooms that worsened the disproportionate impacts of the pandemic on Black and brown people.

The Biden administration can take concrete actions to save journalism and protect our media system from further consolidation:

1. Support legislation to tax the targeted advertising revenue of large online platforms and redirect those funds to public, independent and noncommercial journalism.

2. Provide money for journalists' jobs and for news outlets already struggling before the pandemic hit. Such funding was proposed but not passed in the initial COVID relief bills last spring. In the more recent December stimulus bill, broadcasters got expanded eligibility for paycheck protection plans, but we fear this aid could flow to local affiliates of [giant media conglomerates](#) too easily. Free Press has called for billions to be put more directly into truly local commercial newsrooms and noncommercial outlets alike.
3. Reverse years of runaway broadcast media consolidation by appointing FCC commissioners who will focus on increasing ownership diversity, abandoning the Trump FCC's efforts to eliminate ownership limits and ignore diversity altogether (as argued in the Supreme Court just in January by Free Press and allies).  
Support legislation that carves out a designated path for journalism outlets to apply for 501(c)3 nonprofit status.
4. Endorse state-level initiatives to fund local-news media, especially in so-called "news deserts" where there are no traditional local-news outlets; and efforts like Free Press's [News Voices](#) initiative to promote accountability and dialogue between journalists and the people they cover — centering racial justice, and elevating the voices of communities the media have misrepresented or maligned.
5. Defend the Corporation for Public Broadcasting against congressional efforts to "zero out" its funding, while expanding the concept of public and noncommercial media worthy of support to more than just existing public TV and radio stations, with a new emphasis on supporting local journalism and newsgathering.

## CONCLUSION

As the ongoing efforts to overturn the results of the November election show, the end of the Trump administration is a welcome and essential change but [not a full reprieve](#) from the underlying social, technological and economic forces that brought Trump to power in the first place. If we do not work aggressively to mend the inequities and failings of the technology and media system we will continue to imperil the ability of Americans to discern truth from lies, information from propaganda, and community from divisiveness.

We hope the Biden administration takes a clear-eyed view of the possibilities in Congress, and pushes for new laws there, but also commits to aggressive executive action where possible. The future of our country and our communities depend on it.

### ABOUT THE AUTHORS

#### **Gaurav Laroia**

Senior Policy Counsel, Free Press

Twitter: @GauravLaroia

Gaurav works alongside the Free Press policy team on topics ranging from internet-freedom issues like Net Neutrality and media ownership to consumer privacy and government surveillance.

#### **Matt Wood**

Vice President of Policy and General Counsel, Free Press

Twitter: @MattfWood

Matt leads the Free Press policy and legal team's efforts to protect the open internet, prevent media concentration, promote affordable broadband deployment and safeguard press freedom.

# THE NEXT CYBER STRATEGY: PLAYING A BETTER GAME OF WHACK-A-MOLE

STANFORD CYBER POLICY CENTER

Jacquelyn Schneider, PhD

*Hoover Fellow, Stanford University*

# THE NEXT CYBER STRATEGY: PLAYING A BETTER GAME OF WHACK-A-MOLE

*The article looks at lessons from both the Obama and Trump administrations to recommend strategic priorities of open, free, secure internet that safeguards genuine information by focusing on resilience first, bolstered by strategic deterrence, and complemented by ongoing investments in defense, intelligence, and information sharing while conducting counter-cyber operations.*

---

In 2011, the Obama Administration penned their first cyber strategy. The International Cyber Strategy called for an internet that promoted “prosperity, security, and openness” by upholding principles of “free speech and association, privacy, and the freedom of information.” The strategy leaned heavily on norms, diplomacy, and then dissuasion and deterrence in order to achieve these goals. It has been a decade since this initial strategy and the threats to these strategic principles have been perhaps more diverse and prolific than the strategy had imagined. Over this decade, and two administrations, the US has evolved and experimented its strategic efforts to respond to these threats. Now, as the US moves into a new administration, are we still focused on these same strategic principles? And what have we learned about what works and what doesn’t in cyber strategy?

This article briefly introduces the trajectory of US cyber strategy over the last decade, identifying big changes (both in threat landscape and strategic effort) along the way. In looking back, it identifies a path for the future. Finally, it concludes with pragmatic suggestions for implementing and then evaluating the effectiveness of the cyber strategy.

## A BRIEF TRIP THROUGH THE CYBER PAST

The Obama Administration made the first real forays into US cyber strategy, setting the foundation of US strategic interests and embarking on the first attempts to corral the US government to support those interests.

Throughout these eight years, the Obama Administration made openness and reliability a priority for cyberspace. This belied an assumption made by the administration that freedom of information was both good for the international community and the United States' economic and foreign policy interests. This stood in contrast to other countries like China or Russia that pushed back on openness, instead advocating for more balkanization and domestic sovereignty over cyberspace, ultimately restricting flows of information for domestic control. And while China and Russia represented the far end of this debate, at the same time Europe was experimenting with a hybrid model that focused more on digital sovereignty and regulation.

Perhaps the largest threat to the Obama Administration's strategic priority wasn't the international contest of openness versus balkanization, but instead the proliferation of threats to the capabilities and dependencies that came with the modern digital society. Over this time period, not only did non-state cyber-crime become more capable and ubiquitous, but states started to target cyber vulnerabilities for espionage, coercion, and conflict. From the North Korean-lead cyber-attack on Sony, Russian cyber-attacks within military conflicts in Georgia and Ukraine, Chinese mass exfiltration of data from the Office of Personnel Management and widespread intellectual property theft. Finally, on the tail end of the administration, foreign-led disinformation campaigns with hack and reveal strategies weaponized the free flow of information within US society, turning what had been a strategic strength of the US into a domestic vulnerability.

The Obama Administration's response to these cyber threats was to focus on norms and domestic information coordination and response while relying on the threat of sanctions and department of justice indictments to deter state-sponsored activity. US offensive cyber capabilities resident with the Department of Defense were closely held and restrained at the highest levels, used only sparingly within existing military campaigns (like the fight against ISIS). The Obama Administration spent much of their time creating the foundations of inter-agency coordination, determining the appropriate roles and responsibilities of federal agencies—a daunting task which was codified within an infamous PowerPoint bubble chart that put the Department of

Homeland Security and Federal Bureau of Investigation in charge of most of the existing cyber threats and leaned on the State Department to create and propagate norms that supported US strategic priorities. The Department of Defense was largely a supporting agency in this construct, building capabilities to deploy in conventional conflict and struggling to create credible deterrence options to dissuade states from conducting a wide array of cyber activities, from espionage to attacks against nuclear infrastructure.

