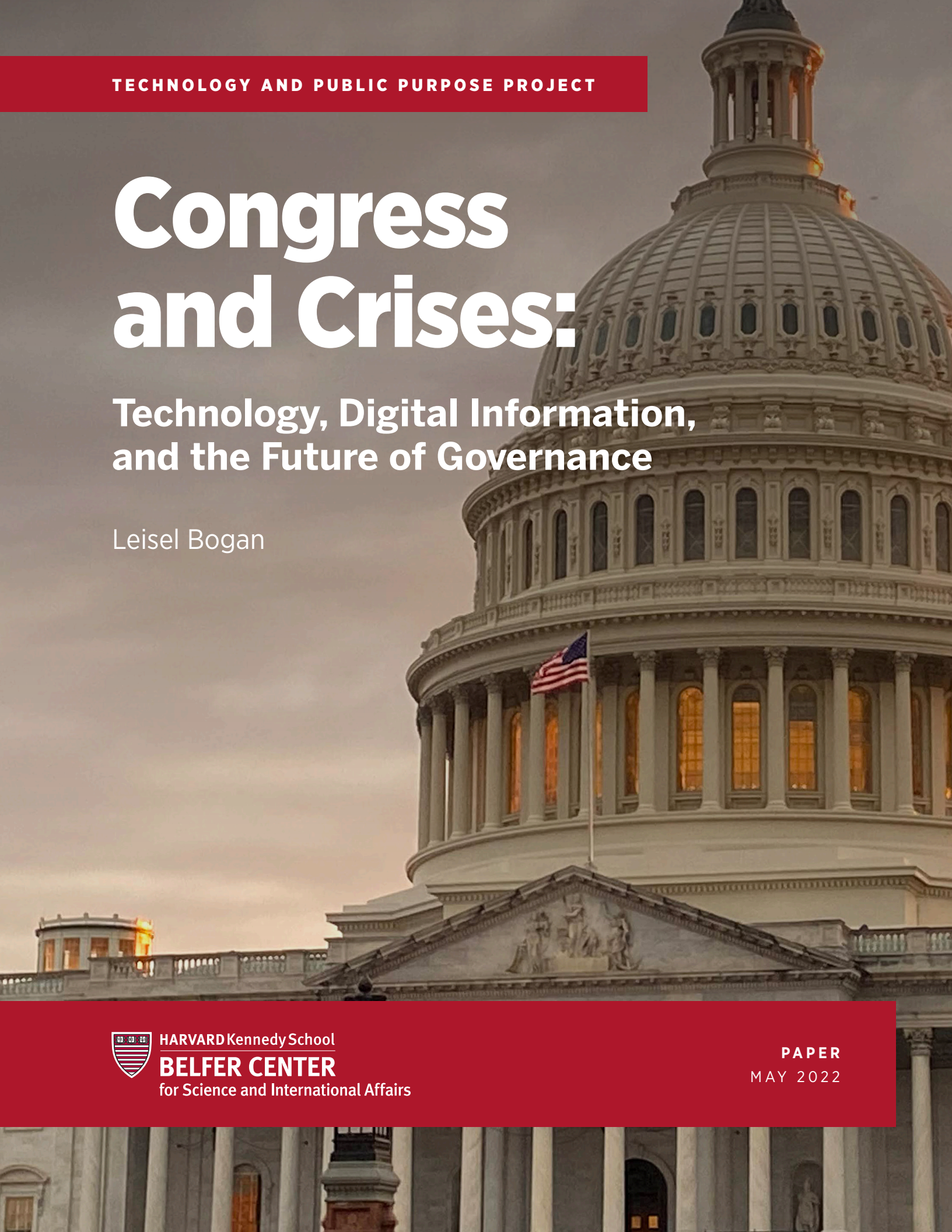


TECHNOLOGY AND PUBLIC PURPOSE PROJECT

# Congress and Crises:

## Technology, Digital Information, and the Future of Governance

Leisel Bogan

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
MAY 2022

**Technology and Public Purpose Project**
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

belfercenter.org/project/technology-and-public-purpose

TECHNOLOGY AND PUBLIC PURPOSE PROJECT

# Congress and Crises:

## Technology, Digital Information, and the Future of Governance

Leisel Bogan

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
MAY 2022

# About the Technology and Public Purpose Project (TAPP)

**The arc of innovative progress has reached an inflection point. It is our responsibility to ensure it bends towards public good.**

Technological change has brought immeasurable benefits to billions through improved health, productivity, and convenience. Yet as recent events have shown, unless we actively manage their risks to society, new technologies may also bring unforeseen destructive consequences.

Making technological change positive for all is the critical challenge of our time. We ourselves — not only the logic of discovery and market forces — must manage it. To create a future where technology serves humanity as a whole and where public purpose drives innovation, we need a new approach.

Founded by Belfer Center Director, MIT Innovation Fellow, and former U.S. Secretary of Defense Ash Carter, the TAPP Project works to ensure that emerging technologies are developed and managed in ways that serve the overall public good.

TAPP Project Principles:

1. Technology's advance is inevitable, and it often brings with it much progress for some. Yet, progress for all is not guaranteed. We have an obligation to foresee the dilemmas presented by emerging technology and to generate solutions to them.

2. There is no silver bullet; effective solutions to technology-induced public dilemmas require a mix of government regulation and tech-sector self-governance. The right mix can only result from strong and trusted linkages between the tech sector and government.

3. Ensuring a future where public purpose drives innovation requires the next generation of tech leaders to act; we must train and inspire them to implement sustainable solutions and carry the torch.

# About the Author

**Leisel Bogan** is a Fellow in the Technology and Public Purpose program at the Harvard Kennedy School's Belfer Center for Science and International Affairs. Before joining the TAPP Fellowship, she led the first Congressional Digital Service pilot fellowship for TechCongress within the House Select Committee on Modernization, which resulted in the recent creation of a permanent House Digital Services organization. Prior to her current role, she served as the Senior Fellow for Cybersecurity, Technology and National Security in the office of Senator Mark Warner. Before Congress, she focused on global strategy for cybersecurity and technology transformation at the professional services firm, PwC. She has held two academic appointments at Stanford University where she researched cybersecurity and emerging technologies, national security, and international institutions, and exhibited work at the International Criminal Court. She has worked at Palantir Technologies and in new media technologies at Warner Bros. Entertainment, and served as former Secretary of State Condoleezza Rice's Chief of Staff and her director of research at Stanford University. At the geopolitical consulting firm, RiceHadleyGates, LLC, she advised clients on technology, strategy and emerging markets. Her work has taken her throughout the EU, the Southern Caucasus, Asia, and MENA. She has written for various publications and has spoken at a DEFCON village, for the National Academy of Sciences, and has guest lectured at Georgetown University, Pepperdine University, and Penn State Law. She studied at the University of San Francisco's School of Law, holds a graduate degree from Pepperdine University, and graduated Magna Cum Laude from California State University. She was a Term Member at the Council on Foreign Relations and a 2016 Gabr Foundation Fellow. She has volunteered and worked for organizations that help vulnerable populations, especially children. She began her career at age five in television and print advertising.

# Acknowledgments

This research would not have been possible without Beth Cartier, and the incredible and generous support of Karen Ejiofor, Amritha Jayanti, and Secretary Ash Carter.

Many thanks to the entire Technology and Public Purpose team, including Henry Kaempf, John Schultz, Ariel Higushi, former TAPP director, Laura Manley and the other TAPP Fellows whose insights and support are deeply appreciated.

Thank you also to Professor Marshall Ganz and Eric Rosenbach for their wonderful support.

Thank you to the many current and former government officials, Congressional staffers, members, and experts who are not named, but whose thoughts, work, expertise, and dedication during recent crises greatly contributed to this effort as well as to my experiences and work on the Hill.

I am especially grateful to my former office in the Senate, who have long been the experts in this space, and whose brilliant work taught me so much, and to my former office in the House, who continue to do such important work.

Thank you to the incredible work of the many veterans, service members, volunteers, and organizations who supported the U.S. evacuation of Afghanistan and continue to support vulnerable allies and friends all over the world.

Many thanks for the great work and thoughtful insights from former Representative Brian Baird, Professor Andrea Matwyshyn, and Professor Herb Lin.

Many thanks to Ishan Mehta, Anna Lenhart, Eleanor Tursman, and Victoria Houed, and to my former colleagues and experts at TechCongress, Travis Moore, Brooke Hunter, Aleena Khan, Marley Rafson, B Cavello, James Gimbi, Mike Wacker, John Yaros, Katya Sedova, and Marissa Gerchick.

Many thanks to Charlotte Day, Ryan Castellucci, Russell Wald, Aysha Chowdhry, Heather Fischer, Wes Mullins, Courtney Lam, Sohum Pawar, Marilyn Stanley, Shannon York, Devika Daga and Nathan Pao for your wisdom, support, and insights.

I am also grateful to my research assistants, Nitin Kumar and Anna Ortez-Rivera, for your support, thoughts, and contributions.

None of the individuals are responsible for the contents of this report and any errors and misjudgments are the responsibility of the author.

# Table of Contents

# Introduction

The 116th Congress began in 2019 with what would become the longest government shutdown in history, and it would end just three days shy of an unprecedented violent attack on the Capitol building during the first week of the 117th Congress. Now, just a few months into the second year of the 117th Congress, the world hovers closer to nuclear war than it has since the Cuban Missile Crisis in 1962.

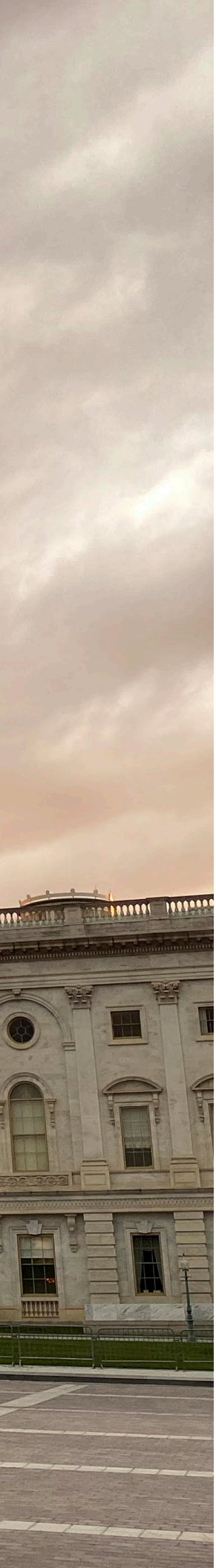
Throughout the 116th and 117th Congresses, the United States government faced a swell of domestic and global challenges, underpinned by what was dubbed in 2016 as a "post-truth" information era. During that period, Congress dealt with a range of crises including a global pandemic and the corresponding economic, and social fallout; a justice crisis and public outcry following the murder of George Floyd; a governance and legitimacy crisis as a result of the digital information crisis; a precipitous escalation of hostilities between the United States and Iran; two Presidential impeachment hearings; a violent and deadly attack on its own Capitol building; a chaotic withdrawal from Afghanistan; and the unprovoked Russian assault and invasion of Ukraine.

Technology and information played a key role in how the crises unfolded, how they were managed and addressed, and how the public was engaged and informed. During both Congresses, information and information communication technologies either facilitated or hindered the government's ability to define or respond to what was happening during the emergency. They continue to play a critical role in how Congress addresses crises, national security, and societal harms involving technology.

Although U.S. and western international institutions have successfully weathered recent challenges, the stress tests of recent years have magnified weaknesses across the U.S. government, our democratic institutions, and in particular, our technology infrastructure. This report provides 1) a brief overview of some of the recent crises Congress has faced, and the role technology played in those events, 2) Congress' historical and recent responses to disinformation, and 3) provides suggestions for a new agency

to help address some of the governance and societal challenges aggravated by the crises and the current information environment.

