liber-net

Federal Policy Proposals to Protect Digital Free Speech in the United States

March 3, 2025
Version 1.4

Table of Contents

Introduction

It is increasingly clear that the U.S. federal government has developed a large-scale system to coordinate the suppression of its citizens' First Amendment-protected speech. Evidence supporting this assertion comes from the Twitter Files, discovery evidence in the combined cases of *Murthy v. Missouri* and *Kennedy v. Biden*, and the U.S. House Judiciary Committee on the Weaponization of the Federal Government. This body of evidence has demonstrated the existence of a network of nongovernmental organizations (NGOs), academic institutions, think tanks, and major technology companies often working directly with, or under pressure from the government to control flows of information and censor online content. This network is sometimes referred to as the "Censorship-Industrial Complex."

On August 27, 2024, Meta CEO Mark Zuckerberg issued a statement confirming that the Biden administration pressured Meta to censor First Amendment-protected speech relating to Covid and the Hunter Biden laptop story. In the case of Covid, Zuckerberg revealed that the Biden White House "repeatedly pressured our teams for months to censor certain Covid content, including humor and satire," and expressed regret that Facebook complied by suppressing the New York Post story about Hunter Biden's laptop after receiving a warning from the Federal Bureau of Investigation (FBI) regarding a "Russian disinformation campaign." Beginning in January 2025, Meta moved to roll back some of their speech controls on the platform, including severing relationships with third-party fact-checkers.

In addition to direct FBI pressure, 50 former national security officials claimed the Hunter Biden story was a "Russian information operation" in an effort to discredit it. A host of major media outlets, NGOs, and fact-checkers repeated this assertion in lockstep. The story was quickly suppressed on platforms like Twitter and Facebook, potentially influencing the outcome of the Presidential election, which was mere weeks away.

Federal officials engaged in similar behavior through the entirety of Covid. Multiple leaked documents revealed the government placing direct pressure on social media platforms to censor online speech, including seeding or supporting academic and NGO consortiums to act as proxies to hide this government pressure. Perhaps the best-known example is the Virality Project, an endeavour initiated by the Department of Homeland Security (DHS) and led by the Stanford Internet Observatory (SIO). This project pushed for the censorship of academics and individuals who disagreed with policies of the Centers for Disease Control (CDC), even advising major social media partners to label true stories of vaccine side effects as "misinformation."

Unfortunately, these high-profile incidents are likely just a small fraction of instances where the U.S. government has put its thumb on the scales to influence content moderation decisions on private platforms. While government officials have claimed that they are merely using their own speech capacities to make policy, their pressure campaigns are implicitly backed by the threat of using broader regulatory or legislative powers to bring companies to heel if they do not comply.

Open discourse is the central pillar of a free society, essential for holding governments accountable and fundamentally protecting and empowering vulnerable groups. Protections for individual speech and expression apply not only to views we agree with but also to those we strongly oppose. The Supreme Court has repeatedly ruled in First Amendment cases that the "government has no power to restrict expression because of its message, its ideas, its subject matter, or its content," and has explained that "if there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion." Indeed, as Justice Breyer noted, "it is perilous to permit the state to be the arbiter of truth," even when such truth can actually be established (*United States v. Alvarez*, 567 U.S. 709, 731–32) – to say nothing of cases when truth, in fact, cannot. Notably, the First Amendment specifies not only government *prohibition* of speech, but the mere *abridging* thereof. The writers of the U.S. Constitution and Bill of Rights deeply understood that the ability to freely speak, write, and publish is a foundational element of human nature and is therefore an inalienable right. The protections they enshrined in the First Amendment remain some of the strongest bulwarks against authoritarian censorship and tyranny ever devised.

The broad pattern of government overreach we have witnessed over recent years demonstrates a strong need to reinvigorate free speech protections across the United States. This document presents a series of ideas for how the federal government might achieve this goal, complimenting our recent research into digital free speech-related legislation at the State level.

Our proposals cover content-based digital speech transmitted on or through the Internet, the restrictions on which would receive strict scrutiny from a court of law. They do not address matters relating to conduct, government speech, or commercial speech, nor do they cover the "unprotected speech" categories of obscenity, defamation, fraud, incitement, immediate threats of violence, speech integral to criminal conduct, and child pornography. Similarly, topical but non-digital matters such as issues of free speech on academic campuses fall outside the scope of this paper.

Overview of Federal Grant Funding for Information Suppression Projects

Many Americans are familiar with the warning delivered by outgoing president Dwight D. Eisenhower of the 'military-industrial complex' and the fundamental changes it brought to American society. Fewer, however, are as familiar with the subsequent warning he delivered in his famous farewell address: that of a rising scientific-technical elite and the federal government's domination of the nation's scientific research funding. In much the same way, agencies across the United States federal government have been administering increasing amounts of funding to U.S. and foreign based academic institutions, NGOs, and private sector enterprises for research and development initiatives relating to Internet content controls for digital speech accessible to American citizens, such as countering mis-, dis-, and malinformation (MDM), "hate speech," and more.

The volume and dollar amount of these grants has increased dramatically as both applicants and grantors reconcile their waning ability to frame and manage narratives, a function which has been usurped by new online media. As a result, increasing energy, attention, and funding has been devoted to a wide variety of strategies to stifle free expression online under the guise of combating "misinformation," protecting public health, and more. Censorship advocates frequently used the phrase "whole-of-government approach" or even "whole-of-society approach" to describe the deployment of official and unofficial government authorities to suppress disfavored speech. The federal government's powers to legislate, regulate, investigate, prosecute, and most importantly-appropriate funds, have all been deployed to varying degrees in the pursuit of this end.

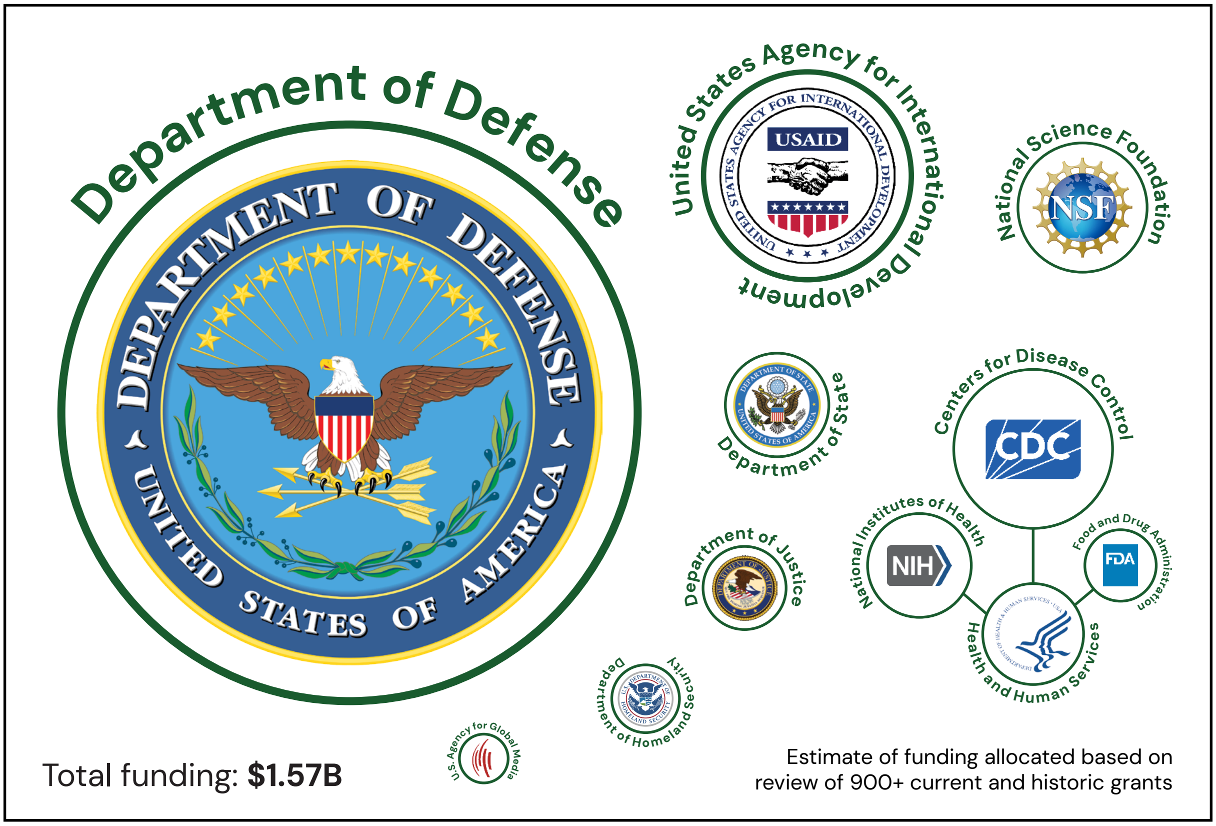
A myriad of federal agencies, including the Department of Defense (DOD), Department of State (DOS), the National Science Foundation (NSF), the DHS - especially the Cybersecurity and Infrastructure Security Agency (CISA) -, the United States Agency for International Development (USAID), and the CDC, National Institutes of Health (NIH), which fall under the Department of Health and Human Services (HHS), have all funded millions of dollars of digital MDM research and development since 2019. This includes, at a minimum, funded grant proposals that include the terms "misinformation," "disinformation", or both. Each of these federal institutions allocates this funding in its own way, but the funded projects are often similar.