This was a period of learning and building, in which the administration focused on creating a unified federal approach to cyberspace. Their work creating lanes of effort within the federal government created a strong foundation for the incoming administration. Further, the administration clearly articulated normative principles and worked hard to propagate these norms within the United Nations and in relationships with allies. Where it was most successful was when it could focus these normative discussions on concrete actions, for instance creating task forces that focused on Chinese intellectual property theft or packaging norms about attacks on civilian infrastructure with executive orders on sanctions.

Despite these successes, this was also a period of relative restraint in US responses to cyber threats, and, coming into the Trump administration, state sponsored cyber activity was in no way slowing down. There was a push from within both the private sector and the Department of Defense for a more active and forward leaning strategy to combat these proliferating cyber threats—a push which found a willing audience in the Trump Administration.

In 2018, the US rewrote all of its [cyber strategies](#) and moved from a diplomacy deterrence-first, “be prepared” stance under the Obama Administration to a forward-leaning, risk acceptant, and active strategy under Trump. In particular, the 2018 summary of the [Department of Defense’s Cyber Strategy](#) introduced the concept of “defend forward,” confronting adversaries before cyber-attacks even occur “to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict.” In general, the Trump Administration’s approach was highly decentralized, giving much more autonomy and newfound responsibilities to the Department of Defense and Cyber Command (which was now a unified command).

This autonomy, combined with very operationally focused leaders like new commander, General Nakasone, led to large scale experimentation in Department of Defense cyber operations. Meanwhile, the Department of Homeland Security leaned forward under new leadership in its Cyber and Infrastructure Security Agency, ushering in a much more publicly responsive face to cybersecurity and new partnerships with both the private sector and the department of defense. Cyber Command and the Cyber and Infrastructure Security Agency began to release information about malware and threats broadly and created new operational structures centered around issue-specific task forces (for instance election security) that appeared to be relatively successful. Meanwhile, Cyber Command used its new authorities to develop new missions like “hunt forward,” which sent US cyber troops into allied and partner networks to search for adversary activity and to grow the new Cyber Mission Force (in both mandate and personnel).

Despite these tactical and operational innovations, the Trump Administration struggled to translate innovation to strategic success. A revolving door of personnel within the National Security Council, White House strategies disconnected with agency or command visions, and conflicting foreign policy priorities within the White House itself stymied cyber progress. Further, unclear language within Department of Defense strategies and Cyber Command Vision, led onlookers to question what the defense cyber was really doing. While [public statements](#) and [DOD-sponsored articles](#) painted a picture of defend forward that included cyber defense teams in allied states or intelligence sharing with private sector, unofficial [reports by the New York Times](#) suggested US was placing malware exploits in Russian critical infrastructure. This led onlookers to question how far forward exactly the US was defending. Faced with this ambiguity, some critics worried the US’ new strategic concept could inadvertently lead to retaliation, potentially violent. Further, even those who supported defend forward, voiced concern that these operations could become never ending task forces, expensive to sustain, and difficult to tell whether they were more or less effective.



## BUILDING THE NEXT CYBER STRATEGY: GOALS

Moving into the new Biden Administration, where does that lead us? The recent SolarWinds hack suggests that the US is still playing whack-a-mole in cyberspace, but after heavy foundational lifting by the Obama Administration and four years of relative neglect but operational innovation from the Trump Administration, the US is playing a much better game. When the Biden Administration rewrites the next cyber strategy (optimally published before any new agency strategies), it should not return to Obama 2.0, nor should it continue on the disorientated path created by the Trump Administration.

---

***While the US may often compete with rising powers within cyberspace, the goal is not to just “win” at competition, but instead influence behaviors across the international community so that the US can create an international order that supports democracy, prosperity, and peace.***

---

Instead, it should draw on the strengths of both: looking to the strategic priorities articulated within Obama strategies while generating new lines of effort from the operational learning done under the Trump Administration.

Building a new cyberspace strategy begins with outlining strategic priorities. Here is where the Obama Administrations’ original focus on an open, free, and secure internet is still incredibly valuable. These characteristics remain noble goals for the US and, if achieved, will support a larger Biden foreign policy strategy that returns to the democratic principles which make the US different from authoritarian states like Russia or China. While the US may often compete with rising powers within cyberspace, the goal is not to just “win” at competition, but instead influence behaviors across the international

community so that the US can create an international order that supports democracy, prosperity, and peace.

The new cyberspace strategy, however, will have to have even loftier goals than the Obama Administration. That is because the US has learned about the danger not only in not having access to information, but also in accessing invalid information—whether that be campaigns of disinformation or the manipulation of data to degrade trust in our economic or governance systems. Therefore, the new US cyber strategy will have to seek not only an open, free, and secure internet but will also have to safeguard genuine or valid information. This is a key addition to strategic priorities because if the Biden Administration’s strategic focus is on restoring economic prosperity and democracy at home, then having a cyberspace that can be relied on for valid or genuine information will be key. How can the US achieve these strategic goals, especially given the proliferation of threats to data and cyberspace?

## **BUILDING THE NEXT CYBER STRATEGY: LINES OF EFFORT**

The primary line of effort for the Biden cyberspace strategy—around which all other lines of effort bolster—should be resilience, or as Dr. Erica Borghard explains, “the ability to anticipate and withstand a disruptive event, and to rapidly restore core functions and services in its wake, whether it be a pandemic, financial crisis, terrorist attack, or large-scale cyber incident.” Resilience requires not only investing in federal networks and technologies that are more technically resilient, but also in building data users that are more resilient. For the largest US government data user, the Department of Defense, this involves building networks that gracefully degrade and campaigns that can be executed with limited access to data. At the core for any data user, whether it is a military officer, a federal civilian, or an American citizen is building human resilience—educating data users to question their data’s biases, to look at data sources, and to have a back-up plan in place when they don’t have access to digital resources.

