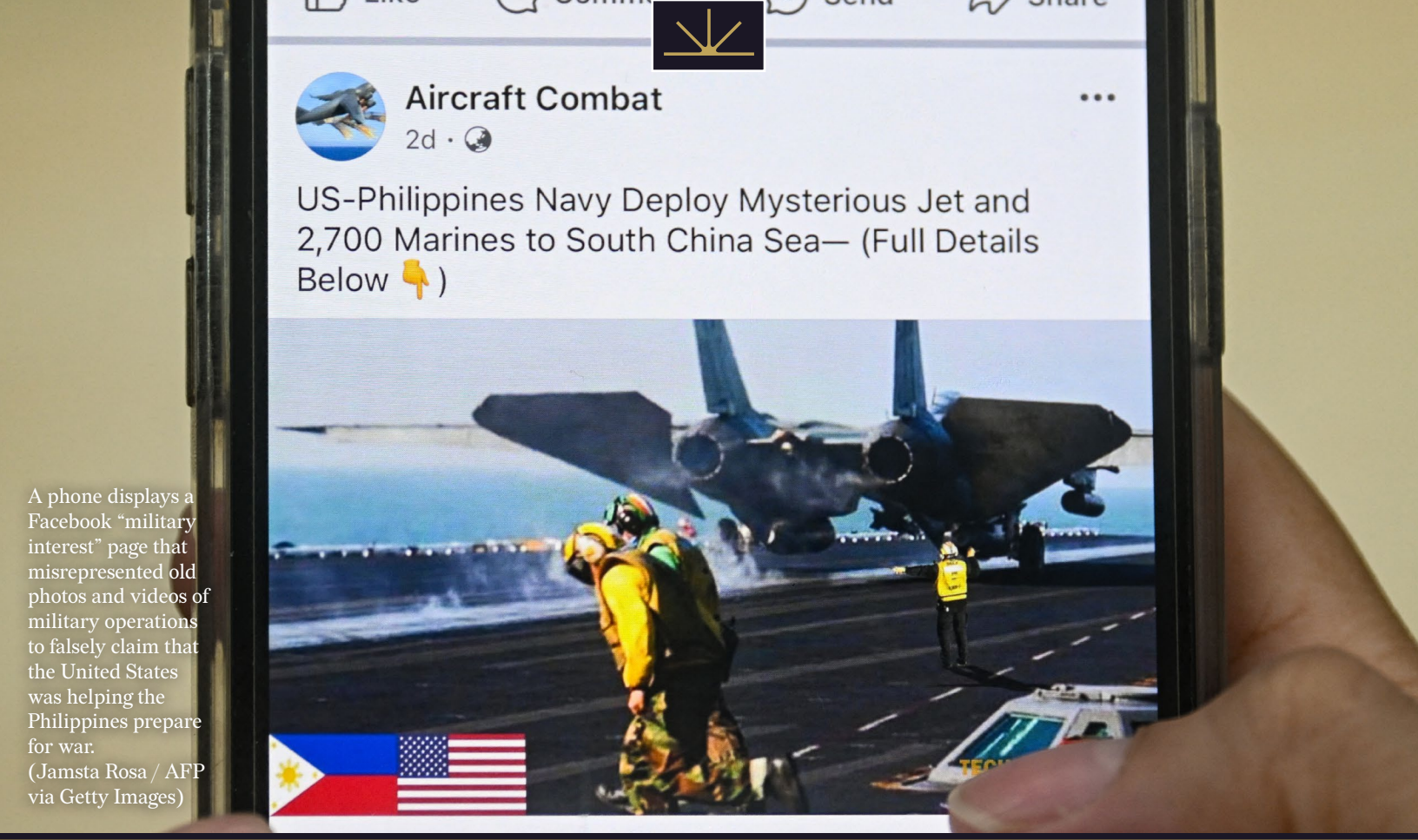


A phone displays a Facebook "military interest" page that misrepresented old photos and videos of military operations to falsely claim that the United States was helping the Philippines prepare for war. (Jamsta Rosa / AFP via Getty Images)

The Double-Edged Sword: How to Win the War on Fake News

Sam Douglas-Bate

Introduction

Misinformation, defined as false content a publisher believes to be true, and disinformation, defined as false content that a publisher knows to be untrue, pose major threats to U.S. society. Most adults in the U.S. report seeing false or misleading information online at least weekly.[1] Artificial intelligence (AI), augmented and virtual reality, the "internet of things," and wireless technologies are increasingly bringing people together but have also elevated their exposure to fake news, which comprises both misinformation and disinformation. Events such as the riot at the U.S. Capitol on Jan. 6, 2021, may become more common as people are influenced by real and fake social media accounts, bot networks, and troll farms deploying fake news that leads to unrest. However, new technologies are a double-edged sword: They can provide defenses to false and misleading information though technologies such as digital watermarks, AI classifiers, user dashboards, and application programming interfaces (APIs) that make it easier for people to sort what is true from what is false.