Toward the end of his long life, former United States Secretary of State George Shultz repeatedly warned that the United States was on a "hinge of history" much like the post-WWII era. He noted that at that time several public servants viewed the horrific events of the first five decades of the 21st century and saw "a crummy world" that they had the power to fix. Those public servants decided to pursue reforms and the creation of domestic and international institutions that could address the vulnerabilities exposed during the 21st-century crises. He said they aimed to prevent repeating the horrors of two World Wars, the Great Depression, the Holocaust, and nuclear devastation by responding to WWII differently than the vindictive way the U.S. had responded to a devastated Europe after WWI. This report suggests that due to recent events the United States should revisit the design and capacity of its existing government infrastructure. The digital information and other crises of the 116th and 117th Congresses provide the United States with an opportunity to address weaknesses in our current approach, and to develop new methods for addressing technology and societal vulnerabilities exposed by recent events.



# Overview of the Crises

## The Global Digital Information Regulatory Perspective

Throughout the 116th and 117th Congresses, the United States was not alone in dealing with the global shocks of the pandemic, polarization, and the outsized role large U.S. technology companies had on governance, democratic institutions, the economy, and information systems. During that period, as the pandemic swept across the globe, many other countries pursued regulations and established new governance institutions to help address societal harms created by the rapid spread of false information and to address other issues with emerging technologies.

Regulating technology and information presents unique challenges for every country, often with a trade-off between encouraging innovation and protecting the public. European privacy regulations are ambitious and they have effective privacy protecting institutions, but apart from Germany's SAP Software Solutions, European countries have failed to incubate any major competitors to U.S. technology companies or their mostly self-made founders. It is also not fully clear if the current regulatory frameworks or institutions in European countries are any less threatened by trends in democratic decline.[1]

China, which has successfully developed large technology competitors, has recently taken aggressive regulatory steps to reign in its emerging technology companies and entrepreneurs including regulating algorithms with the stated intent of ensuring they do not exacerbate harms to society. They have also established a department committed to ensuring data privacy and innovation and have aggressively attempted to set global standards following the United States' implementation of the extraterritorial Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of 2017, which allowed U.S. law enforcement to demand access to data wherever it resides. China's regulatory institutions are forward leaning in their scope and design, but given China's record on surveillance and

1 See the EIU Democracy Index for 2021. https://www.eiu.com/n/campaigns/democracy-index-2021/?utm_source=economist&utm_medium=daily_chart&utm_campaign=democracy-index-2021

suppression of democratic human rights, they do not necessarily create a "better" internet experience or protect the rights and privacy of users.

Other countries have also taken aggressive steps to thwart the digital information crisis -- the rapid expansion and increase of misinformation, malinformation, and disinformation-- which was exacerbated by the spread of Covid-19. Technology-enabled disinformation or misleading information production and distribution became so prevalent during the pandemic that in March 2020 the World Health Organization published a definition for the portmanteau "infodemic" (originally coined by David Rothkopf in 2003) to describe rapidly spreading medical misinformation and disinformation on a global scale. In 2020, 17 countries passed new laws against "online misinformation" or "fake information," primarily led by censorious, authoritarian states like Russia, the Philippines, and Nicaragua.

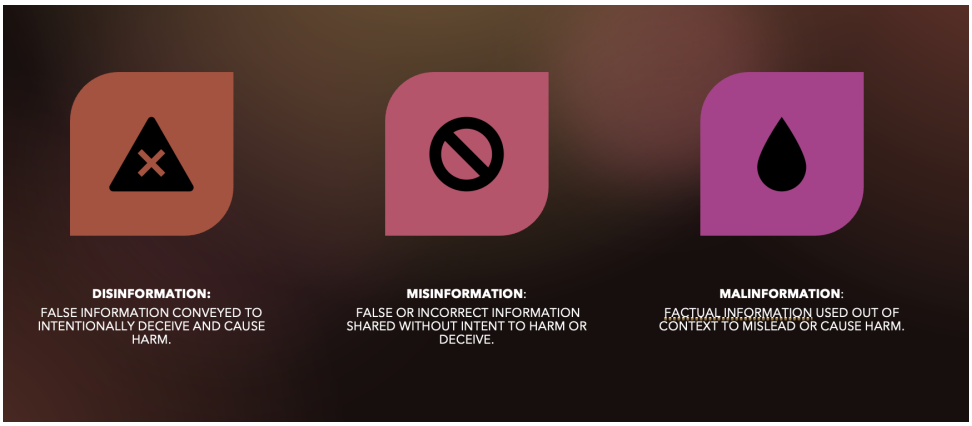



**Figure 1.** The Digital Information Crisis

The digital information crisis, which has played a role in every other emergency, has been a focal point for Congress in its recent legislative efforts to address technology and societal harms, as well as national security threats. Information distribution technologies, particularly those created by the large social media technology companies, have been blamed for radicalizing domestic and international terrorists, facilitating genocide, enabling human trafficking, facilitating digital surveillance and privacy violations, contributing to a mental health crisis in children, worsening a global health crisis, suppressing journalism and dissidents, digital red-lining, investing and other financial scams, fraudulent political and

public relations marketing, and facilitating state actor attacks on elections and democratic institutions, among other harms.[2]

The regulatory optimism and laissez-faire attitude with which Congress approached technology companies in the preceding decades has been replaced by an urgency to reign in the power of technology companies and thwart their negative impacts on society. Although technology regulation has covered everything from artificial intelligence to self-driving cars, to antitrust efforts, much of the regulatory efforts during the 116th and 117th Congresses have focused on disinformation, misinformation, and Section 230 of the Communication and Decency Act.

Between 2017 and 2022, there have been 267 general hearings in the House and the Senate that mentioned disinformation and technology. In 2019 alone, 90 hearings in the House of Representatives and 27 in the Senate noted both disinformation and technology. Since 2017, there have been 24 hearings that have mentioned "interactive computer services," the legal definition for a social media technology company. During the current 117th Congress, 39 bills have been introduced that would have some impact on social media technology companies.

The following report documents how Congress has historically approached disinformation, and how its current efforts have shifted away from focusing on authoritarian governments and disinformation, and toward the business practices and technologies of large social media companies. This analysis briefly mentions problems with some of the current regulatory attempts to rein in "Big Tech" without first establishing privacy guarantees or considering the impact of such legislation on vulnerable communities. It also notes that recent legislation often includes competing goals for the country's strategic interests and its posture toward state actors that weaponize information and would prefer a decline in our technical capabilities.

2 See Anthony Nadler, Matthew Crain, Joan Donovan, "Weaponizing the Digital Influence Machine," Data and Society, 2018. https://www.datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf. Throuvala, Griffiths, M. D., Rennoldson, M., & Kuss, D. J. (2021). Perceived Challenges and Online Harms from Social Media Use on a Severity Continuum: A Qualitative Psychological Stakeholder Perspective. International Journal of Environmental Research and Public Health, 18(6), 3227. https://doi.org/10.3390/ijerph18063227. Yamamoto, & Kushin, M. J. (2014). More Harm Than Good? Online Media Use and Political Disaffection Among College Students in the 2008 Election. Journal of Computer-Mediated Communication, 19(3), 430–445. https://doi.org/10.1111/jcc4.12046

Recent legislative efforts related to technology and social media technology companies suggest that Congress currently recognizes: 1) the government would benefit from greater institutional capacity to address digital information and technology issues 2) the legislative branch and the public would benefit from a stronger understanding of global disinformation and digital information influence operations and 3) all three branches of the U.S. government could benefit from more technical expertise to better understand the problems emanating from the technology sector, particularly regarding social media technology companies and their impact on individuals and society.

## The Domestic Institutional Perspective

From the domestic institutional perspective, recent crises highlighted weaknesses in the Executive and Legislative branches to adopt technology infrastructure, rules, and processes to fully function during a crisis.

In Congress, communication technologies and changes to House and Senate rules played a critical role in how Congress operated during recent crises. Initially, Congress was caught off guard by the pandemic's effects on the legislative process and its inability to hold business meetings, hearings, or vote remotely. However, Congress quickly adapted and adopted new tools and developed new organizations to help it continue to fulfill its Constitutional obligations. It has not yet developed an adequate plan for the next time a crisis incapacitates the U.S. Congress and forces it to work remotely, or if, for example, a nuclear or some other attack were to wipe out the majority of the members of Congress. For a variety of reasons (including Constitutional) we currently do not have the technology or procedural mechanisms in place to allow Congress to convene remotely in the face of a serious emergency or attack on the Capitol. Considering the events of January 6, 2021, this planning failure could prove to be an unnecessary weakness. Additionally, for a variety of jurisdictional and other reasons, Congress is not currently equipped to conduct adequate oversight of the increasingly complex technology sector, as technology harms and failures across various industries demonstrate.

From the Executive Branch perspective, the case of the withdrawal from Afghanistan surfaced several issues that highlighted broader technology weaknesses across agencies. The U.S. State Department had several technology and process weaknesses including its distribution of easily duplicated airport visas for those eligible to evacuate the country[3], and an inability to adequately track how many Americans were in the country[4]. Most of the immigration cases referred to the State Department from Congress, families, or other entities were being sent via email to one email inbox at the State Department. Additionally, utilizing a variety of tools and technologies, an informal network of volunteers assisted the U.S. government and non-government organizations in evacuating, relocating, and providing aid to roughly 124,000 people including 6,000 Americans. For volunteers to rapidly use open-source technology to quickly do what the State Department struggled to do at the time, presents a new challenge for the future of U.S. diplomacy and national security. Almost two months after the withdrawal, Secretary Blinken would acknowledge this fact in a public speech on the importance of modernizing the State Department's technology, communications, and analytical capabilities. He also focused on the necessity of equipping the agency to address cybersecurity and emerging technology threats to meet 21st-century challenges.[5]

## Enhancing Government Capacity through a Department of Technology and Innovation

Historically, U.S. executive branch agencies have been created in response to a crisis and the effort usually reflected the balance of power in the U.S. economy at the time. The Department of Agriculture was established by President Abraham Lincoln during the Civil War when Agriculture represented a large percentage of the U.S. economy. Agriculture currently represents .5 percent of GDP, while the technology sector represents approximately 8 percent of GDP. Part II of this report recommends the

3 Impelli, Matthew. American Trapped in Kabul Explains Bogus Visa Email Sent to thousands," August 20, 2021. https://www.newsweek.com/american-trapped-kabul-explains-bogus-visa-email-sent-thousands-brain-worms-1621668

4 This is largely due to a challenging F-77 process. In 2007, the GAO noted that the U.S. State Department had conducted 270 evacuations since 1988, two years after the first Omnibus Diplomatic Security and Antiterrorism Act of 1986 (P.L. 99-399) created a legal obligation for the Secretary of State to evacuate US citizens during crises. The issues identified in that report have not been revisited by Congress since.

5 Remarks, "Secretary Antony J. Blinken on the Modernization of American Diplomacy," October 27, 2021. https://www.state.gov/secretary-antony-j-blinken-on-the-modernization-of-american-diplomacy/

creation of a new technology and innovation agency to better address how the government deals with technology across the Executive Branch, how it promotes cutting-edge technology developments, and how it regulates the public harms created by the technology industry.

A Department of Technology and Innovation could help the U.S. government maintain international competitiveness, protect users and their privacy, and mitigate societal harms created by rapidly evolving technologies. Congress has increasingly proposed the creation of several technology departments, agencies, and other offices, including a new bureau for cybersecurity at the State Department, a privacy agency, and an office at the Federal Trade Commission staffed with "technologists." It may be more effective to create an executive branch agency, a Department of Technology and Innovation, to address the issues for which many of the smaller offices at the State Department, the Federal Trade Commission (FTC), the Government Services Administration, the Department of Homeland Security, and other agencies were, or are being established.

Recent crises have provided the United States with several use cases to inform how the government can better prepare for emergencies and threats in the future. Ignoring the critical lessons of the 116th and 117th Congresses will not solve any of the problems the country has and will continue to face in the future. The United States has the ability to bolster its institutional and legislative capacity to respond more effectively to the next stress test, and it ought to do so now while it can.