Tied intimately to resilience are three activities: defense, intelligence, and information sharing. Cyber defense includes adopting commercial cybersecurity best practices for the federal government and defense information network but will also require new focus on cybersecurity when acquiring these capabilities. These defense efforts are aided by investments in technical intelligence talent and information sharing across the private sector and federal agencies. All three of these activities benefit from investments in commercial cybersecurity technology, as well as federal investment in research and development in cybersecurity. Further, the Biden administration should continue to build out the interagency and public-

---

***The US needs to resolve a current contradiction in the strategy between a nation that nominally propagates norms to not attack civilian critical infrastructure and yet does not define the limits of its own cyber actions taken under the Department of Defense's defend forward strategy.***

---

private information sharing that matured over the Trump Administration. In particular, creating ways to quickly share threat information across economic sectors and within the existing agency partnerships will reap large rewards.

During the Obama Administration, norms and deterrence played a central role in cyberspace strategy. However, they were largely punted during the Trump Administration in favor of new concepts like “defend forward” and “persistent engagement.” But these concepts are not replacements for each other and can and should co-exist. The difficulty is two-fold. First, the US needs to define what it cares about so that it can have credible cross-domain threats of punishment to deter the worst type of cyber-attacks: those that

create violence to US citizens or threaten the US nuclear arsenal. Secondly, the US needs to resolve a current contradiction in the strategy between a nation that nominally propagates norms to not attack civilian critical infrastructure and yet does not define the limits of its own cyber actions taken under the Department of Defense’s defend forward strategy.

How can the Biden Administration shore up strategic deterrence and maintain stability while being more actively engaged in countering cyber operations? The good news is that key parts of the Department of Defense’s 2018 strategy, and in particular the assumptions behind defend forward, are supported by scholarly research. The increase in cyber-attacks pre and post-COVID, as well as [scholarly analysis of cyber deterrence](#), suggest that ambiguous threats of deterrence are not enough to significantly curtail most cyber-attacks. In addition, [wargames with private sector representatives](#) provide evidence of strong support within American businesses for a more forward leaning cyber strategy to counter adversary cyber-attack. Finally, [experimental research](#) largely supports the strategy’s assumption that cyber operations rarely lead to violent retaliation.

That’s the good news for the 2018 Department of Defense cyber strategy. The US can use “defend forward” to counter adversary’s cyber-attack capabilities and decrease cyber-attacks. The bad news is that if the US defend forward strategy is going to successfully degrade bad guy cyber capability and preserve strategic stability, it still has to rectify the hypocrisy problem lurking in the US’ overly ambiguous strategy.

Here the Biden Administration has a real opportunity—not only to ensure the success of its own strategy, but also to build norms of appropriate behavior in cyberspace. To do this a new strategy first needs to announce to adversaries and allies what is off limits, and subsequently deter these strategic cyber-attacks by threatening credible retaliation options. We’ve come close to this before. The Obama Administration crafted an [Executive Order on sanctions](#) in response to cyber-attacks on critical infrastructure and Trump’s State Department has called out cyber-attacks on health infrastructure as inappropriate behavior in cyberspace. However, the US has always stopped

short of binding its own hands or credibly threatening anything beyond sanctions or tit for tat cyber punishment for these cyber-attacks.

This is partially because the US has been too expansive in what it has deemed as “off limit” cyber targets for adversaries. The Obama Administration’s definition of critical infrastructure spanned 14-16 sectors and both Administrations have struggled to define what kinds of cyber operations against these infrastructures they seek to deter. If everything is important, then nothing is important. Absent an understanding of what the US cares about in cyberspace, ambiguous cyber deterrence by punishment policies have been unable to stem the increasingly prolific and sophisticated wave of cyber operations against US civilian enterprises.

The first step, therefore, in solving the US cyber strategy problem is to decrease strategic ambiguity about what cyber-attacks are serious enough to warrant a violent response from the US. To date, the US has not resorted to violence in response to cyber-attacks, even though the US has threatened up to nuclear response to cyber-attacks. Instead of these ambiguous threats, the US needs to focus strategic deterrence on the cyber-attacks which are the most likely to have credible deterrence options. This is a high bar. Most cyber-attacks will not be able to be credibly deterred, but the US may be able to credibly threaten cross-domain punishment for truly strategic cyber-attacks: those that create violent effects against civilian populations or threaten a state’s nuclear control. At this high strategic level, which is only reserved for the most dangerous cyber operations, the US can credibly threaten its vast and lethal military force and therefore shore up deterrence.

But defining and deterring what the US cares about at the strategic level is only the first necessary step to solving the US cyber strategy problem. The US must not just assert these targets off limits for US adversaries, but also declare them off limits for the US. The adoption of a [no-first-use cyber strategic attack policy](#), especially one buttressed by credible threats of retaliation across military options, can help signal credible US restraint and scope appropriate “status quo” cyber activity, thus shoring up both a strategic threshold of restraint and a lower threshold of status quo cyber

activity that occurs without violent retaliation. Both of these thresholds are essential for the current US cyber strategy to succeed. And while a no first use policy was never adopted in the nuclear world, there are important differences in cyberspace that make no first use more credible and more advantageous than in the nuclear domain.

While the adoption of a no first use strategic cyber-attack policy will help shore up strategic restraint, the US will have to go beyond no first use in order to ensure strategic success. It must also pair a strategic no first use policy with clearer statements about what types of activities fall under defend forward—thus making both ends of the cyber spectrum less ambiguous and more defined. Ideally, defend forward is a concept scoped to include only counter-cyber operations against cyber adversaries and not to target adversary civilian infrastructure. While defend forward may include up to offensive cyber activity, a clearer articulation of the focus of defend forward activities should help assure adversaries (and allies) that the US will restrain these attacks and not target civilian infrastructure preemptively. This may help to solve the US strategy's hypocrisy problem and correct the logical inconsistencies of an otherwise ambiguous defend forward.