The extent of the federal government's attempts to control online speech cannot be understated. Investigative reporting has revealed that numerous federal agencies have been involved in attempts to suppress online speech, including the FBI, the State Department's Global Engagement Center (GEC), the DHS and its CISA, and grantmaking agencies such as the NSF.

While basic information on this grantmaking activity can be easily accessed online, the amount of useful information about these grants varies widely by agency. NIH and NSF grants, for the most part, include detailed explanations of the research work, and the names of both the Primary Investigators (PI) receiving the funds and the agency staff in charge of that grant program.
For some of these grants, and particularly for Track F awards, simple online searches for the grant titles often reveal articles written by university public relations departments or college newspapers explaining and promoting the work and occasionally interviewing the PI. Conversely, grants from USAID and the Departments of State and Defense lack this detailed information, including only grant dates, dollar amounts, recipient names, and very short, often cryptic descriptions of the funded work.

U.S. Government Agencies Funding Information Suppression

2019-Present

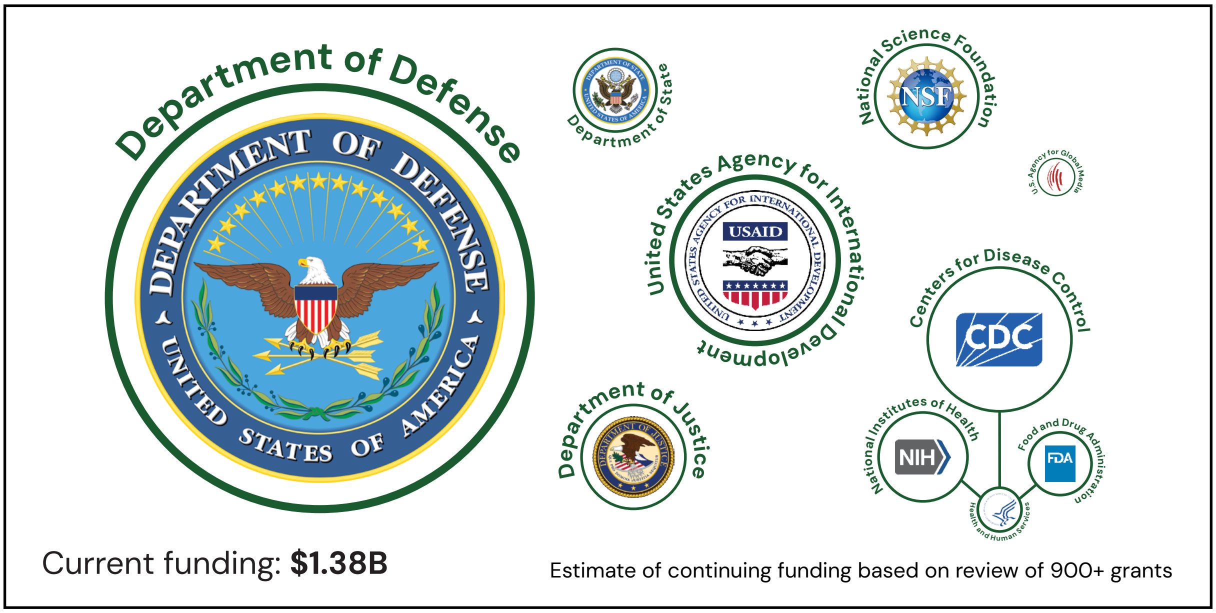


Total funding: **$1.57B**

Estimate of funding allocated based on review of 900+ current and historic grants

Current Funding for Information Suppression

Funding Ending After 2/1/25

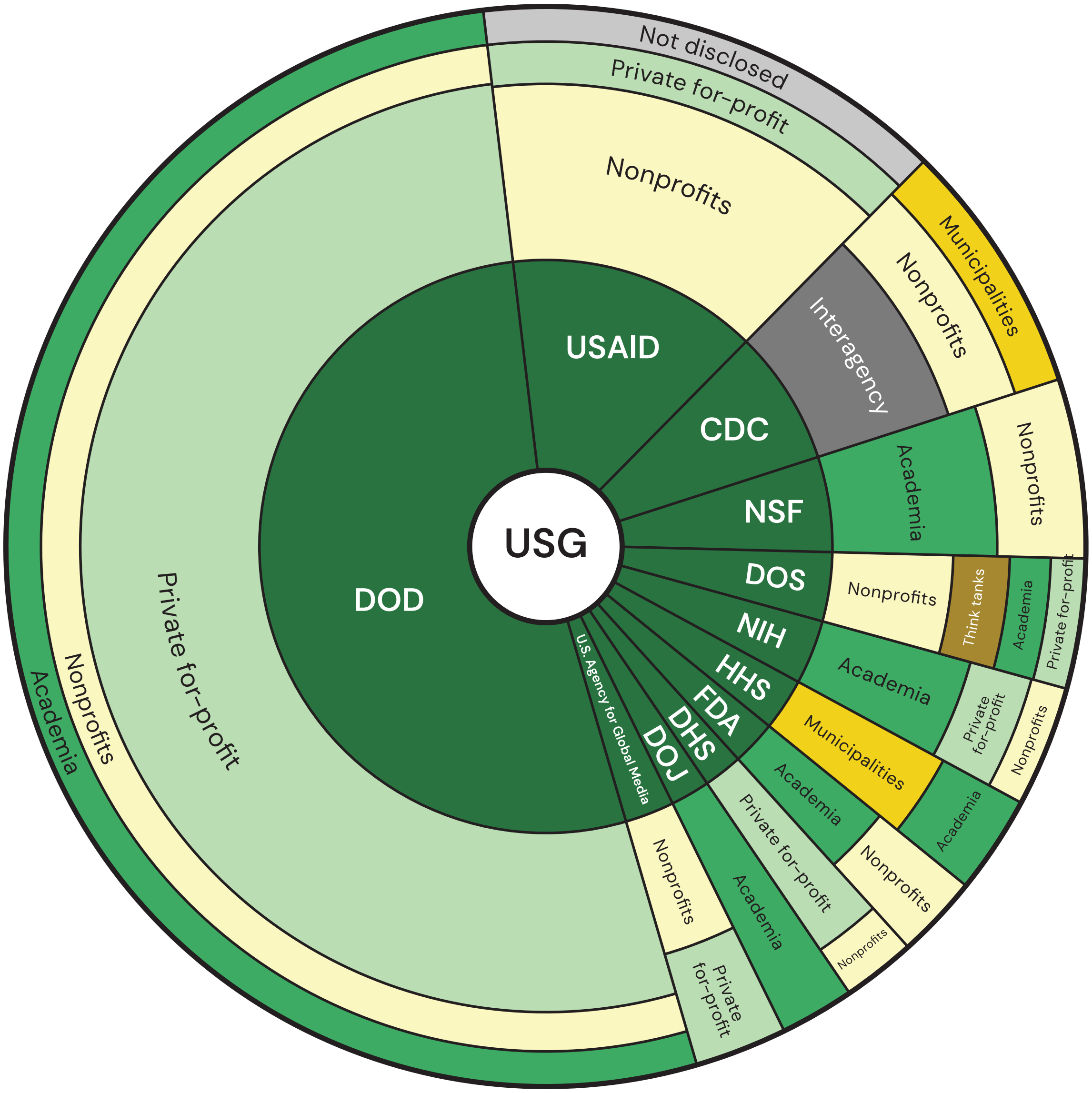


Current funding: **$1.38B**

Estimate of continuing funding based on review of 900+ grants

U.S. Government Agencies Funding Information Suppression

Major recipients of relevant federal grants



Total funding: **$1.57B**

Sectors

🟩 Academia
🟩 Private For-Profits
🟨 Nonprofits
🟨 Municipalities
🟫 Think Tanks
⬛ Interagency
⬜ Not Disclosed

With an annual budget reaching nearly $50 billion, the **National Institutes of Health (NIH)**, with its 27 constituent centers and institutes, is a major funder of biomedical and related research across the country. Our investigation revealed that, at a minimum, the NIH has awarded $50 million to at least 45 various types of MDM research and development projects, 34 of which are ongoing. It is important to highlight the preliminary nature of this accounting; we anticipate these numbers to climb once information can be obtained directly from the agencies. Major recipient institutions include City University of New York, New York University, Duke University, University of Pennsylvania, University of Miami, University of Texas, University of Oregon, Icahn School of Medicine at Mount Sinai, Northwestern University, Wake Forest University, and the private business Gryphon Scientific, Innova8AI, Klein Buendel, Inc., and Melax Tech.