# 1. The Digital Information Crisis

On Wednesday May 5th, 1971, just hours before 1,200 Vietnam War protestors were arrested on the steps of the U.S. Capitol in the midst of what would become the largest mass arrest in U.S. history, forty-year-old Lawrence Britt was testifying before a subcommittee of the United States Senate. Inside what would become the Senate Russell Building, Britt, a former senior intelligence officer for the Czechoslovakian Intelligence Service and Deputy Chief of the country's newly created Department for Disinformation described the Soviet Union's global influence operations, and, despite the risk, did so under his real name.[6] He opened his testimony by clarifying that the term "disinformation" was the same as "active measures" in the Soviet Union and that his department conducted three types of operations: disinformation operations, propaganda operations, and influence operations.

The term "active measures" is an English translation for the title of a Soviet intelligence unit in the 1950's tasked with all disinformation, political influence, and other deceptive influence operations.[7] In his testimony Britt included a description of an unsuccessful Czechoslovakian Intelligence operation that attempted to influence the 1964 U.S. Presidential election by accusing Republican candidate Barry Goldwater of being racist,[8] an operation that was partially influenced by Soviet training and methodology. A Senator pointed out, and Britt confirmed, that the effort was unsuccessful because Americans spread enough false and negative information about the candidate themselves. Britt noted that the effort was an element of a long-term plan by his agency and others like it to isolate the United States "politically and morally," to "disintegrate NATO," and to ensure U.S. troops withdrew from Europe. Britt also pointed out that the United States should not become preoccupied with "espionage paranoia" as it had in the 1950's, because such paranoia, he said, "can weaken the democratic world." Despite learning disinformation operations from the Soviet Union, by 1968, Britt added, his country, in the midst of

6 Britt was the pseudonym used in the documentation for Ladislav Bittman

7 See Dennis Kux, "Soviet Active Measures and Disinformation: Overview and Assessment," Vol. XV. No. 4, Parameters, Journal of the US Army War College.

8 He noted the operation did not have much impact because Americans were very good at smearing candidates on their own.

the "Prague Spring" democratic movements, had itself become a victim of Soviet disinformation efforts immediately before Moscow crushed the Czechoslovakian democratic activity by military force.

Forty-six years later, on March 30, 2017, the Senate Select Committee on Intelligence held another hearing to explore Russia's active measures and the role of Russian disinformation in the United States' democratic process, including the 2016 election. The Senate committee convened twenty-one days after the House of Representatives held a similar hearing on Russian disinformation and its efforts to splinter NATO. The Department of Justice report on Russian interference in the 2016 presidential election published three years later would note that Russian online disinformation included efforts, through fake accounts and other means, to support then-candidates Donald Trump and Senator Bernie Sanders (I- V), with Russian directives clarifying, "We support them".[9] The Justice Department indictment against Russia's Internet Research Agency (IRA) would also highlight the organization's support for candidate Jill Stein (Green Party).[10]

The public hearings about Russian efforts to use disinformation to sway the 2016 presidential election did not include former Intelligence Chiefs from adversarial states like Congress had interviewed in 1971, but the hearings highlighted similar disinformation strategies, tactics, and targets, with a new element that would begin a spike of new hearings in Congress: the role of social media companies in facilitating state actor disinformation and influence operations.

## Congressional Response

Before the 116th Congress, most hearings about the role of social media companies and disinformation mentioned the technology companies obliquely, as a mechanism for information distribution like other forms of media. A few Congressional hearings between 2002 and 2007 mentioned the role U.S. internet service providers (ISP's) and social media websites had played in spreading the ideology of violent extremists and recruiting

9 United States Department of Justice, "Report on the Investigation Into Russian Interference in the 2016 Presidential Election," Vol. I. March, 2019. https://www.justice.gov/archives/sco/file/1373816/download.

10 See: United States of America v. Internet Research Agency, LLC. 18 U.S.C. §§ 2, 371, 1349, 1028A. February, 2018 https://www.justice.gov/file/1035477/download.

terrorists, but they did not, for the most part, focus on the role of the then-nascent social media technology companies.

In 2009, following what was dubbed one of the "Twitter Revolutions", the contested Presidential elections in Iran, and the country's government crackdown on dissent online,[11] Congress held a few hearings that briefly mentioned how social media companies were being abused by authoritarians. A month after the initial revolts in Iran, the House of Representatives Committee on Foreign Affairs held a hearing on the soft power role of Radio Free Europe, Radio Liberty, and Voice of America. The hearing mentioned social media and disinformation briefly but mainly did so to note the hearing was being live-tweeted by a colleague of the witness from Voice of America. The role of social media companies as facilitators and amplifiers of broader disinformation would not start appearing in Congressional hearings until after 2009.

An early indication in Congress that there might be an issue with the design of platforms appeared in 2010 when House Committee on Foreign Affairs held a hearing that examined the U.S. "Strategy for Countering Jihadist Websites." During the hearing, Representative Ed Royce (R-CA) noted that social media platforms and the internet were being used "not only as a tool to recruit and indoctrinate but…beyond that…becoming sort of a virtual radical Madrassas."[12]

Despite some early concerns, after the Arab Spring and the revolution in Egypt in 2010 and early 2011, the U.S. Congress remained mostly optimistic about internet technologies. Hearings suggested it was more concerned with what was characterized at the time as a wave of digital authoritarianism and the suppression of internet activities by authoritarian governments. In July 2011, Congress held a joint hearing on "The Promises We Keep Online, Internet Freedom in the OSCE," which described a "digital curtain" that was descending across the globe. Unusual for the time, the hearing mentioned detailed technical methods by which

11 "Iran and the Twitter Revolution," Pew Research Center, June 25, 2009. https://www.pewresearch.org/journalism/2009/06/25/iran-and-twitter-revolution/

12 Hearing before the House Committee on Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade, "US Strategy for Countering Jihadist Websites," September 29, 2010.

disinformation was being distributed.[13] The witness, describing targeted information warfare operations stated:

> "They also include the application of sophisticated technical means…sowing disinformation and otherwise manipulating information flows. They also include the use of targeted online attacks, denial of service, injecting false content and sophisticated information operations--and I mean this in the military sense--turned inwards at domestic populations."[14]

The primary focus of the hearing, however, was not disinformation operations, but the suppression of freedom of expression, the balkanization of the internet, and how authoritarian governments were using social media and other digital technologies to surveil citizens for dissent. As another witness stated in his testimony that day, "creative hacking and targeting of individuals that are part of the social media network themselves are not just going after elites and journalists, and…leaders or representatives of communities, but individuals who are acting in their own interest, without necessarily an awareness of the impact their participation in these social media networks will have."[15]

Throughout that period Congress' ire would remain directed at authoritarian governments that censored dissent, and at the State Department and other government agencies dealing with terrorist activities online. During a 2014 House Committee on Foreign Affairs hearing on the "Future of Turkish Democracy," one of the witnesses testified that the President of Turkey, Tayyip Erdogan, "had an immediate response, and it was to vilify Twitter stating, 'There is now a menace which is called Twitter. To me, social media is the worst menace to society.' A few days later he

13 The witness stated, "They also include the application of sophisticated technical means, just-in-time blocking, disrupting access to critical information resources at times when they are most needed, sowing disinformation and otherwise manipulating information flows. They also include the use of targeted online attacks, denial of service, injecting false content and sophisticated information operations--and I mean this in the military sense--turned inwards at domestic populations."

14 The Promises We Keep Online: Internet Freedom in the OSCE Region. Hearing before the Commission on Security and Cooperation in Europe, July 15, 2011.

15 Ibid.

moved to block all access to the site and followed shortly thereafter to banning access to YouTube."[16]

It was not until the revelations of Russian interference in the 2016 elections and the subsequent committee hearings by two Senate Committees and one House Committee[17] beginning in mid-January 2017, that social media technology companies became the primary focus of Congressional concern. Facebook's CEO Mark Zuckerberg did not appear before Congress until April 10, 2018, fourteen years after the company was founded.

Throughout 2017 and 2018 Congress began to increasingly examine the architectures and designs of social media technology systems and the companies themselves, led by Senator Mark Warner's (D-VA) Honest Ads Act introduced in 2017 and his white paper, "Policy Proposals for Regulating Social Media and Technology Firms" released in 2018.[18]That year the House Judiciary Committee held two hearings on the "Filtering Practices of Social Media" in April and July of 2018, and later, on November 28, the Commission on Security and Cooperation in Europe conducted a briefing, "Lies, Bots and Computational Propaganda on Social Media." Over the next three years Congress would begin holding an increasing number of hearings to examine the infrastructure, business practices, and technical elements of social media companies.

There are several reasons Congress moved its focus to the architectures and designs of social media technology systems rather than on the disinformation or misinformation being spread. Much of public conversation has centered on the speech and first amendment issues of regulating internet companies. Those protections do not always apply to the production of harmful content, paid content, illegal content, or to the systems that facilitate demonstrable harms that prohibit free speech. Consequently, Congress has increasingly examined problems with the

16 Testimony of Nate Schenkkan of Freedom House, House Foreign Affairs Committee Subcommittee on Europe, Eurasia, and Emerging Threats, July 15, 2014. https://www.govinfo.gov/content/pkg/CHRG-113hhrg88731/pdf/CHRG-113hhrg88731.pdf

17 House Permanent Select Committee on Intelligence (HPSCI), the Senate Select Committee on Intelligence (SSCI), and the Senate Judiciary Committee,

18 Potential Policy Proposals for Regulating Social Media and Technology Firms, August 20, 2018. https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0048-d-0104-155263.pdf

design of tools built by social media companies that have been used to spread digital disinformation and facilitate other types of harm.

## Legislating Harms

The harms, like the societal objectives for regulating them, have often been difficult for Congress to specify without running afoul of the First Amendment. They are also difficult to define because of methodological issues, like being unable to reliably measure human behavior, or utilizing datasets that fail to include all sources of media consumption.[19] Some harms, like buying or selling humans online, are slightly easier to define, but even addressing that behavior faced blowback due to the impact on other vulnerable populations.[20] It is much harder to assess the harms caused when artificial computational amplification[21] of information or sockpuppet[22] accounts, or gaming of trending algorithms– through computational or manual methods– create a deliberately false impression that there is broader consensus or more enthusiasm behind an idea, product, or person than actually exists. Such harms are difficult to regulate partially because the language of law must reflect the rapidly changing technology landscape, the impact of those behaviors is not entirely known, and different entities have different views about what constitutes harm online.[23]

Other well-established online harms like fraud or fakery involve a variety of tactics and techniques that have their non-digital analogs in Soviet influence operations that used disinformation, but that have been changed to work more effectively online.[24] Soviet-era disinformation methods

19 Arayankalam, & Krishnan, S. (2021). Relating foreign disinformation through social media, domestic online media fractionalization, government's control over cyberspace, and social media-induced offline violence: Insights from the agenda-building theoretical perspective. Technological Forecasting & Social Change, 166, 120661. https://doi.org/10.1016/j.techfore.2021.120661

20 FOSTA/SESTA has been one of the few pieces of legislation that has passed as a carve out of Section 230 of the CDA, and it negatively impacted sex workers and their livelihoods. Further, in the GAO review study on the legislation it noted that the provision has rarely been used and that cases are brought under other statutes.

21 Artificial computational amplification refers to the methods by which propaganda is disseminated using automated scripts (bots) and algorithms. It is artificial because the reach and popularity of such messaging, as it appears online, is not a result of real audience engagement.

22 Sockpuppet accounts are fake, or alternative online identity or user accounts used for the purposes of deception.

23 This research included an assessment of the primary harms and harm themes represented in the legal cases against social media companies. See the Appendix for a brief high-level summary of general policy proposal areas, the harms they attempt to regulate and recent legislation.