All of these actions support norms that the strategy should propagate about what are responsible actions in cyberspace—what is off limits (for us and our adversaries) and where does the US need to invest in resiliency, defense, and punishment to make cyber exploits less likely to succeed. Diplomacy should focus on what might be largely popular across both allies and adversary nations, for example agreements (binding or non-binding) to restrain state-sponsored attacks against critical infrastructure. Meanwhile, the State Department could pursue bilateral or hub and spoke agreements that graft off of existing arrangements—for example negotiating agreements to restrain cyber network exploitation or attacks against nuclear arsenals by grafting off existing nuclear arms control agreements. While norms are not a line of effort in the strategy, they are the result all the other lines of effort seek to achieve. They are most likely to succeed when all lines of effort converge and so future diplomatic efforts should include military to military discussions as well as coordinated signaling strategies.

Finally, the Biden Administration will have to carve out of an already tight budget investments in crisis response, cyber support to conventional campaigns, and law enforcement. All of these lines of effort require more cybersecurity talent as well as federal funding for technology and coordination between local governments and federal agencies. The Biden Administration should not be afraid of creative approaches to talent in the federal workforce, including a better use of the military reserves, the development of a civilian reserve corps, and more government fellowships for both academic and industry leaders to contribute to the federal workforce, even for a short time.

These efforts also require a closer look at whether our current planning and organizational structures are optimized for the threat. For example, the development of task forces within Cyber Command and other federal agencies was an important innovation that replaced a rigid military campaign planning structure that never worked for cyber. But how does the US organize task forces for non-time-delineated tasks like dealing with China? Further, these never-ending task forces are expensive and manpower intensive. How do we know how these task forces should be manned and what is working (or not working)?

## FINAL THOUGHTS

Over the last few decades, the US has doubled down on digital technologies, using these digital resources to forge a dominant military, an advanced digital economy, and a highly connected society. But these technologies have also come under threat and the operational cyber innovations made over the last four years at places like the Department of Homeland Security's Cyber and Infrastructure Support Agency or the Department of Defense's U.S. Cyber Command will not be enough to forge strategic success. The incoming Biden Administration should return to the principles and strategic focus of the Obama Administration, but also build on the tactical and operational successes the Trump Administration may have unwittingly created by largely ignoring the cyber efforts at defense or homeland security.



---

***An open and free internet is still important to democracy and a vibrant economy, but the incoming administration will have to do more to safeguard valid information in order to salvage the role of the internet in our society.***

---

Finally, it is important to highlight that the greatest instability created by data has not been in warfare but instead in the ways in which our digital dependencies can be manipulated to further schism already existing divides within our societies. The Biden Administration will have to take on the very difficult task of regulating information without suppressing freedom of speech. An open and free internet is still important to democracy and a vibrant economy, but the incoming administration will have to do more to safeguard valid information in order to salvage the role of the internet in our society. As with all things cyber, the answer is not in the technology, but instead in humans and building resiliency and trust in the data that undergirds our democracy, our society, and our economy. It will be a tall order, but the US is better postured for that challenge today than it has been in the previous decade.

#### ABOUT THE AUTHORS

**Jacquelyn Schneider** is a Hoover Fellow at the Hoover Institution. Her research focuses on the intersection of technology, national security, and political psychology with a special interest in cybersecurity, unmanned technologies, and Northeast Asia. She is a non-resident fellow at the Naval War College's Cyber and Innovation Policy Institute and a senior policy advisor to the Cyberspace Solarium Commission.



# TOP TECHNOLOGY POLICY PRIORITIES FOR THE NEW ADMINISTRATION

STANFORD CYBER POLICY CENTER

Eileen Donahoe

# TOP TECHNOLOGY POLICY PRIORITIES FOR THE NEW ADMINISTRATION

*Eileen Donahoe of the Cyber Policy Center's Global Digital Policy Incubator argues that the U.S. must rally the world around a democratic, human rights-based vision of digital society, and she recommends a range of early concrete actions that can be taken by the new administration to combat the competing digital authoritarianism model.*

---

**T**he incoming Biden-Harris administration will face many urgent and competing priorities as it seeks to signal a distinct shift from the Trump presidency. In the technology policy realm alone, there are many challenges to confront. Chief among them is the urgent need to solidify international support for a values-based vision of “the internet” and a compelling democratic approach to governance of digital society.

Solidifying an open democratic vision of digital society will require robust diplomacy in three areas. First, we must rebuild global commitment to an open, interoperable, secure and reliable internet and to international norms in the cyber realm. Second, we must lead the development of a shared understanding of what democratic, human rights-based governance of digital society entails. Third, we must bring our democratic allies together around a shared strategic technology agenda.

As context for these efforts, we must start by acknowledging that the original U.S. vision of a global, open, interoperable, internet has been clouded by two big trends: first, heightened anxiety within democracies about the myriad risks associated with connectivity and digitization, and second, perhaps more importantly, competition from a much darker vision of digital authoritarianism.

The digital transformation of society has brought profound change to every aspect of connected society and dramatically altered the context for democratic governance. “The internet” has become the infrastructure

---

***The digital transformation of society has brought profound change to every aspect of connected society and dramatically altered the context for democratic governance.***

---

of society, moving well beyond its early core function of facilitating instantaneously global communication. The wide array of advanced technologies that are now intertwined with all sectors of society has created new vulnerabilities for many aspects of public and private life.

While digitization obviously has yielded substantial benefits, democratic governments are struggling to meet their basic obligations to protect the liberty and security of citizens in this radically changed context. Digitization has created security risks for personal data, confidential communications, and connected infrastructure. Democratic governments are now seized with the fact that digital information platforms have been exploited by malign actors to spread propaganda and disinformation, wreaking havoc on democratic elections and eroding trust in the digital information realm. These threats are testing the ability of democratic governments to protect fundamental freedoms like privacy, free expression, freedom of assembly and association and the right to democratic participation in digitized society. At the same time, the malign actors who have capitalized on these vulnerabilities to attack democracy generally have escaped consequences.

All of this is eroding confidence in democratic governance in the digital realm. The sense of radical insecurity has led some democratic governments to undertake security measures or enact regulations that are inconsistent with their human rights commitments, such as unchecked collection of data in violation of privacy or restrictions for online content that undercut free expression. Furthermore, trust between democratic allies has been eroded by competing assessments of what human rights principles and democratic values actually require in the digital context. In particular, a transatlantic rift

has emerged over a broad portfolio of digital policy challenges, ranging from cross-border data transfers; unchecked digital surveillance by governments; private sector “surveillance capitalism;” monopoly power of U.S. platforms; and tech regulations that fail to conform with democratic values. These digital policy tensions between democratic allies have had the unintended effect of undermining global confidence in the feasibility of adhering to international human rights norms and democratic values in digitized societies.