Discoveries to date show that the NIH has doled out Covid-related MDM research funds to a dizzying array of projects, including efforts to scan and track MDM relating to Covid and vaccines on social media, with a handful including interventional efforts to flag content for removal, paying influencers to promote favored content, and 'pre-bunking' vaccine skepticism with tested messaging. Notably, several of these Covid-related projects are still ongoing and funded for several more years to come, including those related to promoting uptake of ineffective vaccines. But studying MDM in relation to diseases, drugs, and vaccines is not limited to Covid. Over the past several years NIH funding of MDM research has crept into the fields of epidemiology, HPV, HIV, tobacco use, and even prostate cancer and sun tanning.

Curiously, many of these grants fund research that is entirely non-biomedical, particularly computer science and related endeavors such as network modeling, development of large language models (LLM) and natural language processing (NLP) to analyze online speech, AI systems, and chatbots, as well as psycho-social research such as vaccine persuasion methods and message testing. Public skepticism towards medical interventions, particularly vaccines, is universally presented as a socially negative obstacle to be overcome with force from above, rather than with open-minded public dialogue. The result, we argue, is less trust in these institutions, not more.

The institutional sources of MDM-related funding are varied and somewhat flexible, with research proposals and abstracts approved in this new, lucrative industry very frequently including references to niche identity groups and their neologisms. Many grants given by the National

Institute of Mental Health (NIMH) relate to infectious disease, and the all-encompassing National Institute on Minority Health and Health Disparities (NIMHD) has funded a wide range of projects involving, even tangentially, any variety of minoritized groups. In fact, NIMHD is the largest NIH source of MDM research funds in our database, followed by the National Cancer Institute (NCI), the NIMH, the National Institute on Drug Abuse (NIDA), and the National Institute of Allergy and Infectious Diseases (NIAID) rounding out the top five. It is likely that the upswell in funding made available for MDM-related projects, as well as those focusing on "marginalized groups," incentivizes grantseekers to incorporate these themes into their existing research niches.

The Centers for Disease Control and Prevention (CDC) is involved in similar biomedical work. Although the CDC is not generally known as a large source of public research funds compared to the NIH, our investigation revealed over $117 million in just six grants at least partially devoted to combatting health-related MDM.

The University of Pittsburgh received a $1 million grant entitled "A Discourse-Aware, Community-Informed Toolkit to Predict Virality and Impact of Vaccine Misinformation Contents" to "develop a contextually grounded natural language processing (NLP) model and build a toolkit around it to leverage the benefit of latest developments in data analytics, network simulations and NLP for increasing vaccine acceptance, vaccination rates and disseminating accurate scientific messages according to community needs."

The municipalities of Pima County, Arizona, and City of Long Beach, California, received large CDC grants of $6.5 million and $6.9 million, respectively, for 'community engagement' projects to "boost vaccine uptake by countering misinformation." Similarly, UnidosUS (formerly known as National Council of La Raza [NCLR]), the largest U.S. NGO promoting the interests of U.S. Latinos, received an enormous grant of over $22 million for an "education and awareness campaign to promote vaccination coverage among latinos" which facilitated "broader, national efforts [including] engagement of trusted influencers from various sectors and use of UnidosUS vast communications assets to deploy this education and awareness campaign." Most notably, the CDC awarded an $80 million grant to its own foundation, the National Foundation for the Centers for Disease Control and Prevention, to "partner with national organizations to support community-based organizations to increase access and acceptance of influenza and Covid vaccines among adults in racial and/or ethnic populations experiencing disparities." Further information on this massive project has been elusive.

With an annual budget floating around $800 billion, our research shows that the **Department of Defense (DOD)** has devoted over $1 billion to what appear to be MDM-related research projects, largely through the Office of Naval Research (ONR), Defense Advanced Research Projects Agency (DARPA), and the Air Force, mostly described as combating foreign influence operations. While very little public information is available on these awards and contracts beyond the brief descriptions on usaspending.gov, it is probable that additional project funding, and details of such projects, will come to light as deeper internal research is conducted. As is its tendency, the Pentagon has awarded a large amount of its MDM-related spending to private contractors like Peraton and Graphika, as well as various high-profile universities such as New York University, Stanford, Arizona State, Carnegie Mellon, and George Mason. The vast majority of the Pentagon's total comes from one massive task order to Peraton, Inc. for $979 million to "counter misinformation from U.S. adversaries." Information on this significant award was only found from a Peraton press release; we were not able to find this award on usaspending.gov as with all the others, which indicates that more such awards are yet to be found.

As one of the nation's largest funders of university research, the **National Science Foundation (NSF)** has also been one of the major funders of MDM-related research. Many recipients include multi-disciplinary teams from computer science, sociology, political science, and communications departments, within and across major university systems. Unlike the NIH, which focuses most of its funding on biomedical and epidemiological research, the NSF's funding is spread among a wider variety of scientific enterprises. For MDM research specifically, the NSF's funding is often awarded to computer science departments, AI, LLM, and NLP projects, and the deployment of such technologies to scan the Internet for disfavored speech. Our research to date has uncovered 94 MDM-related NSF awards totalling almost $65 million.

A large proportion of this spending was made through a grant program called the "Convergence Accelerator," launched by the NSF in 2019. Its stated purpose is to solve "national-scale societal challenges" aligned with specific research "tracks" that "have the potential for significant national impact" by gathering multiple disciplines, ideas, approaches, and technologies under the same umbrella. This two-phase program continues to fund research teams which work "convergently" in collaborative cohorts to solve issues relevant to their track and "impact society at scale."

In March 2021, the NSF introduced a new section of this program called "Track F: Trust & Authenticity in Communication Systems," soliciting proposals to address the manipulation or "unanticipated negative effects" of communication systems, with an allocation of $21 million. Track F was initiated at the height of the Biden Administration's censorship efforts and was one of its most targeted and explicit programs funding digital censorship.

In an early draft solicitation, NSF indicated that Track F projects "address issues of trust and authenticity in communication systems, including predicting, preventing, detecting, correcting, and mitigating the spread of inaccurate information that harms people and society"- essentially research into digital censorship methods. Major recipient institutions include the George Washington University, SUNY Buffalo, University of Michigan, University of Wisconsin, University of Washington, Massachusetts Institute of Technology, the Ohio State University, UC Irvine, and Temple University, as well as the nonprofit groups Meedan and Hacks/Hackers.

Through its global network of consulates and embassies, the **Department of State (DOS)** has distributed MDM research funds in countries all across the planet. The vast majority of these grants are small awards to nonprofits or NGOs under the guise of 'combating foreign influence,' usually from Russia or China, 'protecting journalism,' and 'improving media literacy/resilience.' While it appears that most of the 885 different grants amounting to over $50 million combined uncovered in our investigation were deployed overseas, we know from other investigations that the DOS has been involved in domestic censorship efforts, largely through its **Global Engagement Center (GEC)**. Among other initiatives, the GEC has provided support to the Global Disinformation Index (GDI), which created blacklists of U.S. domestic media voices.

The GEC also made attempts to "insert itself" into domestic content moderation conversations with Twitter, Facebook, and Google, and received pushback as a result. In particular, the underpinnings and operations of the GEC appear to be strongly antagonistic to the First Amendment. In 2019, the founding head of the GEC, Richard Stegnel, published an op-ed in the Washington Post criticizing America's unique First Amendment protections as a "design flaw…in an age when everyone has a megaphone." Stengel also advocated a revision of U.S. speech laws to resemble those of present-day Europe, saying in a televised interview: "The basis of the First Amendment, the marketplace of ideas model, is actually not working. Marketplace of ideas is this notion that good ideas will drive out bad ideas…. I'm actually very sympathetic now to the U.S. adopting some versions of hate speech laws in Europe."