24 For a novel framework and assessment of online fakery, see Matwyshyn, & Mowbray, M. (2021). FAKE. Cardozo Law Review, 43(2), 643.

included creating forgeries, utilizing PR firms to conduct campaigns, and cultivating journalists and other media manipulation tactics like trying to pay Swedish teenagers to riot on television to validate false claims of immigrant violence.[25]

Digital disinformation tactics include (See Figure 2 below) astroturfing, dark ads, deepfakes, fake accounts/sockpuppets, brigading, bot farms and wet bot farms, artificial amplification, sentiment analysis, meme generation, and other methods.[26] The goals are usually to sow discord, influence public sentiment and decision-makers, and weaken states that challenge the strength or influence of the state actor conducting the operation. Digital disinformation methods are also much cheaper, faster, and more efficient than most of the influence operations and disinformation methods used during the Cold War. In the digital age it is much easier for a state actor to plant propaganda on an obscure website and game a recommendation system to migrate it to a more legitimate

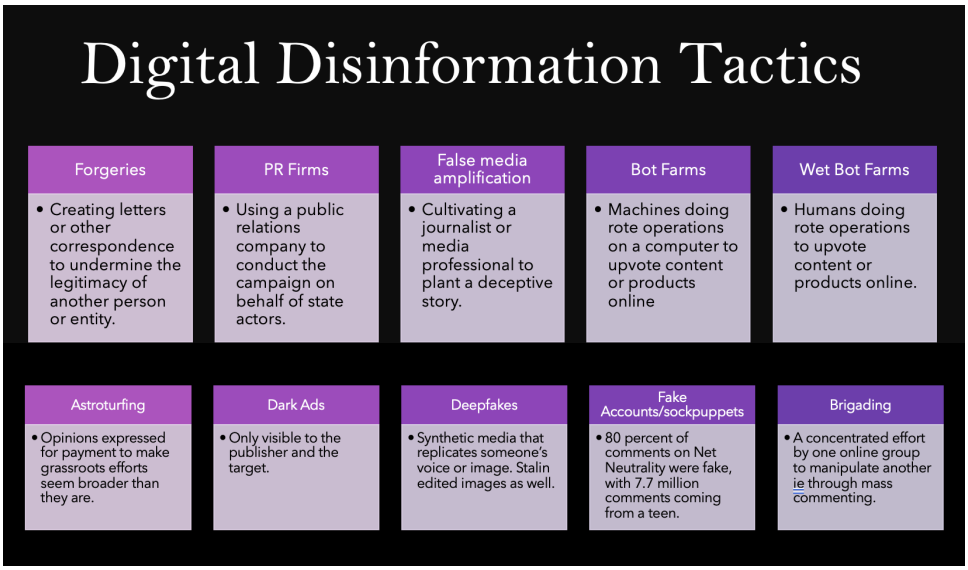



**Figure 2**

25 Gramer, R (2017) Russian TV Crew Tries to Bribe Swedish Youngsters to Riot on Camera. Foreign Policy, 7 March. Available at: http://foreignpolicy.com.ezp-prod1.hul.harvard.edu/2017/03/07/russian-tv-crew-tries-to-bribe-swedish-youngsters-to-riot-on-camera-stockholm-rinkeby-russia-disinformation-media-immigration-migration-sweden/.

26 See Woolley, & Howard, P. N. (2019). Computational propaganda : political parties, politicians, and political manipulation on social media. Oxford University Press. And Marc Dupuis, & Andrew Williams. (2020). Information Warfare: Memes and their Attack on the Most Valued Critical Infrastructure—the Democratic Institution Itself. Journal of Systemics, Cybernetics and Informatics, 18(2), 44–54. And Kula, Choraś, M., Kozik, R., Ksieniewicz, P., & Woźniak, M. (2020). Sentiment Analysis for Fake News Detection by Means of Neural Networks. In Computational Science – ICCS 2020 (pp. 653–666). Springer International Publishing. https://doi.org/10.1007/978-3-030-50423-6_49

website for broader consumption than it is to cultivate a journalist to write a misleading news article.[27]

## Determining Impact

Although current scholarship on social media disinformation operations has illuminated some of the tactics, techniques, and scale of disinformation operations and other nefarious behaviors online, as noted previously, it has not yet fully defined or quantified the impact of those efforts unless there is a physical world harm. Some research has examined the role of social media in the erosion of the multidimensional construct of trust and its implications for the digital economy[28]; political, legal, and social institutions and stability[29]; democracy; and the news industry[30]. Some research has focused on the impacts of social media consumption on qualities like human intelligence,[31] or health information seeking,[32] but there has not been enough scientific research into the impact of digital disinformation consumption and some of the problematic behaviors Congress has attempted to regulate. The impact of digital disinformation has been most clearly evident when amplified incitements to violence online have resulted in physical violence and death, as illustrated by the Burmese genocide against the Rohinga in 2017[33], the January 6th 2021 attack on the U.S.Capitol,[34] or the recent unprovoked invasion of Ukraine by the Russian military under false pretenses widely spread online, some

27 Hanni, Adrian. Secret Bedfellows? The KGB, Carlos the Jackal and Cold War Psychological Warfare." Studies in Conflict and Terrorism, Volume 43. 2020 https://www.tandfonline.com/doi/abs/10.1080/1057610X.2018.1471970

28 Ryan. (2019). Trust and distrust in digital economies. Routledge.

29 Mari, Gil de Zúñiga, H., Suerdem, A., Hanke, K., Brown, G., Vilar, R., Boer, D., & Bilewicz, M. (2022). Conspiracy Theories and Institutional Trust: Examining the Role of Uncertainty Avoidance and Active Social Media Use. Political Psychology, 43(2), 277–296. https://doi.org/10.1111/pops.12754

30 Vaccari, & Chadwick, A. (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. Social Media + Society, 6(1), 205630512090340. https://doi.org/10.1177/2056305120903408

31 Barbetta, Camina, et. al "Let's tweet again? The impact of social networks on literature achievement in high school students: Evidence from a randomized controlled trial," Dipartimento di Economia e Finanza Università Cattolica del Sacro Cuore, Working Paper n.81, May 2019.

32 Boudreau, Singh, N., & Boyd, C. J. (2022). Understanding the Impact of Social Media Information and Misinformation Producers on Health Information Seeking. Comment on "Health Information Seeking Behaviors on Social Media During the COVID-19 Pandemic Among American Social Networking Site Users: Survey Study" Journal of Medical Internet Research, 24(2), e31415–e31415. https://doi.org/10.2196/31415

33 Facebook admits it was used to incite violence offline in Myanmar, BBC, November 6, 2018. https://www.bbc.com/news/world-asia-46105934

34 Inside Facebook, Jan 6 violence fueled anger, regret over missed warning signs, Washington Post, October 22, 2021 https://www.washingtonpost.com/technology/2021/10/22/jan-6-capitol-riot-facebook/

of which were unusually and successfully "pre-bunked" by the Biden Administration.[35]

Some social media researchers and academics argue that the only way to gain an understanding of the impact of certain design decisions and alleged harms of the social media technology companies is for the U.S. government to require social media companies to provide more data to researchers. Data access for researchers has several issues[36] primarily due to the type of data social media companies collect. Unlike requiring tobacco companies (and others) to give the government access to information about their products, social media technology companies and their products are made up of very personalized data. Without privacy provisions in place and a robust and universal standard for what constitutes a researcher, such proposed requirements could present major privacy and surveillance concerns. This is not to say that the government cannot demonstrate a compelling public interest in greater disclosure and transparency requirements for social media technology companies, or in potentially taxing the larger social media technology companies for the negative externalities they create, but this approach, as one former Hill staffer commented, "is like the FDA allowing researchers to do studies, not on the tobacco that impacts children, but on the children themselves."[37]

## Shift Toward Technology Architectures and Design

Some practitioners and scholars, including computer science pioneers Jaron Lanier and Grace Hopper, for decades stressed the importance of understanding and scrutinizing the designs and architectures of systems that provide digital information and data to consumers.[38] By 2021 the

35 "As Russia threatens Ukraine, the U.S. 'pre-bunks' Russian propaganda," NPR, February 8, 2022 https://www.npr.org/2022/02/08/1079213726/as-russia-threatens-ukraine-the-u-s-pre-bunks-russian-propaganda

36 Bogan, Leisel."Congress and Researcher Access to Social Media Data ." Perspectives on Public Purpose, February 4, 2022, https://www.belfercenter.org/index.php/publication/congress-and-researcher-access-social-media-data.

37 Author interview with Congressional staff, 2022.

38 See Lanier, Jaron, "Digital Maoism: the Hazards of the New Online Collectivism," Edge Magazine, May 29, 2006. https://www.edge.org/conversation/jaron_lanier-digital-maoism-the-hazards-of-the-new-online-collectivism and Grace Hopper's MIT Lincoln Laboratory lecture on The Future of Computing, April 25, 1985. https://youtu.be/ZR0ujwlvbkQ

United States Congress had begun demonstrating expanded information technology expertise and shifted its social media technology regulatory focus to the architectures and systems of various technology companies, rather than toward the content they produce. On April 27, 2021, six months before the Wall Street Journal began its series on leaked documents from a whistleblower, the "Facebook Files"[39], the U.S. Senate held a hearing on a specific technical component of social media technology architecture, algorithms, entitled, "Algorithms and Amplification: How Social Media Platforms' Design Choices Shape Our Discourse and Our Minds," featuring the heads of government relations for YouTube, Twitter, Facebook, and two social media researchers.[40] US companies were not the only entities to face criticisms for problematic algorithmic designs. Less than two years after a widely circulated report by Human Rights Watch on China's "algorithms of oppression,"[41] the Chinese Communist Party released draft legislation to regulate algorithms, the "Internet Information Service Algorithmic Recommendation Management Provisions," which came into force on March 1, 2022.[42]

In addition to the hearing on algorithms and amplification methods, other hearings on specific tools, technologies, and harms followed, all highlighting the choices technology companies make in determining how attention to platforms is garnered and retained, and how audiences are manipulated. In a House Armed Services Committee hearing in March 2021 entitled "Disinformation in the Gray Zone," General James Sullivan highlighted the technical and cyber-enabled tools used by various state actors to distribute disinformation across the globe. He noted that Russia believes in a "holistic concept of information confrontation" and spreads propaganda through social media and bots, and that China takes a

39 Facebook Files: Five Things the Leaked Documents Reveal, BBC, September 24, 2021 https://www.bbc.com/news/technology-58678332

40 The hearing featured researchers, Tristan Harris and Dr. Joan Donovan "Algorithms and Amplification: How Social Media Platforms' Design Choices Shape Our Discourse and Our Minds" Senate Banking Committee, Subcommittee on Privacy, Technology, and the Law. April 27, 2021.

41 Human Rights Watch, "China's Algorithms of Repression". May 1st, 2019. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass?gclid=Cj0KCQjwl7qSBhD-ARIsACvV1X2Twrz8u1ZVzPd24tN9XUqa_n8YdEcEEo6DhtfunyGkefWUMkR7OpwaAjvCEALw_wcB#

42 Qu, Tracy. China's algorithm law takes effect to curb Big Tech's sway in public opinion," https://www.scmp.com/tech/policy/article/3168816/chinas-algorithm-law-takes-effect-curb-big-techs-sway-public-opinion

similarly broad approach and is focused on undermining an adversary's "social cohesion, economy, morale, and governance."[43]

Additional hearings focused on technical tools of disinformation like deepfakes, generative adversarial networks (GANS), and other artificial intelligence (AI) and machine learning (ML) tools like GPT-3 which will likely increase the existing amplification of false digital information.[44] The Senate Commerce Committee's report on "Identifying Outputs of Generative Adversarial Networks Act" and its House companion bill outlined previous Senate Intelligence and Commerce Committee hearings on the subject (and related issues) and the need for the National Science Foundation to "support research on manipulated digital content and information authenticity."[45] Subsequent hearings and legislation continue to highlight the technical methods by which disinformation is spread, and have called upon scientific entities to help shed more light on the problem. Many hearings and legislation have also included two other forms of information manipulation that occur online described in Figure 1 – misinformation (the unintentional spread of false information) and malinformation (true information used out of context to mislead or cause harm).