While democratic governments have been inwardly focused and preoccupied with their own tensions, a digital-authoritarian model of control through data and technology has gained traction globally. This digital authoritarian model, which rests on a concept of “cyber sovereignty,” now competes with the open democratic vision of the internet and society. Authoritarian governments, most notably China, have become increasingly adept at using digital technology for repressive purposes at home, role-modeling these practices to the world. They also have capitalized on the growing export-market for surveillance and censorship technologies, spreading these capacities to others to follow their repressive lead.

Unfortunately, China’s leadership also recognized earlier than most that dominance in technology brings significant geopolitical, diplomatic and normative influence. Their massive strategic investments in technology already have translated into the ability to embed and spread China’s authoritarian values globally, particularly within tech standard and protocol setting bodies like the International Telecommunications Union. Sadly, China’s digital authoritarian influence has also shown up in more traditional norm setting arenas, such as the UN Human Rights Council, where absurd declarations of support for China’s repressive use of technology in Xinjiang and in Hong Kong have succeeded. Finally, the digital authoritarian concept of “cyber sovereignty,” which is antithetical to a global, open, interoperable internet and justifies its fragmentation, also serves as support for a more conventional authoritarian stance — rejection of external criticism based on internationally recognized human rights — now applied in the digital realm.

---

***Strong U.S. leadership is needed to develop a compelling democratic conception of digitized society and to rebuild the democratic alliance around a shared strategic technology agenda.***

---

Democracies must recognize that we are in a geopolitical battle over the governance model that will dominate in the 21st Century digital context. This presents an existential threat not just to U.S. economic and national security, but also to our values-based vision for the internet and open democratic digital society. Strong U.S. leadership is needed to develop a compelling democratic conception of digitized society and to rebuild the democratic alliance around a shared strategic technology agenda.

To achieve these aims, the incoming administration should focus on five practical priorities.

First, we must “get our own house in order” by ensuring that U.S. digital technology policy is consistent with human rights and democratic values. The level of attention to the normative dimensions of technology policy, as well as to investment in emerging technology, must adequately reflect its strategic importance to our security.

Second, the digital policy rift with our transatlantic partners must be healed: without U.S.-EU alignment, other democratic partners will lose confidence that a democratic model for digital society is a realistic goal.

Third, the democratic alliance must be rallied around a shared model for democratic governance of digital society and a strategic technology agenda. This democratic model must incorporate institutional constraints on both public and private sector use of data. It also will require further articulation of how government and technology companies apply and adhere to international human rights law and norms in the digital context.

Fourth, we must compete with the digital authoritarian model of governance and develop a comprehensive strategy to combat it. Robust diplomacy in the international normative arena will be essential, both with respect to technical standards and protocols, and with respect to norms on use of data and technology.

Fifth, the U.S. must reclaim the internet for citizens and humanity by investing in innovation and entrepreneurship in regions that have not been included in the digital revolution, both domestically and internationally. Investment in “E-Government” capacities to provide secure and efficient public services should be uncontroversial, as should investments in digital security tools for citizens, consumers and civil society actors. Expanding access to internet connectivity domestically and abroad should also be an early, uncontroversial priority.

This is a full plate. But early attention to these aspects of the democracy and technology portfolio will pay huge dividends for the Biden-Harris team, the U.S. and the democratic world.

## **RECOMMENDATIONS FOR THE BIDEN-HARRIS ADMINISTRATION:**

- I. Recognize the normative dimensions of digital technology policy as a strategic concern distinct from cybersecurity. Ensure coherence between domestic and foreign policy and adherence to international human rights law and norms.**

Building a democratic approach to digitized society must start at home. U.S. domestic digital technology policy must not undermine our vision of an open internet or our commitment to core human rights principles. “To get our own house in order,” we need to assess the use and regulation of data and digital technology by the U.S. government, with reference to fundamental rights to privacy, freedom of expression, and other basic liberties. Accordingly, U.S. policies, applications and regulations related to data, digital platforms, artificial intelligence and other emerging technologies must be evaluated for consistency with human rights principles. Furthermore, the strategic

---

***Building a democratic approach to digitized society must start at home. U.S. domestic digital technology policy must not undermine our vision of an open internet or our commitment to core human rights principles.***

---

importance of technology policy to democracy should be reflected through higher-level coordination across agencies and greater coherence between domestic and foreign policy. The most basic point is that the normative dimensions of technology policy must be seen as a strategic issue and be adequately reflected in both domestic and foreign policy.

The administration should start by strengthening mechanisms for values-based technology policy development and coordination with the United States government.

- **The National Security Council must focus on normative and diplomatic challenges in the digital realm, as distinct from more traditional cybersecurity concerns.** Three focal points include establishing processes to: 1) resolve tensions with allies over how to apply existing international human rights law in the digital context; 2) develop doctrine related to application of international norms in cyberspace related to cross-border harms and malign activity; 3) evaluate human rights impacts of U.S. government use of data and technology across agencies, as well as of the impact of domestic digital technology policies on global internet freedom.
- **The U.S. profile in international technology-related diplomacy must be raised, potentially by establishing an ambassador-at-large for global digital affairs.** The ambassador would elevate U.S. participation in bilateral, multilateral and multi-stakeholder digital and cyber policy development and in international norm-setting arenas. As

a first step, U.S. leadership should be dramatically reinvigorated within the Freedom Online Coalition (FOC), including by seeking to chair the coalition. Robust U.S. diplomacy also is needed at international fora where technology standards and protocols are set, such as the International Telecommunications Union, and in arenas where norms of responsible state behavior in the cyber realm are developed, such as the UN Government Group of Experts. Among the first set of initiatives, the Ambassador could engage the U.S. in the [Paris Call for Trust and Security in Cyberspace](#).