While no longer a separate entity from the DOS as of February 2025, the **United States Agency for International Development (USAID)** was always closely connected with the State Department. Its leadership previously reported to the Secretary of State, and it is funded by Congress as part of the foreign assistance budget, which is typically included in the State Department's broader budget request. Our investigation revealed 28 USAID MDM-related grants since 2019, totalling $141 million to NGOs across the world, mostly to oppose foreign influence operations and bolster messaging efforts, 16 of which are ongoing.

The international nonprofit Internews Network received the vast majority of these funds. Since 2019 it received at least 15 grants totalling over $100 million for globe-spanning efforts including "media strengthening," "developing balanced information environments," "procurement for alternative resources in media," "building societal resilience in the face of disinformation," and even "increasing community awareness of Ebola transmission and treatment through journalist training, rumor tracking, and radio spots." While USAID's future is uncertain at this time and many of these grants may be cancelled, continued vigilance will be necessary as its operations and management of extant grants is transferred to the State Department.

For more on U.S. support for international censorship efforts please see the section entitled "Realigning Foreign Influence Efforts."

The Department of Homeland Security (DHS) has been a focus of anti-censorship investigators due to the outsized role of CISA acting as a hub for communications between government officials and Big Tech companies, as well as the highly controversial and short-lived Disinformation Governance Board. DHS's role in funding nongovernmental MDM research includes $1.2 million grant made through the Federal Emergency Management Agency (FEMA) to government contracting giant Guidehouse, Inc. for a generic "Blanket Purchase Agreement (BPA) call order for misinformation, disinformation, and mal-information analysis."

Additionally, CISA disbursed over $87 million to build the Center for Internet Security (CIS), which was ostensibly created to "collaborate with state and local governments on cybersecurity risks and incidents" but was additionally used to monitor lawful speech. The CIS runs the Election Infrastructure Information Sharing and Analysis Center, which in past elections operated a ticketing system staffed by Stanford University-employed CISA interns and other members of CISA's MDM team to report posts to social media companies and pressure them into removing content that academics and CISA deemed dangerous. The Election Integrity Partnership (EIP) and Virality Project were DHS-seeded initiatives led by the SIO. Both flagged First Amendment protected speech to social media content that was, as a result, taken down or labeled, and rotated a staff of content-flagging visiting interns between Stanford and Washington, DC. In fact, SIO head Alex Stamos has stated that the purpose of the EIP was "to fill the gap of things that the government could not do themselves" because the government "lacked both . . . the funding and the legal authorizations."

In addition to their own projects, these various agencies have also collaborated on information control efforts. In October 2024, the House Oversight Committee revealed that the DOD, DOS, other U.S. agencies, and the European Union (EU) helped fund the for-profit "fact-checking" firm Newsguard, including a $25,000 joint Pentagon-State Department contract in August 2020 to run a pilot program countering "disinformation" about Covid. In June 2024, the Committee launched an investigation into NewsGuard's apparent participation in a government-funded "censorship campaign" allegedly aimed at discrediting and even demonetizing news outlets by promoting its ratings of their reliability with advertisers.

NewsGuard had previously briefed the committee on contracts it had with the DOD, including the Cyber National Mission Force within U.S. Cyber Command, as well as the GEC and the EU's Joint Research Centre. Oversight Committee Chairman James Comer wrote letters to NewsGuard demanding more details about their government collaboration and expressed concern about the firm throttling disfavored outlets' "misinformation," including a published academic study on the failure of lockdowns. Comer noted that "these wide-ranging connections with various government agencies are taking place as the government is rapidly expanding into the censorship sphere."

Ending Government Coercion of Social Media Platforms and Restrictions on Legal Speech

Much of the justification for government censorship has occurred under the rubric of countering so-called “mis-, dis-, and malinformation” (MDM) and “hate speech.” An immediate step should be to remove the concept of “malinformation” from all government documents and policies. This concept is deeply flawed, as it often involves factual or true information presented in a context that is inconvenient for another social actor or interest group.

The concepts of “misinformation” and “disinformation,” should only come under the purview of the U.S. government when they clearly involve defamation, fraud, criminal activity, or large-scale foreign interference operations. Even then, caution is essential, as recent years have seen legitimate domestic dissent frequently labeled as “Russian disinformation” or other delegitimizing terms as a pretext for censorship. Indeed, the First Amendment creates “breathing space,” protecting hyperbole and even false statements “inevitable in free debate.” This applies even to deliberately false statements said with “actual malice,” as the Constitution does not allow for prosecutions for libel on the government as an entity. (*New York Times Co. v. Sullivan*, 376 U.S. 254 [1964]).

The second key justification for censorship has been claiming the need to counter “hate speech,” an inherently subjective concept. Courts have ruled that restrictions on hate speech would conflict with the First Amendment’s protection of the freedom of expression, and thus “hate speech” receives constitutional protection. The federal government cannot and should not police “hate speech,” except in limited cases of true threats, incitement to imminent lawless action, discriminatory harassment, or defamation. In all other cases, it is simply not within the purview of the government to police legal online speech. We do not mean to suggest that hate speech is not problematic in online spaces, but rather that it is not the government’s role to act as an arbiter of such speech. Other, more creative modalities that do not infringe upon the First Amendment need to be employed to tackle these challenges.

Unfortunately, the federal government has engaged in unprecedented attempts to control information flows and public opinion over the past few years, attempting to circumvent First Amendment limitations via the use of NGO, academic and think tank intermediaries who present themselves as research or policy initiatives but in fact frequently flag content to social media platforms for labeling and removal. As we suggest below in our list of proposed executive orders and legislation, all government funding to such initiatives should be terminated immediately.

Allowing free and rigorous debate within the marketplace of ideas, where disfavored speech is countered by favored speech, is the only acceptable - albeit, imperfect - alternative to centralized control of information. The Trump-Vance administration should prioritize reversing the digital speech restrictions and policies implemented by the Biden-Harris administration. The following list of model executive orders and legislation would be an excellent start toward meaningful reform:

1) Create a new position of White House Free Speech 'Czar' to oversee all free-speech and anti-censorship activity, as well as the implementation of the following reforms across the federal government.
2) An Executive Order declaring that it will be the policy of the administration to uphold First Amendment-protected speech across the federal government, and that all contractors, enterprises, schools, and universities that receive federal funding must make a similar commitment in writing in order to remain eligible for receipt of federal funds.
3) An Executive Order implementing similar language to that in HR 140, prohibiting federal employees from engaging in, supporting, or funding censorship of U.S. citizens, and encouraging Congress to pass a new version of the bill.
4) Similarly, an Executive Order initiating a government-wide audit of all spending on federally-funded anti-misinformation or disinformation initiatives until it can be thoroughly ascertained that they are not in any way facilitating or enabling the censorship of lawful speech. If violations are found, funding should be frozen and future funding barred for at least five years for any person or entity involved.
5) An Executive Order directing the Department of Education to conduct an audit of all institutions of higher education (IHEs) that receive any federal funding from any federal agency, including NIH, DHS, NSF, DOD, DOE, and/or who have one or more enrolled students that received federal student loans or Pell grants. This audit should identify any programs, initiatives, offices, or curricula that promote or promoted restrictions of legal online speech. Any IHEs found to be in violation should lose federal funding and become ineligible to receive future funds for at least five years.
6) An Executive Order implementing the language in S. 1672, requiring federal employees to disclose communications with providers of interactive computer services regarding restricting speech, and encouraging Congress to pass a new version of the bill; or,
7) An Executive Order implementing as much of HR 8838 as possible, and encouraging Congress to pass a new version of the bill which should prohibit agencies from directing or encouraging social media companies to remove users, label content as misinformation, or share user data, except in specific cases like criminal investigations or threats to public safety. It should also prohibit public-private partnerships where agencies collaborate with social media companies to monitor content, except in emergencies or related to imminent threats, and it should bar agencies and their employees from accepting free or discounted advertising. Every office of Inspector General should be charged with ensuring compliance with these provisions.

8) Direct the Attorney General to pursue legal actions likely to result in court decisions holding that the government violates the First Amendment when it privately solicits a third party to remove another person's lawful political speech from an online platform, and move legal precedent away from a focus on the line between "persuasion" and "coercion," since all requests from government officials are inherently intimidating.
9) An Executive Order requiring SF-424 (Application for Federal Assistance) grant applications to contain assurances that the applicant will commit to opposing censorship and promoting freedom of speech and expression in all funded programs and related work.
10) Create an internal policy wherein all candidates for the positions of solicitor general, U.S. attorney and the entire federal judiciary will be evaluated based on their answers to mandatory questions relating to policy and precedent about the First Amendment, censorship, government coercion, and Section 230 of the Communications Act.
11) Urge Congress to amend the Hatch Act by extending the Act's limitations on political activity to intelligence officials who retain a clearance after leaving government service. This would help prevent official authorities or credentials from being used inappropriately, as they were during the 2020 election.
12) In the interests of transparency, an Executive Order directing all federal agency defendants named in *Missouri v. Biden* and *Kennedy v. Biden* to make public within 60 days unredacted versions of all documents related to these cases.