Senator Sheldon Whitehouse (D-RI) has a long history of accurately using the term "misinformation" in his speeches regarding some of the behaviors of the tobacco industry and in relation to climate change. On September 28, 2018, he stated into the record, "What I want to talk about is a new form of political weapon that has emerged on the political battlefield in America, and it is a political weapon for which the American system is not well prepared yet…what you might call weaponized fake news." He then, without mentioning state actors, disinformation, or the origins of

43 Hearing: "Hearing: Disinformation in the Gray Zone: Opportunities, Limitations, and Challenges," Subcommittee on Intelligence and Special Operations, Senate Armed Services Committee March 16, 2021. https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=111323

44 Deepfakes are digital images or videos where the image and voice have been altered to appear to be someone else. A Generative Adversarial Model (GAN) is an unsupervised machine learning technique that identifies patterns or regularities that could have been drawn from the original dataset. GANS can generate and detect fake news. See: Zellers, Rowan, Holtzman, Ari et. al "Defending Against Neural Fake News," Allen Institute for Artificial Intelligence, December 11, 2020, https://arxiv.org/pdf/1905.12616.pdf. GPT-3 is an autoregressive language model that uses deep learning to produce human-like text. See Buchanan, Ben, Lohn, Andrew, Sedova, Katerina, "Truth Lies and Automation, How Language Models Could Change Disinformation," May 2021. https://cset.georgetown.edu/publication/truth-lies-and-automation/

45 "Identifying Outputs of Generative Adversarial Networks Act" or the "IOGAN Act".

fake news,[46] added, "Americans are the subjects of propaganda warfare by powerful economic interests." From then on, he and other members have increasingly focused on the issue of misinformation, rather than disinformation, and Congress' concerns about false information influence would increasingly focus on the U.S. private sector. This change is reflective of the broader American population's growing awareness of the term, misinformation, rather than disinformation. Misinformation is also the term polls usually use when they inquire about false information. Recent polling of the U.S. public by the Pew Research Center and Gallup have used the term "misinformation" in their research instruments, not disinformation.[47]

## Regulatory Proposals

Congress's move from focusing on deliberately deceptive false information fed to a population by an unknown state actor, to exploring how social media companies should ensure the veracity of the information on their websites and protect Americans from extremism, was a significant shift in legislative perspective that began to be reflected in hearings and newly introduced bills. Hearings examined the role of social media companies in promoting and financing different social harms like "domestic extremism" associated with Charlottesville, and the deadly attacks on the U.S. Capitol on January 6th, 2021. Hearings also began examining the role of technology companies in the facilitation of digital redlining, the practice of perpetuating discrimination of marginalized groups through digital technologies and the internet,[48,49] and combating misinformation related to the Covid-19 global pandemic. However, the shift has lacked, with the

46 In the 1890's, the era of "Yellow Journalism", the term "fake news" regularly appeared in headlines. See Merriam Webster, The Real Story of Fake News, https://www.merriam-webster.com/words-at-play/the-real-story-of-fake-news and McQueen. (2018). From Yellow Journalism to Tabloids to Clickbait: The Origins of Fake News in the United States. In Information Literacy and Libraries in the Age of Fake News (pp. 12–35).

47 See "Media and Democracy, Unpacking America's Complex Views on the Digital Public Square,"The Knight Foundation and Gallup, March 9, 2022. https://knightfoundation.org/wp-content/uploads/2022/03/KMAD-2022-1.pdf and Pew Research's work on misinformation: https://www.pewresearch.org/journalism/news-category/misinformation/

48 Gilliard, C. (2016). Digital redlining and privacy with Chris Gilliard, Teaching in HigherEd Podcast. See also the testimony of Francella Ochillo before the U.S. House Committee on Energy and Commerce Subcommittee on Communications and Technology hearing on "Broadband Equity: Addressing Disparities in Access and Affordability," p.4. https://docs.house.gov/meetings/IF/IF16/20210506/112553/HHRG-117-IF16-Wstate-OchilloF-20210506-U1.pdf, May 6, 2021. See also: Noble, S. U. (2018). Algorithms of oppression: How search engines reinforce racism. New York University Press.

49 Digital redlining appears in Congress mostly in testimony and legislation related to broadband.

exception of the House Energy and Commerce Committee's investigations (including a prescient 2009 hearing on behavioral advertising and the internet)[50] a thorough examination of the underlying data infrastructures that feed and motivate some of the behaviors and design decisions of the social media technology companies– data brokers, third-party advertising companies, and audience measurement organizations.[51]

During the 116th and 117th Congresses, Congress has introduced or reintroduced over 110 bills that mention disinformation, misinformation, and social media, with the majority of Congressional mentions of those issues in the last four years led by Senators Ben Cardin (D-MD) and Amy Klobuchar (D-MN).[52] Since 2019, bills introduced in both chambers have ranged in subject matter from the "Disinformation Research and Reporting Act of 2021," the "Social Media Disclosure and Transparency of Advertisements Act of 2021," the "Deceptive Experiences to Online Users Act (DETOUR)," the "Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act (SAFE TECH)," to "Anti-CCP Espionage via Social Media Act of 2021,"[53] the "Health Misinformation Act of 2021," the reintroduction of the "Honest Ads Act," the "Deepfake Taskforce Act," "Stop Shielding Culpable Platforms Act," "Protecting Americans from Dangerous Algorithms Act," "The Data Elimination and Limiting Extensive Tracking and Exchange Act (DELETE)" and "Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT)".

Legislative proposals during this period ranged from completely repealing Section 230 of the Communications Act, to regulating state-sponsored disinformation, to proposals that would create offices within the Federal Trade Commission for researchers to collect and analyze social media data

50 Joint Hearing before the Subcommittee on Commerce, Trade, and Consumer Protection and the Subcommittee on Communications, Technology and the Internet, "Behavioral Advertising: Industry Practices And Consumers' Expectations," June 18, 2009.

51 See Rubin. (2019). Disinformation and misinformation triangle A conceptual model for "fake news" epidemic, causal factors and interventions. Journal of Documentation, 75(5), 1013–1034. https://doi.org/10.1108/JD-12-2018-0209

52 According to the aggregate number of bills introduced by member on Congress.gov.

53 One of the few bills to address disinformation and misinformation created by a foreign entity.

to better understand how social media technology companies analyze and manipulate Americans online.[54]

"Interactive computer services," the legal term for a social media technology website like Facebook or Twitter, has so far appeared in 82 pieces of legislation in the 116th and 117th Congresses, with none of them passing into law. Challenges to passing federal regulations on social media technologies and the harms they inflict on society have included previously noted issues with technical definitions, a wide range of stakeholders with competing interests, and Section 230 of the Communications Act of 1934, enacted as part of the Communications and Decency Act (CDA) of 1994.[55]

Members of Congress hold a range of views on Section 230 that are not consistent across party lines. Some conservatives oppose Section 230 and argue that it has been an extended subsidy for an industry that has now made competition in the sector impossible and should be eliminated. Other conservatives believe the law should be repealed because technology companies use the immunity provisions to censor conservative speech. Progressives believe it should be repealed because they believe Section 230 protects hate speech, harmful behavior, and discrimination on the internet, or view it as part of a larger antitrust issue. As one staffer and researcher observed, "social media products are the only consumer products with almost no product liability."[56]

Social media technology companies are subject to federal criminal statutes, and they are responsible for the content they create rather than simply host. They are also subject to Article 5 of the FTC which prohibits unfair and deceptive acts, but compared to other industries like aviation, radio, television, or even cybersecurity,[57] social media technology companies have largely been left to regulate themselves. They have also not been clearly defined as an industry– social media companies host websites, but

54 "Platform Accountability and Transparency Act" https://www.coons.senate.gov/imo/media/doc/text_pata_117.pdf

55 Section 230 of the CDA immunizes online service providers like social media companies from some legal liability for transmitting or taking down user-generated content.

56 Author interview with Congressional staffer and researcher, 2022.

57 Regulations pertaining to cybersecurity are few but cut across industries, including health, finance, and federal agencies. Congress recently passed legislation requiring Federal civil agencies to provide breach notifications within 72 hours of a significant event.

they also provide payment systems, operate very similarly to traditional and regulated media companies, and collect and utilize vast amounts of personal and other data.

Other members, like Senator Ron Wyden (D-OR) who was one of the drafters of the original legislation, are staunch supporters of Section 230 as a guarantor of freedom of expression online, protection for vulnerable users, and user-generated content, and a key element in the promotion of technology innovation. The debate around what Congress should do to protect Americans from the internet has always been fierce, however, even in its origins.

On February 1, 1995, just a few months after the House of Representatives launched its first website, Senator James Exon (D-NB) introduced into the Senate the Communications and Decency Act (CDA) as an amendment to the Telecommunications Act of 1996. It would pass five months later, with the indecency provisions overturned by the Supreme Court on June 26, 1996. The stated purpose of the CDA was to protect children from online obscenity. Senator Exon's bill was drafted in response to a widely publicized, and later widely criticized study published in the Georgetown Law Review that claimed there was far more pornography and obscenity online than previously thought.[58]

During the introduction and unanimous consent decree for the bill, Senator Barbara Boxer (D-CA) queried Senator Exon about whether the bill would curb online discussions about abortions. He responded that discussions about abortion are Constitutionally protected but that "our interest in adopting this provision was to curb the spread of obscenity–speech that is not protected by the first amendment." She subsequently agreed to support the legislation.[59] When it passed a Senate Committee vote on March 24, a spokesperson for the Electronic Frontier Foundation told the Washington Post, "Welcome to Digital Singapore." Roughly 24 years later, just after Singapore passed its "Protection from Online

58 Rimm, Marty. Marketing "Pornography on the Information Superhighway: A Survey of 9l 7,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories." Georgetown Law Review, 1995.

59 Unanimous-Consent Agreement; Congressional Record Vol. 142, No. 14 Issue and Section: February 01, 1996 - Senate (Vol. 142, No. 14)

Falsehoods and Manipulation Act" in May 2019, the U.S. Congress considered draft versions of new bills to address disinformation and misinformation online, and free speech advocates would make the same point.

# Global to Local Influence

Technology-enabled disinformation and misleading information production and spread became so prevalent during the global pandemic that in March 2020 the World Health Organization published a definition for the portmanteau "infodemic," originally coined by David Rothkopf in 2003, to describe medical misinformation and on a global scale. Throughout the pandemic, most countries saw a proliferation of misinformation and disinformation about the novel coronavirus, with spikes in interest in conspiracy theories, as demonstrated by a few new infodemiological studies including one that focused on conspiracy theories and Google searches, with no direct findings for impact. It was also clear throughout the pandemic that state actors were developing and spreading disinformation related to the origins of the coronavirus.

In its report, "Hijacking Our Heroes: Exploiting Veterans Through Disinformation on Social Media," on December 16, 2020, the House Committee on Veteran's Affairs explored internet protocol (IP) spoofing[60], the spread of memes, and other technical methods of disinformation campaigns. It also noted, "Russia and Iran are the most prominent state actors in this context, but recent work has identified additional state actors, such as China and Saudi Arabia, using information operations to target

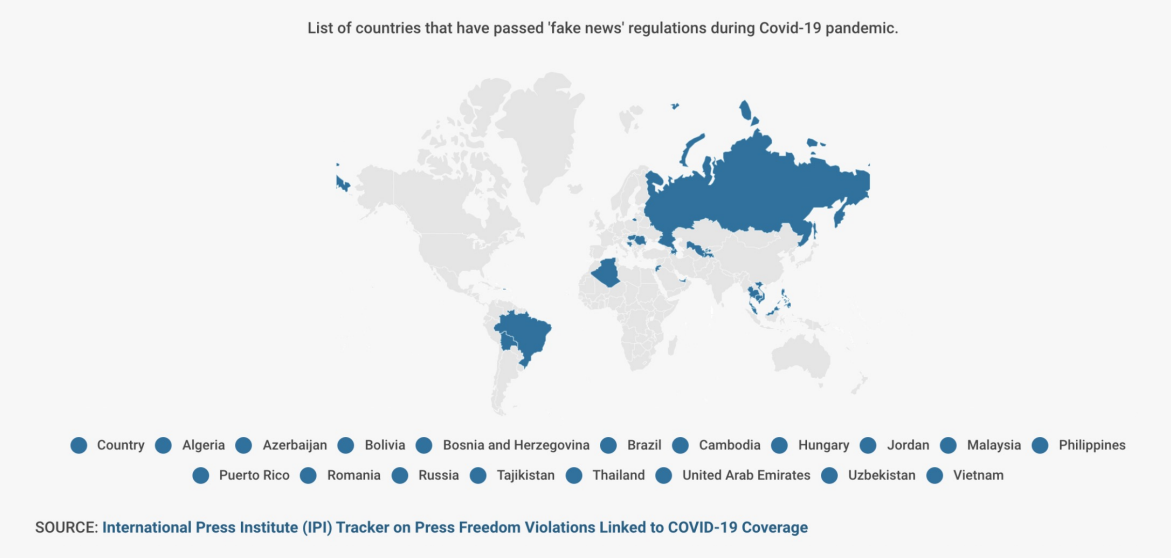



**Figure 3** A Domestic Crisis

60 IP spoofing is when an IP packet address is forged to hide the identity of a sender, or impersonate another computer, and is usually used by bad actors to conduct DDOS attacks.

communities and topics of interest." As it described the Senate Select Committee on Intelligence report, the House report switched again from disinformation to misinformation, "The Senate Report sheds light on the broader issues of misinformation campaigns and predatory schemes targeting veterans presented in a report prepared by the Vietnam Veterans of America (VVA)."