- **The new Cyberspace Security and Emerging Technology Bureau at the Department of State announced on Jan. 7, 2021 should be quickly built to serve the goals outlined in the [Cyber Diplomacy Act](#).** The Bureau should cover the full spectrum of technology policy challenges, including development of international norms for cyberspace, tech standard-setting, human rights-based analysis of government and private sector use of data, democratic export controls on technologies of repression, and democratic regulation of digital platforms. The office should take responsibility for developing more robust export controls for repressive technologies and appropriate democratic institutional constraints with respect to government use of data and technologies.
- **Establish a Department of State unit in Silicon Valley, comparable to the Defense Innovation Unit created by the Department of Defense.** Its mandate should include exploration of technology innovations related to more effective use of data and technology in governance and provision of public services, as well as technologies that enhance citizens' privacy, digital security, digital literacy and civic engagement—innovations that the State Departments could then help diffuse worldwide. The office should also be tasked with engaging on policy development with digital platforms and other technology companies, particularly with respect to private sector responsibilities to respect human rights as outlined in the UN Guiding Principles on Business and Human Rights. The unit should also lead in



multi-stakeholder digital policy development processes that bring civil society voices into democratic technology policy development.

## **II. Resolve the transatlantic digital policy divide, particularly with respect to cross-border data transfers and digital platform regulation.**

Any prospect of building a shared democratic technology agenda will require resolution of current tensions between the U.S. and the EU over technology and data. Without U.S.-EU alignment, other democratic partners will lose confidence that a democratic model for digital society is a realistic goal.

Among the most urgent issues to be address are substantial divisions over cross-border data transfer arrangements, digital surveillance by both governments and the private sector, and regulation of digital platforms consistent with democratic values. These disagreements have already [placed](#) \$7 trillion in transatlantic digital trade at risk and led some members of the EU toward a vision of digital sovereignty that could undermine any potential for a shared democratic approach to digital society.

The first step in healing the transatlantic digital policy divide must be an early concerted dialogue with the EU on three priority issues:

- **Rapid development of an alternative to the Privacy Shield data arrangement.** This agreement, negotiated between the U.S. and Europe during the Obama-Biden administration, was struck down in July 2020 by the EU Court of Justice as inconsistent with fundamental rights. Rectifying this problem will require high level negotiations about adequate institutional constraints on government surveillance and appropriate restraints on data-sharing between government and private sector platforms.
- **Agreement on a transparency and accountability regime for digital information platforms applicable to U.S. platforms operating in the EU.** This framework should emphasize users' procedural rights and control of data. Recommendations from

the Transatlantic high level working group [Transparency and Accountability Framework](#) can provide a starting place. Instead of content-based regulations that place liability on platforms for user-generated content and put freedom of expression at risk, (as seen in some EU country regulations), transparency and accountability mechanisms enhance democratic oversight in ways that are consistent with free expression principles. In addition, greater platform transparency can help educate users, regulators and researchers about algorithmic information systems and build civic resilience to disinformation.

- **A process for resolving conflicting U.S.-EU approaches to fundamental rights in the digital policy realm.** This new process should serve as a vehicle for resolving tensions over conflicting interpretations of how to protect substantive human rights, how to apply international process principles of necessity and proportionality, and how to assess government regulation of digital platforms so that they are consistent with human rights.

### **III. Galvanize the democratic alliance around a shared values-based vision of digital society and a comprehensive digital technology agenda.**

The U.S. should lead a process of renewal for the democratic alliance that inspires optimism and confidence in the superiority of a democratic approach to governance of digital society, as well as commitment to an open internet.

To start the process, the administration should:

- **Capitalize on the opportunity provided by the Summit For Democracy by bringing concerted focus to challenges related to democratic governance of digital society and the strategic importance of values-based digital technology policy for the future of democracy.** The Summit setting will provide a vehicle to jump start the process of developing a more strategic digital technology agenda. It will also provide an early opportunity to help heal democratic divisions over tech regulation, align responses to

tech-related security threats, and expand tech-based partnership. The Summit should cover the full spectrum of technology policy challenges, including strategic tech R&D investment, tech standard-setting, human rights-based analysis of government and private sector use of data, democratic export controls on technologies of repression, democratic regulation of digital platforms, and civic education on responsible use of social media. In addition to policy, a coordinated plan among trusted democratic partners should be initiated to protect the supply chain for essential technologies, such as semiconductors and 5G infrastructure, as well as strategic commitments from democratic partners for increased R&D investments in emerging technologies. Top policy priorities must include development of a mutually beneficial data sharing arrangement among democracies, and shared norms on government surveillance consistent with human rights principles.

- **Following the summit, an ongoing process for developing a shared democratic approach to technology and digital society should be instituted. The process could be divided into different work streams with different “Digital Technology” (DT) partner-groupings:**
  - **DT-10: to develop a strategic technology investment agenda.** Many different configurations are possible. This cohort could be comprised of the U.S., UK, Canada, Australia, France, Germany, Sweden, Finland, South Korea, Japan, plus Taiwan perhaps as an observer-participant. Its primary aim would be to advance a plan to secure supply-chains for critical tech and joint strategic investments in emerging tech.
  - **DT-12: to resolve democratic tensions and seek harmony on digital technology policies.** This groups could be comprised of the G7, the EU, Australia, New Zealand, India, and Brazil. Its aim would be to resolve tensions between democratic allies over appropriate checks on government and private sector used of data, as well as harmonious regulatory approaches to private sector platforms.

- **DT+: to defend democratic, human rights-based governance of digital society.**

This group should include all FOC members (Australia, Austria, Canada, Costa Rica, the Czech Republic, Estonia, Finland, France, Georgia, Germany, Ghana, Ireland, Japan, Kenya, Latvia, Lithuania, the Republic of Maldives, Mexico, Moldova, Mongolia, the Netherlands, New Zealand, Norway, Poland, Spain, Sweden, Switzerland, Tunisia, UK, U.S.), and be open to other democratic allies. The focal point would be to reinforce commitment to freedom in the digital context and to develop a democratic human-rights based approach to governance of digital society.