Special attention should also be paid to Section 230 of the Communications Act, a critical law that generally protects "interactive computer services" like social media companies from liability for user-generated content on their platforms. This legal shield allows companies like Meta (Facebook), Twitter (now X), and Google (YouTube) to host a vast range of content without liability for defamation, unlike news outlets, while simultaneously permitting them to moderate content by removing what they determine to be harmful or inappropriate without being liable for censorship claims. Social media companies as we know them would likely not exist without the delicate balance created by this section of law and the jurisprudence it has inspired.

Social media companies' use of Section 230 has sparked heated debate over the past decade or so, as the role of these influential companies in controlling the flow of news and information has grown. Some critics have argued that these platforms have overreached in moderating content by removing posts or banning users without transparency, acts which potentially violate the spirit, if not the letter of Section 230. Others believe platforms should bear more responsibility, especially when their services are used to spread disfavored information. This has led to calls for reform from across the partisan spectrum, with proposals ranging from limiting the immunity provided by Section 230, to enhancing transparency in content moderation practices, to repealing the law altogether.

Should social media companies wish to continue curating the content on their platforms (as is their right), then antitrust options may need to be investigated to ensure that diverse viewpoints can be shared across a range of channels. Amending Section 230 could dramatically impact how social media companies operate. Changes might require these companies to take greater responsibility for curating user content or offer clearer pathways for users to appeal content takedowns. While Section 230 has been vital in fostering the growth of social media, its future may include reforms aimed at addressing the complexities of moderating speech in the digital age.

The following options should be considered as these changes are debated:

1) An Executive Order directing the Federal Trade Commission (FTC), National Institute of Standards and Technology (NIST), and the Department of Justice (DOJ) to produce a collaborative report within a year evaluating antitrust proposals that could break up large social media and technology companies and reset the market so as to create space for a wider range of platforms that could better express the diversity of viewpoints within the country.

2) New legislation requiring all large social media companies to submit to the FTC on a bi-annual basis detailed reports which the FTC shall make public 30 days after receipt, which must include:

   - Descriptions of their content management and terms of use policies;
   - Use of third party fact-checking organizations;
   - Who or what employees or systems are used to enforce their policies; and,
   - Detailed, fully de-identified information on the number of moderated or affected posts, the number of impacted individual users, and justifications for any actions taken.

3) An Executive Order creating a new office or fourth Bureau of the FTC with the unique authority to enforce all new laws, regulations, and reporting requirements relating to large social media companies. The purpose of these proposals is to consolidate the enforcement and supervision of any new laws regulating social media companies, and to avoid inter-agency confusion or conflict.

4) An Executive Order creating a new division of the Federal Communications Commission (FCC) specifically to oversee and enforce Section 230, particularly if Congress amends it.

Reining in Public Health Censorship

While the federal government's censorship operation has targeted a range of issues, the response to Covid was a major acceleration point in the development of the Censorship-Industrial Complex.

Throughout the Covid period, the federal government collaborated with and pressured social media companies to control information about vaccines, lockdowns, treatments, masks, and other 'public health' measures. Documents revealed by the Twitter Files, *Murthy v. Missouri*, and investigations from the House Select Subcommittee on the Weaponization of Government revealed that CISA officials were in regular contact with social media companies via shared content-flagging platforms, in which companies were urged to remove or flag content that contradicted official public health guidance. Senior officials in the Executive Office of the President, including White House Senior Advisor for the Covid response Andy Slavitt and White House Director of Digital Strategy Rob Flaherty, also directly pressured these corporations to remove even content described by the platforms as "often-true." This led to accusations that the government was pressuring social media companies to suppress free speech, particularly content critical of the government's pandemic response or expressing vaccine skepticism.

As described above, CISA shifted some of its operations to a Stanford University-run entity to act on its behalf so as to "avoid the appearance of government propaganda" after CISA and the Biden Administration were sued in federal court, implicitly acknowledging that these censorship activities were unconstitutional. CISA subsequently scrubbed its website of references to its domestic surveillance and censorship activities.

While the Supreme Court ruled 6-3 in June 2024 that the plaintiffs in *Murthy v. Missouri* did not have legal standing to block Biden Administration officials from communicating with social media companies, the justices notably declined to opine on the merits of the case's First Amendment claim. However, in August 2024, a very similar lawsuit filed by Robert F. Kennedy Jr. (*Kennedy v. Biden*) prevailed on the standing question in U.S. district court and is now proceeding.

While the policies suggested in the "General Reforms" section will help to stop many of these abuses, reforms targeting the most egregious censorship offenders will provide an extra layer of protection. To put an end to these egregious breaches of constitutional constraints, the new administration could:

1) Conduct an audit of all funding provided to NGOs, universities, think tanks or other contractors that engaged in combating pandemic-related MDM, including a detailed list of all content that was removed.

2) Place a five-year ban on receipt of any further federal funding for any nonprofit, think tank or university initiative found to have suppressed or coerced lawful speech.

3) Implement an Executive Order banning the NIH, CISA, NSF, CDC, or any other federal agency from providing grant funding or any other material support to governmental and nongovernmental initiatives, projects, or research relating to misinformation or disinformation.

4) Implement an Executive Order banning all federal agencies and employees not under HHS or the Department of Agriculture (USDA) from developing, funding, or materially supporting any programs, policies, statements, regulations, or guidance documents relating in any way to human health.

5) Direct the Inspector General of HHS to issue a report detailing all health-related misinformation it has disseminated online since 2019, and the Inspector Generals of HHS and DHS to issue a report detailing all instances in which either agency directly or indirectly potentially violated the civil liberties of American citizens during the same period.

Protecting Children while Resisting Scope Creep

One of the most daunting challenges in online policymaking is protecting children from Internet-based harms while safeguarding free speech. Children face various forms of harm from Internet use, including exposure to violent and sexually explicit material, and cyberbullying, where peers or strangers harass or embarrass them online, which can lead to anxiety, depression, and low self-esteem. Data privacy concerns are also mounting, as tech companies increasingly collect and monetize children's personal information, which can be misused for targeted advertising or put them at risk of exploitation by online predators.

Children and adults alike are also increasingly developing Internet addiction, where excessive screen time interferes with circadian rhythms, academic performance, and social interactions, contributing to long-term issues in cognitive and social development. Children and teens are particularly vulnerable to exploitation by algorithms designed to maximize engagement. Many existing regulations, such as the Children's Online Privacy Protection Act (COPPA), were enacted before the rise of platforms like TikTok and Instagram, which makes them outdated in addressing today's complex online environment. Policymakers across the political spectrum have acknowledged that the U.S. needs new laws to protect children online due to the increasing risks they face in the digital world. These new laws could enhance data privacy protections by limiting the collection and sale of children's personal information, requiring platforms to clearly inform parents about data usage, and giving children and parents more control over their digital footprint. Dozens of states have introduced and passed legislation to tackle this issue from several angles, such as limiting the use of manipulative algorithms, though many of these efforts have been met with legal resistance from social media companies and pornography websites.

However, many public policies designed to protect children risk overreaching into the adult world. Free speech advocates should always remain aware of the risk that such actions can become Trojan Horses that may amplify surveillance and other restrictions that would otherwise be difficult to pass. The Kids Online Safety Act (KOSA), originally introduced in 2022, was described by the Electronic Frontier Foundation as "fundamentally a censorship bill" for compelling even the smallest online forums to remove content that may cause "anxiety." Normalizing this sort of subjective, Internet-wide content-sanitization under the benevolent-sounding banner of protecting children is a dangerous heading. As such we propose the Executive Branch move to urge a new approach to the question of Internet content consumption by minors.

Empowering Parents Through Effective Digital Safety Control Standards

We believe that parents should be empowered to make the best decisions for their children, with any government regulation tailored towards that goal. This philosophy often results in proposals or policies where social media platforms and Internet Service Providers (ISPs) are compelled to provide easy-to-use tools so parents, schools, and local libraries can best shape the settings and experiences they require. However, any age verification requirements should not infringe on the privacy rights of adults, and platforms should make sure that configurations can be easily modified and understood by parents or guardians, as well as schools and other community institutions, which provide children with access to the Internet. Any requirements to provide ID to a platform should be entirely voluntary, and not government mandated.