On May 12, 2021, The Senate Foreign Relations Committee held a hearing on "Covid-19 and the U.S. International Response," where two witnesses from the State Department and United States Agency for International Development (USAID) outlined how authoritarian regimes were responding to the information crisis in the midst of the pandemic, stating "public health responses to COVID–19 are critical, they have also been exploited by authoritarian governments to violate and abuse human rights, engage in inappropriate or excessive monitoring of citizens, and to enable disinformation and hate speech. In particular, these responses have negatively affected freedom of peaceful assembly and freedom of expression."

During the hearing Senator Chris Coons (D-DE) asked several pointed questions about how to counter disinformation, and the State Department official noted that the disinformation narratives pushed by the People's Republic of China and Russia since the beginning of the pandemic were being closely monitored and shared with global partners to drive coordinated responses to it. The hearing and supporting documents, to its credit, included the word "misinformation" only three times, and otherwise both the witnesses and the Senators focused exclusively on disinformation.

As the terms misinformation and disinformation merge or become confused for each other, and as false information proliferates, there has been a push in the United States and across the globe to move away from a targeted effort to tackle disinformation and toward a broader effort to address information integrity and "fake news". In 2020, 17 countries passed or tightened laws on misinformation and "fake news," primarily in authoritarian states like Russia, the Philippines and Nicaragua (See Figure 3).[61]

61 "Censorious governments are abusing fake news laws," The Economist, February 11, 2021. https://www.economist.com/international/2021/02/11/censorious-governments-are-abusing-fake-news-laws

In the United States, as massive metal and cement fences and U.S. troops circled the U.S. Capitol complex, Congress, reeling from the attacks on the Capitol on January 6th, focused on misinformation and disinformation from yet another perspective. Several committees and members sought to determine how false information online could have contributed to the deadly events that day, and how and where domestic violent extremism spread. To a lesser extent, Congress explored the possibility of foreign and domestic influence operations in stoking the violence. Ten days after the attacks, the Chairs of the House Select Committee on Intelligence and the Chair of the House Committee on Homeland Security asked the Director of the FBI, the Acting Director of the National Counterterrorism Center, the Acting Undersecretary for Intelligence Analysis at the Department of Homeland Security, and the Director of National Intelligence for details on the events of that day, with the purpose of remedying any gaps in legislation or policy. In the letter, they asked, "whether the insurrection had any nexus to foreign influence or misinformation efforts."[62]

By March 2021, the House was holding hearings on state and local government responses to domestic extremism. Additionally. Congress moved to evaluate the events more formally and to bolster the institutional security organizations. One day after it established the January 6th Commission to investigate the causes of the attacks, the House of Representatives passed a $1.9 billion U.S. Capitol Security bill that included a new rapid response team to respond to future attacks. It is not clear if that entity will be tasked with countering misinformation and disinformation influence operations directed at Congress.

62 January 16, 2021. Congressional letter to the heads of the FBI, NCTC, DHS, and DNI on the January 6 attacks. https://intelligence.house.gov/uploadedfiles/20210116_hpsci_chs_hjc_cor_letter_to_fbi_dhs_nctc__odni_on_capitol_insurrection.pdf

## New Offices and Entities

Just as both the House and the Senate have introduced legislation to regulate the architecture and designs of products created by the social media technology companies, Congress has also created new offices or has attempted to augment existing ones that could be equipped to deal with technology issues and harms created by social media companies.[63]

It has also begun to direct non-agency scientific entities to conduct research into misinformation and disinformation online, requesting that they consider research proposals by social media researchers embedded in federally funded entities. In March 2021, seven months after Senator Gary Peters (D-MI) proposed a "Misinformation and Disinformation Task Force of 2020," and roughly six months after Representative Jennifer Wexton (D-VA) led Representatives Don Beyer, (D-VA), Sean Casten (D-IL), Bill Foster (D-IL) and Jamie Raskin (D-MD) in introducing the bill in September 2019, Senators Mazie Hirono (D-HI), Corey Booker (D-NJ), Richard Blumenthal (D-CT), Amy Klobuchar (D-MN), Jack Reed (D-RI) and Elizabeth Warren (D-MA) introduced the "Covid-19 Disinformation Research and Reporting Act of 2021."

Rather than directing the social media companies to evaluate misinformation and disinformation online which would face numerous legal challenges, the bill directs the National Academy of Sciences to conduct a study "on the current understanding of disinformation and misinformation influence on the public debate…the role of social media companies…potential financial returns for creators of such content….and strategies to mitigate the dissemination and negative impacts of Covid-19-related disinformation and misinformation."[64]

Since its creation during the Civil War (see Part II of this report) the National Academies of Sciences has regularly been tasked by the U.S. President and Congress to provide sound scientific advice on scientific questions pertaining to the U.S. Government, but misinformation analysis

63 See the "Federal Trade Commission Technologists Act of 2021," introduced July 19 2021. It establishes a new Office of Technologists at the FTC.

64 S. 913 (IS) - COVID–19 Disinformation Research and Reporting Act of 2021

is not widely considered a scientific discipline.[65] Studies of the spread and scale of misinformation currently blend a variety of other disciplines and techniques, like intelligence, network analysis, and the study of algorithms. Something as politically and socially sensitive as whether information or ideas are true seems outside of the scope of the traditional role of the National Academies of Sciences. There is also reasonable concern that such a task could potentially politicize the National Academies of Sciences.

Congress has long grappled with legislating science and technology across various domains, given the rapid pace of most technology developments compared to the legislative process. It has provided funding and new responsibilities to a wide variety of offices and roles that deal with technology across the three branches of government and in the White House. It has considered restoring the Office of Technology Assessment.[66] It created the Cybersecurity Solarium to evaluate how the U.S. Government should deal with cybersecurity issues, resulting in the recent creation of the new Bureau of Cyberspace and Digital Policy[67] at the Department of State. It has also contemplated the reestablishment of the United States Information Agency (USIA).[68] In recent years it has also begun to modernize itself, creating a Select Committee on Modernization in the House, moving to virtual hearings during the pandemic, acquiring more technical staff to help draft technical legislation, and creating a Congressional Digital Service.[69]

Despite many efforts to both encourage technology innovation, reign in the excesses of technology giants, and address the issues of disinformation, misinformation and other forms of fake information and influence online, Congress continues to stall on privacy regulation, a necessary component

65 See Kumar, K.P.K., Geethakumari, G. Detecting misinformation in online social networks using cognitive psychology. Hum. Cent. Comput. Inf. Sci. 4, 14 (2014). https://doi.org/10.1186/s13673-014-0014- And Jooho Kim, Makarand Hastak, Social network analysis: Characteristics of online social networks after a disaster, International Journal of Information Management, Volume 38, Issue 1, 2018, Pages 86-96, ISSN 0268-4012, https://doi.org/10.1016/j.ijinfomgt.2017.08.003.

66 Statement of Representative Holt on the Office of Technology Assessment. February 14, 2009. https://ota.fas.org/reports/AAAS-holt.pdf

67 Establishment of the Bureau of Cyberspace and Digital Policy. April, 2022. https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/

68 Brezezinski, Ian testimony before the US Senate Committee on Foreign Relations, Subcommittee on Europe and Regional Security Cooperation. Hearing on Black Sea security: Reviving US policy toward the region, October 27, 2021.

69 The Hill Gets Serious About Digital Service, Jan 20, 2022 https://fcw.com/digital-government/2022/01/hill-gets-serious-about-digital-services/360994/

of addressing many harms created by social media technology companies, data brokers, and other technologies. To a lesser extent, it has also struggled to pass legislation focused on innovation and competition related to technology, and legislation that takes a whole-of-government approach to emerging technologies like artificial intelligence, machine learning, and quantum computing.[70]

The final report of the recently concluded National Security Commission on Artificial Intelligence recommended a number of solutions to ensure that the U.S. maintains competitiveness in one area of science and technology, Artificial Intelligence. It made recommendations to several agencies including the Department of Defense and the Office of the Director of National Intelligence (ODNI), but it specifically stated that the Department of State, "[should] be reoriented, reorganized, and resourced to lead diplomacy in emerging technologies,"[71] just seven months before Secretary Blinken made his October 2021 speech committing to the modernization of the agency.

On June 1, 1953, President Eisenhower presented to Congress a similar call for the reorganization of the State Department to better respond to the country's leadership role in the world at that time and the foreign policy and information threats that emanated from the Cold War disinformation apparatus.[72]

That day, in his eight-part reorganization proposal, Eisenhower outlined in Reorganization Plan No. 8, the establishment of a new agency– the United States Information Agency (USIA)– for the conduct of information programs. The Agency operated for 46 years during the height of the Cold War. After it was completely shuttered, USIA published the final report of the Active Measures Working Group, an unclassified interagency working

70 The creation of the National Quantum Office at the White was an accomplishment that did not get the attention it deserved, but could be elevated by an executive branch agency.

71 National Security Commission on Artificial Intelligence Final Report, March 3, 2021. https://www.nscai.gov/wp-content/auploads/2021/03/Final_Report_Executive_Summary.pdf

72 "Special Message to the Congress on the Organization of the Executive Branch for the Conduct of Foreign Affairs."

group under the Department of State.[73] In that report the members of the group admonished, ``[a]s long as states and groups interested in manipulating world opinion, limiting U.S. Government actions, or generating opposition to U.S. policies and interests continue to use these techniques, there will be a need for the United States Information Agency to systematically monitor, analyze, and counter them.'[74] Yet, Congress dissolved the United States Information Agency in 1999.

It has been twenty-three years since Congress shuttered the USIA, largely because the Cold War had ended, but as an institution, it is still grappling to understand and respond to information operations and disinformation, and it is still struggling to protect our institutions and our global partners from the effects of those efforts. Congress has an opportunity to bolster our existing institutions with a stronger entity that could help ensure that in the next twenty-three years we are better positioned to address disinformation and other threats created by new technologies.

73 The Active Measures Working Group was created by President Reagan in 1981 to counter Soviet Propaganda. For an extensive description of Soviet Active Measures and the efforts of the Working Group between 1986-1987, see Soviet Influence Activities: A Report on Active Measures. US Department of State, August 1987. https://jmw.typepad.com/files/state-department---a-report-on-active-measures-and-propaganda.pdf

74 USIA, Soviet Active measures in the "Post-Cold War" Era: 1988-1991 (Washington, DC: USIA, June 1992), available at <http://intellit.muskingum.edu/russia_folder/pcw_era/index. htm#Contents>.

# 2. Congress and Crises: Toward a Department of Technology and Innovation

On March 3rd, 1863, two years into the Civil War and during the third session of the 37th Congress of the United States, the Senate passed a bill establishing the National Academy Sciences. The bill was quickly passed by the House and signed into law by President Abraham Lincoln in a matter of hours.[75] One year before, President Lincoln had created the United States Department of Agriculture, an agency he would later call, "The People's Department."[76] Within two years, in the midst of several crises including the expulsion of three more of its members from the Senate[77], the United States Congress and the President of the United States worked together to create two important institutions to reflect the needs of the U.S. and its economy at the time and to prepare the country for the future. The organizations were created to encourage industry, innovation, and science, and to coordinate and communicate critical information about the work of the government as it pertained to science information and an essential industry, and agriculture.