#### **IV. Combat the emerging digital authoritarian model of governance.**

AS the U.S. and our democratic allies struggle to address tensions between ourselves and to reconcile our conflicting digital technology policies, we must not lose sight of the threat posed by authoritarian export of technology and norms. A top priority for the U.S. and our democratic allies must be to develop a comprehensive strategy to combat the rise of digital authoritarianism. To this end, the U.S. must:

- Renew global advocacy for a free and open internet with an updated vision for how to protect it.
- **Rejoin the UN Human Rights Council (HRC) to rebuild the global normative consensus around internet freedom.**  
The U.S. should lead in developing an advocacy strategy to counter authoritarian influence at norm setting bodies and normalization of authoritarian applications of digital technology that violate human rights.
- **Invest in coordinated international diplomacy at multilateral and multi-stakeholder fora where technology standards and protocols are developed.**

- **Resist export of authoritarian digital information infrastructure and support a stronger export control regime for authoritarian surveillance and censorship tools.**
  - In particular, restrict China’s access to technology and equipment that facilitates domestic semiconductor manufacturing.
- **Prioritize development of civic resilience to cross-border information operations and the spread of propaganda and disinformation by authoritarian governments.** Rebuilding trust in information will be essential for civic engagement in democratic digital society. To date, democratic governments have been inadequately prepared to combat these challenges and need significant improvements to stay ahead of adversaries.
  - **Build a multistakeholder mechanism for developing best practices to combat disinformation,** modeled on the Global Internet Forum to Counter Terrorism ([GIFCT](#)), including a vehicle for information-sharing between government, civil society, the research community and the private sector.
  - **Build stronger transnational information sharing mechanisms between democratic allies,** to counter foreign malign information operations and share best practices in building civic resilience.
  - **Advocate for new norms for professional reporting on hacked material and disinformation,** as proposed in the [Stanford Guidelines for reporting on disinformation and hacked material](#)
  - **Increase investments in building civic resilience to digital disinformation, including public education on norms of civic discourse, media literacy and digital literacy.**
  - **Advocate for the Transatlantic Commission on Election integrity** [Election Pledge](#) to strengthen norms and expectations for political candidates and parties to reject and denounce propagation of disinformation around elections.

## V. Reclaim digital technology for civil society and humanity.

To rally the democratic world around a democratic vision of digital society, the U.S. must help restore a positive vision of how technology can support democratic activity, civic engagement and the enjoyment of human rights. The new administration should invest in innovation and access to technology to empower citizens. To this end, the U.S. should:

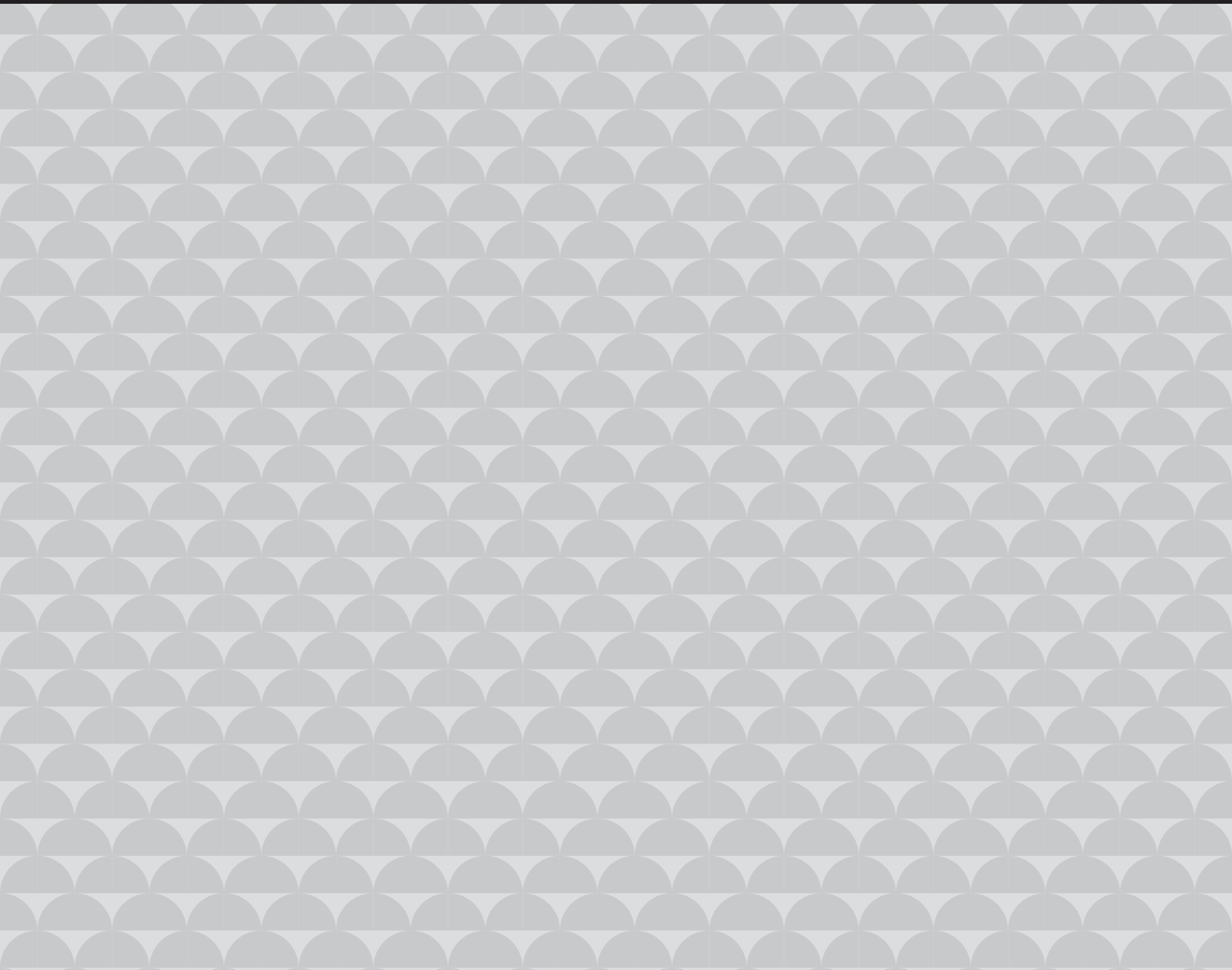
- **Support development of artificial intelligence (AI) applications to achieve the Sustainable Development Goals**, while respecting the right to equal protection and nondiscrimination by ensuring inclusion in the benefits of AI; the data used to feed AI; the coding community that builds AI; and in AI policymaking.
- **Role-model inclusivity in the U.S. domestic context, by pledging to provide Internet access for all Americans**, with particular focus on access for minorities, vulnerable communities, women, and economically disenfranchised citizens. Invest in rural and urban broadband in unserved areas, commit to ensure internet connectivity across the U.S., and advocate for universal internet access internationally.
- **Provide digital security education and tools for U.S. citizens and global civil society** and funding for digital and media literacy education and **create a fund to invest in emerging technologies to support and encourage civic participation.**
- **Invest in “E-government” technology innovations that enhance efficiency, security and accountability in government provision of public services.** Explore the use of public data trusts, secure digital ID, and technology platforms that enhance citizen communication with elected representatives.