For this solution to work, parents must be empowered with tools that genuinely allow them to manage their minor children's digital lives. This is not something the tech industry will likely ever do voluntarily; their track record speaks for itself. After over a decade of testing various tools, it's clear that existing parental controls are inadequate and the industry's current solutions ineffective. Therefore, the next administration should legislate a straightforward mandate that tackles the problem at the level of the operating system (OS), making obsolete the clunky "Are you 18?" checkboxes that are universally ignored. With the following proposals, responsibility can be shifted upstream to OS providers, websites, and app developers ensuring consistency and minimal burden on app and website developers:

1) OS providers must make age configuration an integral part of their systems, allowing parents to input their child's age.
2) Web browsers must allow the option for guardians to transmit age as an HTTP header for all requests, when set.
3) Seamless Access for Developers: Apps and online apps must retrieve the age data directly from the OS, requiring no extra effort from parents or guardians once set.

This framework ensures that parents have meaningful control while the underlying mechanism is universally enforced and simple for developers to implement. It also gives parents the freedom to be less strict with age requirements if they deem fit for the needs and capabilities of a particular child. When a parent sets up a device, they will input the child's age into the OS: from then on, web browsers include the age in an HTTP header for every request, and apps can query the OS to retrieve the age dynamically.

This proposal tackles online dangers like pornography, predatory content, and unregulated social media in one sweep without compromising online anonymity. Instead of relying on intrusive and error-prone verification systems, this solution empowers parents to make decisions for their own children while leaving the rest of the Internet untouched. By focusing on OS level implementation, the solution is efficient, scalable, and preserves the freedom of developers and users alike. Importantly, it empowers parents, and everyone remains anonymous. The only significant task lies with the OS vendors; once the infrastructure is in place, everyone else benefits from its simplicity.

In addition to OS-level reforms, to protect free speech while simultaneously building a safer and more transparent online environment for children, 'Trojan Horse' measures that could one day be used for surveillance or control of adults should be avoided. The new administration could:

4) Pursue policies that would prevent deployment of any form of digital identification requirements for Internet access.

5) Urge Congress to amend the COPPA to extend its protections to children under the age of 18 (from the current age of 13), and to prohibit online platforms from collecting information from a child using the "constructive knowledge" standard. Practically, this would prohibit platforms from collecting information from a user reasonably assumed to be underage, instead of the currently used "actual knowledge" standard which is narrower in scope.

6) Consider urging Congress to pass a federal law similar to those introduced in at least 29 states and adopted in 11, which would require parental consent for minors to use social media.

Realigning U.S. Foreign Influence Efforts

A variety of U.S. agencies, including the State Department and USAID, have supported a range of international initiatives to "counter mis-and-disinformation" that have promoted censorship abroad and, in some cases, have been used as workarounds to censor American citizens. These initiatives provide funding for staff, technology, and training programs to governments, consultancies, academia, and NGOs.

The federal government has supported a host of organizations including the Atlantic Council, Meedan, Graphika, Countering Disinformation, Polygraph, the Alliance for Securing Democracy, the GDI, the Institute for Strategic Dialogue (ISD), and many, many more. For example the State Department's GEC- funded GDI produced a "dynamic exclusion list" of media outlets that allegedly traffic in "disinformation" with the aim of starving those outlets of advertisers. This list included several legitimate media publications whose primary transgression appears to have been straying from elite consensus opinion.

A recent investigation from Civilization Works found that "several U.S. entities were directly and indirectly involved in Brazil's Censorship Industrial Complex," which included coordination with Supreme Court Justice Alexandre de Moraes on campaigns to censor and shutdown Twitter and Telegram and to interfere in Brazil's 2022 presidential election. These organizations included the Atlantic Council's Digital Forensic Research Lab (DFRLab), the Central Intelligence Agency (CIA), FBI, CISA, NSF, DOS, USAID, the National Endowment for Democracy (NED), the Wilson Center, the George Washington University, the White House, and others.

U.S. government agencies have worked in close collaboration with other governments to advance a censorship agenda, particularly in collaboration with Five Eyes partners. In September 2024, a memo obtained by the campaign group Big Brother Watch under freedom of information laws detailed an August 10, 2021 domestic censorship strategy meeting between the United Kingdom's "Counter Disinformation Unit (CDU) and the Biden-Harris National Security Council (NSC) Interagency Policy Committee (IPC). Attendees included high-level staff from the White House, the NSC, the Office of the Director of National Intelligence (ODNI), CIA, FBI, the Departments of State, Treasury, Defense, Homeland Security, and Health and Human Services, as well as USAID, U.S. Agency for Global Media (USAGM), and high-ranking officers in the Army, Navy, and Air Force."

At this meeting, the CDU outlined how they had been mediating the civil information flows of the British public and described how governments worldwide were working together to challenge traditional free speech paradigms. The Biden-Harris NSC subsequently invited the British government to share its censorship strategies, recommending the creation of a dedicated hub to lead government-wide efforts, passing legislation to coerce social media companies, and enlisting the DOS to partner with foreign allies and multilateral institutions to coordinate the global censorship agenda.

Worse, a Reuters report revealed that the Pentagon produced a disinformation campaign targeted at the Philippines to undermine uptake of China's Sinovac vaccine.

In addition to violating the universal human right of free expression and the sovereignty of many foreign nations, these types of U.S. global influence operations are harmful to American interests in the long-run. Once exposed, these operations erode trust, goodwill, and open dialogue among nations that is so critical to maintaining peace and stability. In order to roll back this dangerous global bureaucratic encroachment, promote national sovereignty and dignity, and re-build healthy relationships with the world, the new administration could:

1) Direct a rigorous audit of all international activities funded by the federal government to ensure they are neither promoting censorship at home or abroad, and that all such activities adhere to the Article 19 of the Universal Declaration of Human Rights. Any organization found to have violated the spirit of Article 19 should be barred from any future federal government funding.

2) In the same vein, conduct a full audit of all Five Eye coordination to ensure U.S. intelligence agencies are neither importing, nor exporting censorship tools and strategies targeting legal speech.

3) Urge Congress to pass HR 9850, the *No Funding or Enforcement of Censorship Abroad Act*, which would:

    a) Cut off U.S. foreign assistance to any entities that promote censorship of lawful speech (Except in instances of immediate public corporeal safety or defamation, for example.);

    b) Allow the U.S. Attorney General to prohibit U.S. law enforcement cooperation with foreign government censorship directives against Internet companies headquartered in the U.S.; and,

    c) Prohibit U.S. law enforcement agencies from cooperating with foreign countries to promote censorship against speech that would otherwise be protected if the speaker was located in the U.S.

4) Implement an Executive Order to audit and immediately halt all federal funding to foreign government efforts to control journalism, manage social media content, or remove misinformation and/or disinformation, and halt funding to any similar activities run by groups such as the GDI, the Atlantic Council's DFRLab, the NED, or the National Democratic Institute (NDI).

5) Implement an Executive Order to audit and, if either is found to be currently operating programs to control or interfere with U.S. media or the speech of American citizens, immediately terminate the State Department's GEC and USAID's Global Elections and Political Transitions (GEPT) Program.

6) Implement an Executive Order requiring the public disclosure of all GEC-funded programs, both internal and external, as well as any other federal funding of programs to explicitly counter "misinformation," "disinformation" or "hate speech."

7) Implement an Executive Order requiring the State Department, CDC, NSC, ODNI, and FBI to immediately de-classify, fully un-redact, and make public all documents, meetings, calendars, and communications relating to censorship, misinformation, and disinformation campaigns that any of its staff may have been involved in since 2012.

Personnel and Political Appointments

The old cliche is worth repeating: personnel is policy. The best efforts and intentions of any administration can be easily thwarted by the poor selection of appointees or by retaining appointees from a previous opposing administration. In order to quickly turn the gargantuan ship of state toward free speech, the new administration must give the highest priority to expeditiously turning over executive branch positions to appointees willing to protect the First Amendment and uncover and dismantle the government censorship apparatus.

To that end, we have prepared a list of political appointments scattered throughout the federal bureaucracy that could in any way influence digital free speech. These positions were listed in the 2020 Plum Book. Working under the assumption that most, if not all high and cabinet-level positions (along with Inspectors General, their direct reports and office staff) will be filled quickly, this list is intended to highlight positions crucial to digital freedom of speech that may not be as rapidly filled or may be overlooked during the initial stages of a new administration. While this document focuses on executive branch strategy and does not outline a strategy for federal judicial appointments and U.S. attorneys, we believe all Senate-confirmed judicial candidates should pass a "free speech test."