In the runup to the 2024 presidential election, a "whirlwind"[2] of fake news around voter fraud emerged on social media platforms. Federal investigators described Russia as the "most active threat"[3] during the period with alleged Kremlin-backed online accounts posting and amplifying articles pushing false election fraud narratives. For example, U.S. intelligence agencies explained that one widely shared piece of content, which allegedly showed people from the

Haitian community illegally voting, was fabricated by "Russian influence actors."[4]

While Russia represents a bigger existing threat, the risk of similar activity from China needs to be taken seriously given geopolitical competition is likely to escalate during the Trump presidency. While the National Intelligence Council (NIC) assessed that Beijing did not attempt to influence the 2020 presidential elections,[5] an increase in the spread of fake news by Chinese-linked actors was seen in 2024. The prospect is more alarming in light of China's online information campaigns. While measuring the levels of fake news originating from sources is fraught with complexity, the country undoubtedly plays host to one the world's most sophisticated influencing operations.

"Spamouflage," also known as "Dragonbridge," is a wide online network of Chinese actors that has sought to promote Beijing's national interests by creating and posting fake news. Microsoft estimates Spamouflage's influence operation targets 175 websites and 58 languages.[6] Meta announced in August 2023 that it had taken down thousands of China-linked Facebook pages and claimed it to be the "largest known cross-platform covert influence operation in the world."[7] U.S. policymakers must act accordingly.

The spread of fake news is a cross-cutting issue that adds fuel to the fire by augmenting three areas prioritized by lawmakers in their interaction with Beijing:[8] competition in the South China Sea, hacking of U.S. infrastructure,[9] and economic competition. Furthermore, any fake news, whether from China or elsewhere, has widespread implications for public trust in government, the electoral process, and much more besides.

The War of Words

Ever since the Chinese Communist Party came to power, China and the U.S. have exchanged terse diplomatic language on issues pertaining to influence over each other's national life. This stands in stark contrast to China's well acknowledged and publicly proclaimed commitment of noninterference in other countries' internal affairs.[10] In many cases, the two have accused each other publicly of spreading fake news. As recently as February 2023, Chinese representatives to the U.N. claimed the U.S. had used biological weapons in North Korea in the 1950s,[11] an accusation the U.S. strongly denies.[12] China has accused the U.S. military of spreading "anti-vax" misinformation during the COVID-19 pandemic, a claim that was backed up by Reuters research.[13] More recently, these claims surfaced again on Chinese social media.[14]

The risk of Chinese-backed actors spreading fake news is increasing. Despite the NIC's assessment of the 2020 vote, research from Microsoft found that Chinese influence campaigns targeted the 2024 elections and were focused on Republican candidates who had known "anti-China" stances. These accounts "parroted antisemitic messages, amplified accusations of corruption, and promoted opposition candidates."[15] Analysis concluded that Spamouflage accounts did not favor one presidential candidate but instead focused on down-ballot elections to sway local results. Influence attempts by Beijing-backed actors included impersonating Americans, spreading inflammatory messaging[16] on cultural issues, and even amplifying Russian interference attempts.[17]

The Impact of Foreign Influence Campaigns

While China has been culpable of spreading fake news in the U.S., Russia is often cited as the main state orchestrator of such campaigns. It is worth noting, too, that recent conspiracy theories, such as that the U.S. government manipulated Hurricane Milton, or relating to the motivations behind the assassination attempt on Donald Trump in Pennsylvania , originated in the U.S. rather than abroad. Domestic technology can also be to blame for false information, with recent research by Full Fact showing that Amazon Alexa, partly built in California and accessible via half a billion devices globally, has supplied users with incorrect information on a number of important topics.[18]