- **Support global technology innovation and entrepreneurship particularly in the Global South.** A genuinely inclusive and democracy-sustaining global internet must entail some “home-grown” digital platforms and services emerging in the developing world, especially in countries where internet adoption is growing fastest.

#### ABOUT THE AUTHOR

**Eileen Donahoe** is the Executive Director of the Global Digital Policy Incubator at Stanford’s Cyber Policy Center. She served as U.S. Ambassador to the UN Human Rights Council during the Obama administration, and then as Director of Global Affairs at Human Rights Watch.

# CONCLUSION





## CONCLUSION, AND ADDITIONAL PRIORITIES

New and emerging technologies promise to be amongst the most influential forces of this century and will transform every aspect of our public and private lives. The policies developed to govern these new technologies will play a pivotal role in shaping our global future. The incoming administration and Congress is encouraged to make significant headway by considering the recommendations included by the authors highlighted here.

At the same time, a range of important issues are necessarily left unaddressed in this report, but are too significant to fail to mention. The following section on Additional Priorities highlights other areas requiring urgent attention from federal policymakers. These priorities are covered thoughtfully in related publications, including the Aspen Cybersecurity Group's [A National Cybersecurity Agenda for Resilient Digital Infrastructure](#) and the German Marshall Fund's [#Tech2021 - Ideas for Digital Democracy](#), while these and many more urgent needs are addressed in the [March 2020 Cyber Solarium Commission Report](#).

- **Education and Workforce:** The [prior two](#) administrations have highlighted that the nation's cybersecurity workforce is a "strategic asset" suffering from a persistent supply shortage: employers in the United States alone report over [520,000](#) open cybersecurity roles. The field is both under-staffed, and much less diverse than it should be. To address this, policymakers and the field writ large must increase awareness of cybersecurity as a potential career path, improve relevant education and skill development, and support the public and private sector in improving their practices to ensure better representation from underrepresented groups.
- **Protecting the Public Core:** The public core point to the core elements that enable the Internet to function, and that create extraordinary public value. It is comprised of the primary rules, processes, protocols and infrastructure that allow Internet operability, including packet routing and forwarding, naming and numbering systems, cryptographic means of security and identity, etc. When

these central elements of the public core were created, the need for strong security features was less clear. It is now too late to supplant many of these elements with more secure substitutes. Instead, many argue that protecting the public core will require the development of [new universal norms](#) as a basis for responsible behavior, as suggested by the Global Commission on the Stability of Cyberspace in 2018 on which the Cyber Center’s Marietje Schaake served. Development of such norms will require global collaboration between state and non-state actors, as well as with the private companies and international nonprofits that manage most aspects of the public core.

- **Cybersecurity Metrics:** It has been widely noted that the U.S. government lacks even the most basic data about the frequency and severity of cyber attacks, the most prevalent security failures, and the most successful interventions impeding attempted attacks, as well as data or research indicating the return-on-investment for security measures taken. These gaps make it difficult to incentivize better government and private sector risk management. Experts have recommended that the government must, most urgently: develop a Bureau of Cyber Statistics, as [recommended](#) by the U.S. Cyberspace Solarium Commission; begin to collect a limited set of basic data; and begin to assess the cost-effectiveness of competing cybersecurity frameworks.
- **Supply Chain Security:** Most new technologies include hardware and software components sourced from multiple vendors, with additional potential vulnerabilities introduced during assembly and routine updating. To address this, experts have proposed a wide range of interventions including: reforming the federal acquisition process; improving transparency, including the potential introduction of “ingredients lists” indicating software and hardware components integrated into new technologies, and new device labeling regimes; mandating risk analysis; creating “critical technology testing centers” as recommended by the U.S. Cyberspace Solarium; increasing competition amongst producers; and transferring some liability for

supply-chain risk to the primary vendors responsible for integrating complete products and systems.

- Public-Private Sector Collaboration:** In cyberspace the private sector, rather than the government, is often the primary actor. In order to either proactively disrupt threats before harm occurs, or better respond to and recover from cyber events, the U.S. government must better communicate with the private sector regarding emerging threats, and establish mechanisms for better operational cross-sector collaboration. Experts have noted that doing so will require the creation of new roles within federal government, new incentives for law enforcement (who are currently rewarded more for prosecution of crimes than for disruption of crimes before they occur), revisions to legal barriers that inhibit government-private sector coordination, and more.
- Predictive AI and Algorithmic Bias:** Predictive analytics tools use algorithms and machine learning, informed by historical data, to predict the likelihood of future outcomes. Their use in the private sector, by companies like Amazon to recommend future purchases, has been seen as (relatively) innocuous. However, these tools have been increasingly deployed in the public sector, with [demonstrated biases](#) in terms of race, age and gender when informing [housing loan decisions](#), [prison sentencing and parole eligibility](#), and more. To address these concerns, experts have suggested: mandating government disclosure of all predictive analytics tools in use by government, and their impacts; requiring audits of decision-making algorithms before they are adopted; issuing guidelines for assessing algorithms during the government procurement process; and Congressional designation of [regulatory sandboxes and safe harbors](#) for predictive technologies. Congress has also introduced several relevant acts, including the Facial Recognition and Biometric Technology Moratorium Act of 2020, and the No Biometric Barriers to Housing Act and Algorithmic Accountability Act of 2019.

The **Stanford Cyber Policy Center** at the Freeman Spogli Institute for International Studies is Stanford University's premier center for the interdisciplinary study of issues at the nexus of technology, governance, and public policy. Program areas address topics including cybersecurity, election security, misinformation, digital democracy and human rights, artificial intelligence, and emerging technologies. Through research, policy engagement, and teaching, the Cyber Policy Center seeks to bring cutting-edge insights and solutions to national governments, international institutions, and industry.