Likewise, an administration which seeks to prioritize free speech should focus on filling at least the following critical offices with aligned individuals who understand the importance of this particularly American value and the risks at stake:

- Executive Office of the President
    - White House Office of Digital Strategy: all positions
    - Office of Science and Technology Policy: Director; Assistant to the President for Science and Technology; Associate Director, National Security and International Affairs
    - Office of Management and Budget
        - Associate Director, General Government Programs/Transportation, Homeland Security, Justice Services
- Department of Homeland Security
    - Office of the Secretary: White House Liaison
    - Office of the General Counsel: Associate General Counsel for Technology Programs
    - Office of Policy, Strategy, and Plans: Assistant Secretary for Cyber, Infrastructure, Risk, and Resilience

    - Cybersecurity and Infrastructure Security Agency: all 18 positions
    - Science and Technology Directorate: Deputy Under Secretary for Science and Technology
- Department of Health and Human Services
    - Office of General Counsel:
        - Deputy Associate General Counsel for Public Health (National Institutes of Health); Deputy Program Integrity
    - National Institutes of Health (all 11 positions)
- Department of Justice
    - Office of Privacy and Civil Liberties: Director
    - Office of the Associate Attorney General: Director, Constitutional and Specialized Tort Litigation Section
    - Federal Bureau of Investigation: Director
- Department of State
    - Office of Civil Rights: Director
    - Office of the Legal Advisor: Legal Advisor
    - Bureau of Global Public Affairs: Assistant Secretary of State (Public Affairs); Deputy Assistant Secretary for Digital Strategy
    - Office of the Under Secretary for Civilian Security, Democracy, and Human Rights; all 8 positions
- Department of Commerce
    - National Telecommunications and Information Administration; all three positions
- National Science Foundation
    - Office of the Director: Director; Deputy Director; Senior Advisor to the Director for Strategic Initiatives; Chief of Staff; Chief of Research Security Strategy and Policy
    - Office of Advanced Cyberinfrastructure: Office Director
- Federal Communications Commission
    - Public Safety and Homeland Security Bureau: Chief; Deputy Chief
- Federal Trade Commission
    - Bureau of Competition: Director; Assistant Director for Technology Enforcement
    - Bureau of Consumer Protection: Associate Director for Privacy and Identity Protection
- U.S. Agency for Global Media
    - Chief Executive Officer; Chief Strategy Officer, Director, Office of Technology Services and Innovation

Appendix: List of Federal Censorship and Speech-Related Legislation 2019-Present

Of the many thousands of bills introduced during each congressional session, only a few ever become law. It is not uncommon for members of Congress to re-introduce the same bill year after year, particularly if it relates to an issue that is of particular importance for them. The following bills, or sections of them, could serve as models for the new administration and Congress as they develop their policy priorities. Many of these bills are referenced in the relevant sections of this paper.

Of these bills, Rep. Jim Jordan's Free Speech Protection Act is perhaps the most comprehensive, while Rep. James Comer's Protecting Speech from Government Interference Act of 2023 is the only one which has successfully passed a floor vote. Although none of these bills have yet become law, it is certainly possible that future versions may be more successful.

The list below includes Democrat and Republican-sponsored House and Senate bills related to protecting children, promoting free speech, and preventing government and social media censorship. It is not intended to be comprehensive. Bills are listed in reverse chronological order.

H.R. 1233- To prohibit the obligation or expenditure of Federal funds for disinformation research grants. Rep. Thomas Massie [R-KY]. Introduced 02/12/2025. 11 Republican co-sponsors.

No federal funds may be obligated or expended by any federal department or agency for: Disinformation research grants, Secure and Trustworthy Cyberspace grants, or Programs within the National Science Foundation's Track F: Trust and Authenticity in Communications Systems.

H.R. 9850- The No Funding or Enforcement of Censorship Abroad Act of 2024. Rep. Christopher Smith [R-NJ-4]. Introduced 09/25/2024. Two Republican co-sponsors (Rep. Jim Jordan and Rep. Maria Salazar).

This bill would cut off U.S. foreign assistance to any entities that promote censorship and prohibit U.S. law enforcement agencies from cooperating with foreign countries to promote censorship against speech that would otherwise be protected if the speaker was located in the U.S.

H.R.9605 - The No Censors on our Shores Act of 2024. Rep. Darrell Issa [R-CA-48] Introduced 09/16/2024. One Republican co-sponsor (Rep. Maria Salazar).

This bill would provide that any foreign government official who engages in censorship of American speech is inadmissible and deportable.

H.R.8838 - Free Speech Defense Act of 2024. Rep. Andrew Clyde. [R-GA-9] Introduced 06/26/2024. One Republican co-sponsor (Rep. Byron Donalds).

This bill prohibits agencies from directing or encouraging social media companies to remove users, label content as misinformation, or share user data, except in specific cases like criminal investigations or threats to public safety (e.g.: human trafficking, child exploitation). The law also prohibits public-private partnerships where agencies collaborate with social media companies to monitor content, except in emergencies. Moreover, federal funding cannot support censorship-related activities, and agencies cannot accept free or discounted social media advertising. Federal employees who violate these rules are subject to fines or imprisonment. Additionally, individuals affected by agency actions under this law can file civil suits against the U.S. government. Lastly, the Attorney General must report on compliance annually.

H.R.4848 - Censorship Accountability Act of 2023. Rep. Dan Bishop [R-NC-8]. Introduced 07/25/2023. Reported favorably by the Committee on Judiciary in July 2024. 38 Republican co-sponsors.

This bill establishes a right of action against Federal employees for violations of First Amendment rights. A Federal employee who, under color of any statute, ordinance, regulation, custom, or usage, of the United States, subjects, or causes to be subjected, any citizen of the United States or any person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the First Amendment, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress.

H.R.4791 - Free Speech Protection Act. Rep. Jim Jordan [R-OH-4]. Introduced 07/20/2023. 19 Republican co-sponsors. In committee.

Definitions (Sec. 2):

- **Covered Information:** Includes various forms of personal and communication data such as phone calls, digital messages, location data, and user demographics.
- **Covered Platform:** Refers to interactive computer services and media organizations disseminating information.
- **Employee:** Defined broadly to include federal agency employees and contractors.

- **Executive Agency:** Defined according to federal law, including the Executive Office of the President.
- **Provider:** Refers to those operating covered platforms.

Findings (Sec. 3):

Congress affirms the First Amendment's protection of free speech, emphasizing its role in liberty and government accountability. Citing historical legal precedents, it highlights concerns about government overreach in censoring speech, particularly during recent events like the covid-19 pandemic and the 2020 election.

Employee Prohibitions (Sec. 4):

Without a warrant issued by a federal or state court, federal employees and contractors cannot use their positions to directly or indirectly influence covered platforms to:

- Censor, suppress or label as misinformation protected speech;
- Remove users;
- Block, ban, delete, deprioritize, demonetize, deboost, limiting the reach of, or restrict access to the speech;
- Enter into a partnership with a provider to monitor any content disseminated on the applicable covered platform;
- Solicit, accept, or enter into a contract or other agreement (including a no-cost agreement) for free advertising or another promotion on a covered platform; and,
- Direct or encourage a provider to share with an Executive agency covered information containing data or information regarding a particular topic, or a user or group of users on the applicable covered platform, including any covered information shared or stored by users on the covered platform.

Violations can lead to severe penalties, including fines and job loss, with affected individuals eligible to sue for damages. The bill creates a private right of action for citizens to bring suit in the United States District court for the District of Columbia for reasonable attorneys' fees, injunctive relief, and actual damages federal contractors are included, and can be barred from receiving further federal contracts if found to be in violation.

Reporting Requirements (Sec. 5):

Requires that executive agencies must report communications with providers related to censorship every 90 days, ensuring transparency and accountability.

CISA Report (Sec. 6):

Requires the Secretary of Homeland Security to submit a report to the Director and the chair and ranking member of the Senate Committee on Homeland Security and Governmental Affairs, and the House Committee on Oversight and Accountability. The report must disclose any actions by Cybersecurity and Infrastructure Security Agency (CISA) employees that occurred from November 16, 2018 until the enactment of this Act,and would have been in violation of the Act.

Disinformation Governance Board (Sec. 7):

Terminates the Disinformation Governance Board and prohibits federal funding for similar entities.

Grants and Misinformation (Sec. 8-9):

Prohibits federal agencies from awarding grants for misinformation programs, requiring grant recipients to certify they will not label news creators as misinformation sources.

Presidential Powers (Sec. 10):

Amends the Communications Act of 1934 by striking sections that create presidential war powers relating to the "rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations within the jurisdiction of the United States as prescribed by the FCC [Federal Communications Commission]."