Although President Abraham Lincoln is credited with establishing the Department of Agriculture amid a serious existential crisis for the country, one of the initial advocates for the creation of that department was President George Washington.[78]

75 H. Journal 37-3 - Journal of the House of Representatives of the United States, Third Session of the Thirty-Seventh Congress, March 3, 1863.

76 U.S. Department of Agriculture History. https://www.usda.gov/our-agency/about-usda#:~:text=On%20May%2015%2C%201862%2C%20President,economic%20development%2C%20science%2C%20natural%20resource.

77 See Senate Civil War Expulsion Cases: https://www.senate.gov/about/powers-procedures/expulsion/039CivilWarCases_expulsion.htm and Missouri State Archives, Trusten Park, https://www.sos.mo.gov/archives/mdh_splash/default.asp?coll=trustpolk,

78 Bushman, Mark. "George Washington, The Farmer". February 27, 2017. NRCS, United States Department of Agriculture.

Thirteen years before, on December 31, 1849, a Joint Committee of the Vermont Legislature submitted a resolution and proposal for a Department of Agriculture to Congress.[79] The submission quoted former President Washington:

> "It will not be doubted that with reference to individual or national welfare, agriculture is of primary importance. In proportion as nations advance in population, and other circumstances of maturity, this becomes more apparent, and renders the cultivation of the soil more and more an object of public patronage. Institutions for promoting it grow up, supported by the public purse; and to what object can it be dedicated with greater propriety?"

In response to pressure from the public and the President, Congress established the U.S. Department of Agriculture originally as a small office within the U.S. Patent Office.[80] During his address to Congress on December 1, 1862, Lincoln emphasized the importance of the newly created agency and highlighted that it had already established "exchanges of information at home and abroad." The agency's international effort was partially a result of the fact that four years before, in his report to Congress, the U.S. Commissioner for Patents, Henry Leavett Ellsworth, included an extensive assessment of the Department of Agriculture in Prussia, and Russia's Ministry of the Interior and its satellite education programs related to agriculture.[81] Some of the United States' earliest efforts to create new agencies and offices included engagement with other countries and models, a trend that continues today.

79 31st Congress, First Session. December 31, 1849. Resolutions of the Legislature of Vermont relative to the establishment of an Agricultural Bureau.

80 Griesbach, R.J. "Putting down roots in the U.S. Patent Office," US Office of Technology Transfer, United States Patent and Trademark Office. https://www.uspto.gov/learning-and-resources/newsletter/inventors-eye/putting-down-roots-patent-office

81 U.S. House of Representatives, Report to Congress on Agriculture for the Year 1857. U.S. Commissioner for Patents, May 19, 1858.

## Crises and the Creation and Reorganization of Executive Branch Agencies

Since then, the Cabinet of the President of the United States has expanded from five members to 15, several independent and non-independent agencies as well as several independent.[82] Many Executive Branch agencies were established during or immediately following a major crisis, often of existential importance. The first three Executive Branch agencies (State, War, and Treasury) were created shortly after the Revolutionary War, with the Treasury Department created to try to help pay for the war. The Department of the Interior was created by Congress following the conclusion of the Mexican-American War. The Department of Labor was originally proposed after the Civil War, because, as the labor leader William Sylvis said, no department had its "sole object the care and protection of labor."[83] The Department of Labor was eventually separated from the Department of Commerce and created on March 4, 1913, hesitantly signed into law by President Taft within the Senate Chambers, just hours before President Woodrow Wilson was inaugurated.

The Department of Defense (a consolidation of the Department of War and the Department of the Navy) was created following the crises of World War I and World War II, the Department of Energy was established after the energy crisis of the 1970's, and the Department of Homeland Security was created as an amalgamation of 22 other smaller agencies after the crisis of 9/11. Other agencies and government entities followed the same pattern. The President and Congress established the Securities and Exchange Commission (SEC) to restore the public's trust in the stock market following the 1929 market crash, and the FTC was created to address the 19th-century monopolistic trust crisis.

82 President Biden's Cabinet includes the heads of 15 departments led by the Secretaries of Agriculture, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Labor, Transportation, State, Treasury, Veterans Affairs and the Attorney General. It also includes the White House Chief of Staff, the US Ambassador to the United Nations, the Director of National Intelligence, the US Trade Representative, the heads of the Environmental Protection Agency, Office of Management and Budget, Council of Economic Advisors, Office of Science and Technology Policy, and Small Business Administration.

83 Grossman, Jonathan, The Origin of the Department of Labor, https://www.dol.gov/general/aboutdol/history/dolorigabridge

Several Executive Branch agencies have been reorganized during or because of crises, like the Federal Emergency Management Agency (FEMA). Originally the "Office of Emergency Planning," FEMA was established by Executive Order by President Carter in 1979, but after repeated failures, it was reorganized in 1993 after Congress threatened to abolish it.[84] After 9/11 it was absorbed into the Department of Homeland Security. After Hurricane Katrina and FEMA's widely criticized failures, it was reorganized a fifth time.[85] Efforts to reorganize or establish new agencies in the Executive Branch have occurred during every administration, with varying degrees of success.

Congress has also encouraged the creation of self-regulating entities. In the 1960's when the TV and Radio industries were faced with concerns about fraud in media ratings and audience assessments, Congress explored regulations, especially for the "purpose and accuracy of audience research" through what would become known as the Harris Committee hearings on broadcast ratings. The hearings were held by a Special Subcommittee on Investigations of the House of Representatives Committee on Interstate and Foreign Commerce.[86] After extensive hearings and witness testimony, Congress concluded that the administration of a statute regulating the industry would be too burdensome for the Federal government, and encouraged the industry to establish ratings, accreditations, and audits of ratings services.[87] The recommendations resulted in the formation of an organization funded by the industry that would review and accredit audience ratings services, include audits by independent CPA firms, through what is now called the Media Ratings Council, an entity that has operated with relative success for over fifty years.

During the 116th and 117th Congresses alone, the United States has suffered through a deadly global pandemic, a violent, lethal attack on the U.S. Capitol, a growing nuclear threat from Russia, a tumultuous withdrawal from Afghanistan, atrocities in Ukraine and Tigray, and a

84 The Federal Emergency Management Publication 1. https://www.fema.gov/sites/default/files/2020-03/publication-one_english_2010.pdf

85 Camacho, Alejandro and Glicksman, Robert. Reorganizing Government. NYU Press, 2019. muse.jhu.edu/book/76033.

86 The Fair Ratings Act Hearing Before the Committee on Commerce, Science, and Transportation United States Senate, One Hundred Ninth Congress, First Session, July 27, 2005.

87 House Report No. 1212, January 1, 1966

suspected disinformation campaign to blame Covid-19 on the United States. Most of the crises involved an element of technology, or the use of social media technologies that created or made them worse. Yet, with the exceptions of elevating the Office of Science and Technology Policy to the Cabinet level, a few of the Congressional proposals mentioned in Part I, and Leader Chuck Schumer's (D-NY) Endless Frontier Act (now included in the United States Innovation and Competition Act), Congress has not passed a major Congressional or agency effort to address technology harms and how they might be remedied. As noted in the overview, the agriculture industry comprises .5 percent of gross domestic product (GDP), and technology comprises an estimated 8 percent of GDP and according to one industry study, employs over 12 million workers.[88] The current organization of the executive branch agencies does not accurately reflect the balance of power or wealth in the United States or prepare the country for future challenges. Like labor, technology is in everything, but unlike labor, it does not have its own agency.

Congress has also not solved the state actor disinformation problem. As mentioned in Part I, in the 1950's, to combat the global Soviet disinformation apparatus, the United States established the United States Information Agency at the State Department, and later, the unclassified interagency Active Measures Working Group, which were later closed. The current Global Engagement Center (GEC), like its predecessors including the USIA, is responsible for the interagency process of the Federal Government to "recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations."[89] The GEC has been effective, but it could be enhanced if combined with the efforts of a more powerful agency dedicated to addressing the way technology is used by state actors and others to conduct influence operations and disseminate disinformation.

88 CompTIA Cyberstates State of the Tech Workforce. 2020. https://www.cyberstates.org/

89 Core Mission of the State Department's Global Engagement Center. https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/

## The Opportunity

Although Congress has introduced many bills to regulate large technology companies and to incentivize technology development and competitiveness, with the exception of Representative Ro Khanna's 2020 (reintroduced in 2021) bill to create a new independent agency, "to be known as the Federal Institute of Technology", there has not been a concerted effort by Congress to give a federal entity the power needed to encourage innovation and regulate and sanction the technology industry in a timely manner. Congress considered creating an agency for innovation when it prepared the Endless Frontier Act but ultimately it decided to create a new Technology Directorate at the National Sciences Foundation. While it was a valiant effort in a positive direction, it is unlikely that the Directorate provides enough empowerment to encourage innovation across the technology sectors.

Currently, there is no executive branch agency that can address cross-agency safety issues that are not completely owned by any single agency. For example, the U.S. Consumer Product Safety Commission (CPSC) currently lacks the power to order companies that produce deadly products to recall them. They are only empowered to request that the products be removed. It took several years to recall over 4 million Fisher-Price Rock and Play Sleepers after 30 deaths of infants over ten years were tied to the products.[90] The FDA spent three years approving a protocol for Picture and Archiving Communication Systems (PACS) for medical scans, but they failed to conduct a security assessment for them. Meanwhile, thousands of medical images are widely available online because of a flaw in that protocol. Health and Human Services has been aware of the vulnerabilities of at least 30 systems with thousands of medical images for over two years and has yet to act to have them removed.[91] A department of technology could escalate and act on such issues when other agencies fail to, or it could help augment the existing efforts of agencies.

90 Fisher-Price Recalls 4.7 million sleepers recalled as officials confirm over 30 deaths. https://www.cnn.com/2019/04/12/us/fisher-price-rock-n-play-sleeper-recall/index.html

91 Bogan, Leisel."Your Insides Are Online: Government Capacity and Technology." Perspectives on Public Purpose, April 5, 2022, https://www.belfercenter.org/publication/your-insides-are-online-government-capacity-and-technology.

## Considerations for a Department of Technology and Innovation

If Congress establishes a Department of Innovation, the new agency should consider the following:

- **Use human-centered design in the creation of the agency.** The academic literature and practitioner case studies on executive branch agencies and their organization and design focus primarily on the merits of coordination, centralization, and communication, and less on the user experience of agencies. The literature rarely focuses on what are known as human-centered design principles.

  Human-Centered Design was originally pioneered by Stanford Professor John E. Arnold in the 1950's. He encouraged his student engineers to be creative, and orient the engineering toward creative solutions, in part by asking many questions, imagining various scenarios, and other methods.[92] If Congress were to establish a new Department of Technology and Innovation it could draw from a variety of existing models, but it should also consider utilizing a human-centered design process in the creation of a new department. This would entail in-depth interviews to understand what the end-users of the agency– the public, other government agencies, and the private sector– might need, or want from the agency. Interviews should incorporate "user journeys", step-by-step documentation of how a user approaches and engages with an agency. Interviews would differ based on the user—how end-users at multiple hospitals that have been overtaken by ransomware might experience and utilize the agency would likely be very different from how an end-user at the Department of Transportation might utilize the agency. Arnold's approach to human-centered design centered on four steps: question, observe, associate, and predict. Each step should be used to design an executive branch agency based on how the agency can best solve problems for various stakeholders.

92 See the collection of Professor Arnold's public remarks in, "Creative Engineering: Promoting Innovation by Thinking Differently," 2016. https://www.inist.org/library/1959.John%20E%20Arnold.Creative%20Engineering.pdf.

Congress should also design the institution around use cases like some of the harms and issues outlined in Part I, rather than around areas of jurisdiction.

By asking questions of users, observing how users engage with existing agencies related to technology, and associating those actions with predictions about what could be done differently or effectively, the agency could better anticipate and avoid some of the pitfalls faced by agencies like the Department of Homeland Security, and provide more value to users and the American people.

- **Include a digital services organization within the agency.** Digital services organizations usually include technologists, designers, user experience researchers, and developers who tackle technical challenges outside of the scope of existing IT/CIO functions and that are usually more agile and capable of working on problems across an organization.