FOIA Applicability (Sec. 11):

Enhances transparency by allowing public access to records of communications between agency employees and providers, with specific protections for user identities. This section overrides sections of the Freedom Of Information Act (FOIA) statute that allow agencies to withhold certain information from requests, saying "any request made to an agency pursuant to that section for records relating to communication between an employee and a representative of a provide shall be granted by the agency without regard to any exemption" in the FOIA statute. However, the release of identifiable information without the user's permission, and instances where a warrant has been issued, remain exempt from the changes in this bill.

S.1672 - Disclose Government Censorship Act of 2023. Sen. Bill Hagerty [R-TN]. Introduced 05/18/2023. In committee. Eight Republican co-sponsors.

This bill requires officers and employees of the legislative and executive branches to disclose communications with providers of interactive computer services (e.g.: Internet Service Providers) regarding restricting speech. The disclosure must be made within seven days of the date on which the communication is made.

Specifically, executive and legislative branch officers and employees must disclose their communications with a provider or operator of an interactive computer service regarding action to restrict access to material posted by another information content provider. The bill makes exceptions for legitimate law enforcement and national security purposes and establishes penalties for violations.

H.R.140 - Protecting Speech from Government Interference Act of 2023. Rep. James Comer [R-KY-1]. Introduced 01/09/2023. 16 Republican co-sponsors. Passed House on party-line vote on March 3, 2023 and sent to the Senate.

This bill generally prohibits federal employees from censoring the speech of others while acting in an official capacity. Specifically, the bill prohibits employees of executive agencies or who are otherwise in the competitive service from (1) using their official authority to censor a private entity; or (2) engaging in censorship of a private entity while on duty, wearing a uniform, or using official government property. The bill provides certain exceptions for law enforcement, subject to specified reporting requirements.

Employees are subject to disciplinary action, civil penalties, or both for violations.

The bill defines censor or censorship to mean influencing or coercing, or directing another to influence or coerce, for the removal of lawful speech, the addition of disclaimers, or the restriction of access with respect to any interactive computer service (e.g.: social media).

S.797 - PACT Act of 2021. Sen. Brian Schatz [D-HI]. Introduced 03/17/2021. Seven co-sponsors, four Republican, three Democrat. Died in Committee.

Platform Accountability and Consumer Transparency Act or the PACT Act. This bill requires providers of interactive computer services (e.g.: social media companies) to publish their policy explaining the types of content permissible on the service and provide a system for users to submit complaints about content that may violate the policy or involve illegal content.

Additionally, social media companies must establish a process for removing certain content that violates their policies and notifying the information content provider about the removal, including a mechanism to appeal the removal. Social media companies also must publish a report every six months that details the instances in which the company took action with respect to content, including removing content, deprioritizing content, and suspending content provider accounts. The bill removes certain liability protections for companies if the company has actual knowledge of illegal content on its service and does not remove it within specified time frames. The bill provides for enforcement of these requirements by the Federal Trade Commission.

SB 299: SAFE TECH Act of 2021. Sen. Mark Warner [D-VA]. Introduced 02/08/2021. Four Democrat co-sponsors. Died in committee.

This bill limits federal liability protection that applies to a user or provider of an interactive computer service (e.g.: a social media company) for claims related to content provided by third parties. Specifically, the bill applies the liability protection to claims arising from third-party speech rather than third-party information. Additionally, the liability protection shall not apply if a user or provider (1) accepts payment to make the speech available, or (2) creates or funds (in whole or in part) the speech.

The bill changes legal procedures concerning the liability protection by (1) requiring a defendant in a lawsuit to raise the liability protection as an affirmative defense, and (2) placing the burden of proving that the defense applies on the defendant. Some courts have held that the current liability protection bars claims for civil penalties and injunctive relief. The bill expressly excludes from the liability protection requests for injunctive relief arising from a provider's failure to remove, restrict access to, or prevent dissemination of material likely to cause irreparable harm. However, the bill protects a provider from liability for actions taken to comply with such injunctions. Under current law, the liability protection does not apply to federal criminal law, intellectual property law, and other designated areas of law. The bill further specifies that the liability protection shall not apply to civil rights law; antitrust law; stalking, harassment, or intimidation laws; international human rights law; and civil actions for wrongful death.

H.R.8636 - Protecting Americans from Dangerous Algorithms Act of 2020. Rep. Tom Malinowski [D-NJ-7]. Introduced 10/20/2020. One Democrat co-sponsor (Rep. Anna Eshoo). Died in committee.

This bill limits a social media company's Section 230 immunity from liability if it promotes certain content on its platform. Specifically, the bill removes this immunity from a social media company with more than 50 million monthly users if it utilizes an algorithm, model, or other computational process to amplify or recommend content to a user that is directly relevant to a claim involving (1) interference with civil rights, (2) neglect to prevent interference with civil rights, or (3) acts of international terrorism.

S.4534 - Online Freedom and Viewpoint Diversity Act of 2020. Sen. Roger Wicker [R-MS]. Introduced 09/08/2020. Two Republican co-sponsors (Sens. Graham and Blackburn). Died in committee.

This bill limits the immunity of a provider or user of an interactive computer service (i.e.: social media platform) for screening and blocking offensive material on the service's platform. It revises the applicability of civil liability for this moderation of offensive material, and changes a definition that governs applicability of the immunity. Under current law, this immunity protects a provider or user of a social media platform from being treated as the publisher or speaker of information provided by another information content provider.

The bill removes this immunity from a decision, agreement, or action by a provider or user of a social media platform to restrict access to or availability of material provided by another information content provider. To avoid liability for this conduct, in addition to acting in good faith, the bill requires that the actor must have an objectively reasonable belief that the material is obscene, lewd, lascivious, filthy, excessively violent, harassing, promoting self-harm, promoting terrorism, or unlawful. Currently, a good faith actor must only consider such material to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.

Further, the bill redefines *"information content provider"* to encompass any person who editorializes or affirmatively and substantively modifies the content of another person or entity.

H.R.7808 - Stop the Censorship Act of 2020. Rep. Paul Gosar [R-AZ-4]. Introduced 07/29/2020. 23 co-sponsors: 22 Republican, one Democrat (Rep. Tulsi Gabbard). Died in committee.

This bill modifies a social media company's immunity from liability for screening and blocking offensive content on its platform. Under current law, the immunity applies for action taken to restrict content that is obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable. The bill eliminates immunity for restricting content that is otherwise objectionable and applies such immunity when a company restricts content that is unlawful or that promotes violence or terrorism. Under current law, such immunity also applies to actions taken to enable or make available the technical means to restrict access to such content. The bill applies this immunity to actions taken that provide users with the option to restrict access to any material, regardless of whether such material is constitutionally protected.

S.4062 - Stopping Big Tech's Censorship Act of 2020. Sen. Kelly Loeffler [R-GA]. Introduced 06/24/2020. No co-sponsors. Died in committee.

This bill modifies the requirements that providers and users of interactive computer services (e.g.: social media companies) must meet in order to qualify for certain liability protections. Specifically, in order to be exempt from being treated as the publisher or speaker of any information published by a third-party information content provider, a provider or user of an interactive computer service must take reasonable steps to prevent or address the unlawful use of such service or unlawful publication of information on the service.

Furthermore, the bill removes the protection against civil liability for a provider or user of an interactive computer service that voluntarily takes action in good faith to restrict access to or availability of certain offensive material, unless such action meets specified First Amendment requirements.

Lastly, to be eligible for protection from liability for information published by a third-party information content provider, a provider or user of an interactive computer service must meet certain notice requirements.

S.1914: Ending Support for Internet Censorship Act of 2019. Sen. Josh Hawley [R-MO]. Introduced 06/19/2019. No co-sponsors. Died in committee.

This bill prohibits a large social media company from moderating information on its platform from a politically biased standpoint.

Under current law, a social media company is generally immune from liability with respect to content posted on its platform by users and other content providers. However, the bill removes this statutory immunity unless the social media company obtains certification from the Federal Trade Commission that it does not moderate information on its platform in a manner that is biased against a political party, candidate, or viewpoint.

About liber-net

liber-net combats the emerging trend of digital authoritarianism and works to reestablish free speech and civil liberties as the norm for our networked age. Through journalism, research, media production, network-building, and campaigning, liber-net provides a platform to create alliances, expose civil society corruption, and foster open conversations.

We are driven by the urgent need to reject digital authoritarianism, and are committed to promoting human autonomy, dignity, and pluralism. We oppose systems of online censorship, their growing social acquiescence, and the accelerating surveillance regimes operating in and through information technology. The liber-net team comes from the progressive digital rights and public policy field, with decades of combined experience. We have a deep understanding of these issues and are working to connect with the many disaffected advocates in this space.

liber-net

𝕏 @liber_net   in liber-net   🌐 liber-net.org