  The pandemic initiated a bigger push for digital service efforts throughout governments all over the world. In early 2020, in a matter of weeks, the U.S. Congress was forced to adjust from being a paper-based institution with all in-person hearings to conducting hearings and other business remotely. Executive Branch agencies also adjusted rapidly, enhanced by the efforts of the United States Digital Service established by President Obama in 2014, and 18F, which was established by two former Presidential Innovation Fellows the same year.[93]

  The House of Representatives, as mentioned, now has its own digital service organization within the House Information Resources. Such agile approaches to government problems have proven to be effective across the United States and around the world. Equipping the Department of Technology and Innovation with a dedicated Congressional Digital Service, or having it absorb the USDS with a broader portfolio, would ensure that the new agency has the talent and tools to address a wide variety of problems internally, across the executive branch, and that emanate from the technology sector.

93 USDS is a technology unit located within the Executive Office of the President of the United States and provides consultative services to Executive Branch Agencies.See: https://www.usds.gov/ 18F is a digital services organization within the Government Services Agency.

- **Ensure the agency has the power to both regulate the technology industry and encourage technology innovation.** Congress has repeatedly tried to create a centralized agency for scientific R&D within the federal government since Vannevar Bush's original, "Science: The Endless Frontier" report in 1945. Instead, it succeeded in creating the National Science Foundation and several other smaller entities.[94] Given the global technology landscape, however, the need for a broader, R&D-focused public-interest agency like the one envisioned by Bush remains a compelling idea for advocates for the expansion of U.S. federal government-supported scientific R&D.

  A Department of Technology and Innovation should not, as its sole purpose, be created to regulate the technology or scientific R&D industries to the point of stifling innovation. Rather, the Department of Innovation and Technology should be provided with tools and resources to encourage existing R&D innovation across the U.S. government and in the private sector. Combining an innovation entity with a regulatory entity might offset the possibility that the agency could restrain industry and R&D innovation.

  Although the broader U.S. government is unlikely to catch up to the speed of the private sector as it relates to technology, it could provide the lead in considering the public purpose and public interest elements of those advancements. It could also provide value by providing expert evaluations of the second and third-order implications of technology advancements and their impact on society.

  A Department of Technology and Innovation should also use its resources to encourage innovative organizations, like an entity designed to promote "moonshot" projects within the Department of Technology and Innovation, and that would encourage the development of cutting-edge technologies that serve the public interest.

94 "Science, the Endless Frontier," A Report to the President, by Vannevar Bush, Director of the Office of Scientific Research and Development, July 1945. https://www.nsf.gov/about/history/EndlessFrontier_w.pdf

- **Include accountability mechanisms in its design.** Any organization can be politicized but ensuring that there is bipartisan representation within the organization as well as apolitical civil servants and an inspector general and office of the Ombud will be crucial to protecting the organization from being weaponized for political purposes. For this reason, including four Senate-confirmed Advisors to the Secretary of the agency, two from each party for terms of at least six years, might help mitigate the politicization of the organization. To avoid bureaucratic bloat, Congress might also consider three Advisors– with the President's party in the majority.

- **Facilitate representation of the expertise in each of the existing agencies.** Because most organizations know their technology and technology needs best, the Department of Technology and Innovation should not strip agencies of their expertise, but rather include a Principals Coordination and Communications Committee, and Deputy Principals Coordination and Communications Committee comprised of the heads (Principals) of existing agencies and their deputies. This element of the Department of Technology and Innovation would be designed like the President's National Security Committee, and subject to review following a human-centered design research process.

- **Foster collaboration with international peers.** Congress has attempted to address internet and social media harms by empowering the FTC and providing it with greater resources. However, the FTC does not have the authority to coordinate and collaborate with international peers. Empowering the Department of Technology and Innovation to work with international institutions and peer organizations could help improve the United States' current lead on standards-setting and countering authoritarian censorship of the internet.

- **Encourage collaboration with the State Department's Global Engagement Center.** Given that Congress has tended to conflate misinformation and disinformation in legislative hearings, it could be problematic to create a bureau of disinformation within the Department of Technology and Innovation. However, it might be valuable to create an engagement mechanism with the State

Department's Global Engagement Center, or to re-activate the Active Measures Working Group to engage with the new agency, as well as with existing cybersecurity agencies. Some of the harms the agency will be tasked with addressing will likely involve the impact of digital disinformation efforts, and it should be equipped with experts and the authority to help the U.S. government develop a coordinated, whole-of-society approach to it.

- **Include various bureaus for ethics, civil rights, civil liberties, etc.** Congress has attempted to establish offices and entities to ensure that the privacy of Americans is protected, that their civil rights and civil liberties are ensured, and that promotes innovations like the national research cloud for artificial intelligence. The Department of Innovation and Technology should ensure those rights are protected by both the government and the private sector.

  Suggested Bureaus for the Department of Technology and Innovation:

  - Bureau of Civil Rights and Civil Liberties
  - Bureau of Privacy
  - Bureau of Innovation
  - Bureau of Emerging Technologies
  - Bureau of Resilience
  - Bureau of Research
  - Bureau of Digital Services
  - Bureau of Infrastructure and Telecoms
  - Bureau of Intelligence
  - Bureau of Global Affairs
  - Bureau of Information Security
  - Bureau of Ethics
  - Office of the Technology Inspector General
  - Office of the Ombud

- **Provide better information for the government and the public about emerging threats.** Having a dedicated agency to prepare regular status reports on and predictive models for the technology sector as well as to identify threats related to the technology industry like the Department of Defense's Annual Threat Assessment would help enhance the accountability of the industry and regularly and reliably inform the public and the industry about threats and trends the technology sector presents.

- **Continue regulation by vertical with a slight adjustment.** The U.S. currently regulates technology by verticals--- medical devices are regulated by the FDA, for example. However, the FDA is currently considering how to regulate AI in medical devices, when there is no entity that fully regulates AI. A Department of Technology and Innovation could leverage its expertise in AI to advise the FDA via the Principals Coordination and Communication Council. As mentioned, the Consumer Product Safety Commission (CPSC) could regulate AI, but as mentioned, they are not powerful enough to be very effective.

- **Ensure organizations like the National Academy of Sciences remain independent.** If the Department of Technology takes on some of the issues that Congress has previously tried to direct to the National Academy of Sciences or other entities, those valuable, independent, and apolitical organizations can continue doing rigorous scientific work. As mentioned in Part I, social media research comprises several disciplines and is not a traditional or standardized science. It should not be absorbed by organizations that are known for their apolitical, robust, scientific expertise in specific areas.

- **Harmonize issues where agencies overlap in jurisdiction.** For example, tobacco products are regulated by the FDA, but the FCC regulates billboard and television advertisements about tobacco products directed at children, and the FTC regulates those same ads online. The agency could harmonize those approaches through the Principal Coordination Council and the Deputy Coordination Council, subject to a human-centered design research process, so that they are more efficient, effective, and include relevant expertise.

The Department of Technology and Innovation should be approached thoughtfully to avoid the jurisdictional and other issues new agencies like the Department of Homeland Security have encountered, and to protect against perpetuating inefficient, bureaucratic bloat. There are, however, innovations in design, research, and funding mechanisms that could be leveraged toward a new effort to address an increasingly unruly and potentially threatening technology landscape, and the technology weaknesses across the U.S. government. Congress can also iterate on the Department of Technology and Innovation if it does not serve the purposes for which it was created or the needs of the American people.

Congress should also consider fully investing in its own Article 1 authority and, as it did in 1946 after the crisis of WWII, and again in the 1970's, due to concerns over what was called the "imperial Presidency", and Watergate and the Vietnam War.[95] Similarly, Congress could consider reorganizing itself to conduct better oversight of a new technology agency, as well as those currently in existence. Such a reorganization might enable Congress to better address future threats and challenges to the United States.

Finally, the Department of Technology and Innovation, both in its creation and in the authorities it is granted by Congress, should consider the strategic interests of the United States, and how such an agency could better equip the United States to mitigate and withstand future threats and crises.

The current Administration and the 117th Congress, having weathered multiple crises domestically and globally during which technology played a critical role, is uniquely poised to ensure it, the U.S. government, our international partners, and the public are better equipped for an uncertain future.

95 Wolfensberger, Donald. "A Brief History of Congressional Reform Efforts," Bipartisan Policy Center, February 22, 2013.

# Appendix

## Policy Proposals and Harms

| General Policy Area Regulated | Harms to be addressed[1] | Example of policy proposals in the 116th/117th Congresses |
|---|---|---|
| Disinformation/ Foreign Influence | Usually strategic and reputational, i.e. enhance the stature of the state actor, diminish the global stature of the U.S. , enhance the military capabilities of the state actor, diminish US capabilities, restore state actor influence at the expense of the U.S., sow chaos, increase polarization, and societal fragmentation. | • Honest Ads Act<br>• Combatting Foreign Influence Act<br>• Hijacking Our Heroes: Exploiting Our Veterans Through Disinformation Act<br>• Anti-CCP Espionage via Social Media Act of 2021<br>• Special Russian Sanctions Authority Act of 2022<br>• United States Information Abroad for Strategic Competition Act |
| Misinformation/ Content Moderation/ Technical Architecture and Design (most of these proposals also include an element of Section 230 as well, but are related specifically to content issues more than directly to Section 230) | Mental and public health, terrorist recruitment, violence, false news, harassment, incitement to violence. | • Deceptive Experiences to Online Users Act (DETOUR)<br>• Health Misinformation Act of 2021<br>• Stop Shielding Culpable Platforms Act<br>• Justice Against Malicious Algorithms Act of 2021<br>• Preserving Political Speech Online Act<br>• The Disincentivizing Internet Service Censorship of Online Users and Restrictions on Speech and Expression Act (DISCOURSE)<br>• Protect Speech Act<br>• SAFETECH Act<br>• Protecting Americans from Dangerous Algorithms Act<br>• Platform Accountability and Consumer Transparency Act (PACT Act)<br>• See Something Say Something Act of 2021<br>• CASE-IT Act<br>• Protecting Constitutional Rights from Online Platform Censorship Act |

1 This is a high-level overview of the more detailed Harms Taxonomy developed as part of this research and that will be featured in a subsequent publication..

| General Policy Area Regulated | Harms to be addressed[1] | Example of policy proposals in the 116th/117th Congresses |
|---|---|---|
| Section 230 (directly repealing or primarily focused on Section 230) | Social media platform immunity from civil litigation, hate speech, harassment, incitement to violence. | • Violence Against Women Act<br>• A Bill to Repeal Section 230 of the Communications Act of 1930<br>• The Accountability for Online Firearms Marketplaces Act of 2021<br>• 21st Century FREE SPEECH Act<br>• Abandoning Online Censorship Act |
| Data Privacy and Protection | Surveillance, profiling, targeting, lack of consent, invasion, information dissemination without consent, public embarrassment, false representation. See Solove's Taxonomy of Privacy.[2] | • The Data Elimination and Limiting Extensive Tracking and Exchange Act (DELETE)<br>• Social Media Privacy Protection and Consumer Rights Act of 2021 |
| Creation of a new technology regulatory entity | Coordination and enforcement issues. | • Misinformation and Disinformation Task Force of 2020<br>• Deepfake Taskforce Act |
| Research requirement | Lack of empirical data on harms, understanding of nefarious behaviors and the impact of them. | Covid-19 Disinformation Research and Reporting Act of 2021 |
| Antitrust | Lack of industry competition, predatory business practices. | Federal Big Tech Tort Act of 2020 |
| Industry-wide duties | Inconsistent standards for different companies. | Efforts to define what industry social media technology companies are.[3] |

2 See Solove's Taxonomy of Privacy https://wiki.openrightsgroup.org/wiki/A_Taxonomy_of_Privacy

3 Don't Ask Whether Facebook Can Be Regulated, Ask Which Facebook to Regulate. August 19, 2018. https://www.vox.com/technology/2018/4/12/17224096/regulating-facebook-problems

**Technology and Public Purpose Project**
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
belfercenter.org/project/technology-and-public-purpose



Printed in the United States of America