However, because of China's rapidly increasing technological maturity, policymakers need to take a new approach to counter fake news from Beijing-linked actors. The Canadian Centre for Cyber Security (CCSC) singles out China specifically for its "massive" data collection campaigns, which allows it to collect "billions of data points on democratic politicians, public figures and citizens around the world."[19] This was brought into sharp focus most recently in March 2025, when the DOJ charged 12 Chinese nationals, including officers from China's Ministry of Public Security (MPS), with stealing data. The DOJ's announcement also revealed

that the MPS and the Ministry of State Security "employed an extensive network of private companies and contractors in China to hack and steal information in a manner that obscured the PRC government's involvement." Both ministries were paying hackers "handsomely" for this data, with victims including U.S. federal and state government agencies."[20] Chinese President Xi Jinping has talked openly of using AI in "news collection, production, distribution, reception and feedback,"[21] state-backed media outlets have talked about its relevance for "construction of international communication capabilities,"[22] and researchers have claimed the Chinese military is "clearly interested"[23] in leveraging AI for social media manipulation.

Chinese fake social media accounts, bot networks, troll farms, and content farms, as well as more traditional state-run media and wolf diplomacy, have been used to push fake news. Chinese actors are increasingly using new technologies including deepfakes and generative AI to create a large amount of new content quickly.[24]

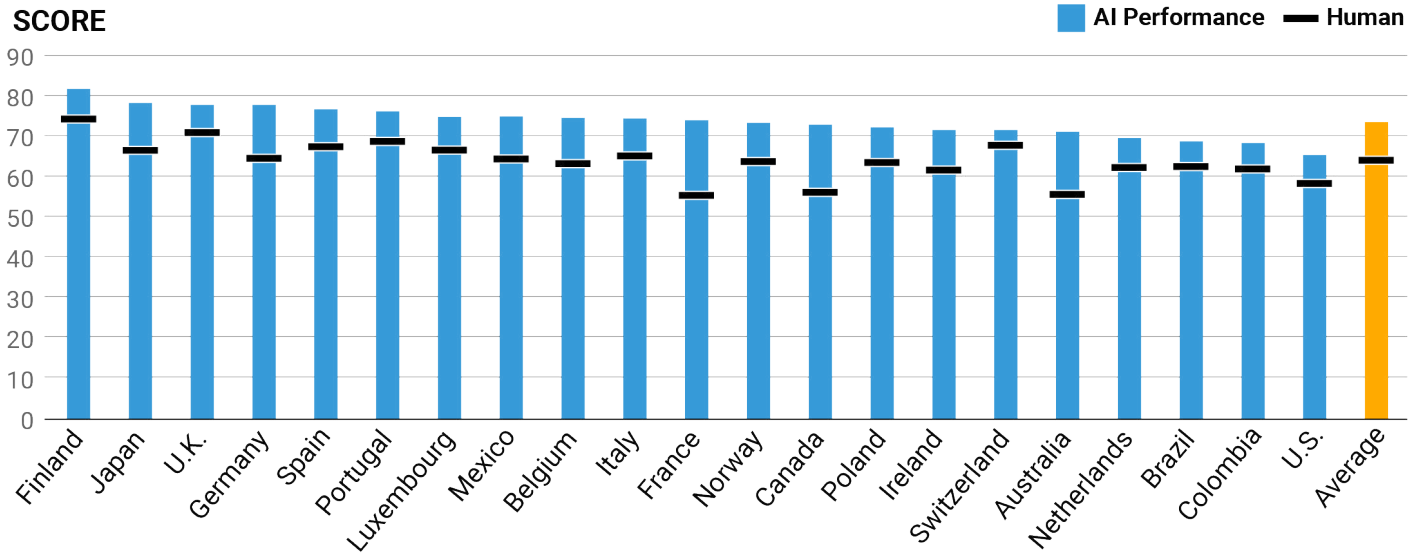
Tackling the growing issue requires balancing freedoms, such as the First Amendment, with penalties for foreign actors spreading fake news. Domestic approaches to combating the issue could include establishing incentives for the private sector to provide new ways of delivering impartial fact-checking and, as seen with the use of X's established and Meta's new Community Notes programs, encouraging the public to have the agency to do their own research. Any government approach should be consistent regardless of the source of the fake news, whether foreign or domestic.

Beijing's influence campaigns have not improved China's image among U.S. citizens. In the last five years, Americans claiming to have an unfavorable view of the country has grown from 47% to 81%.[25] However, fake news campaigns are complex, and reversing such a trend may not be the primary goal of Chinese actors.

A survey by the Organization for Economic Cooperation and Development (OECD) of citizens in 21 countries shows that U.S. users rank last in their ability to identify AI generated disinformation and third-to-last in their capability to recognize human generated disinformation (see Graphic 1).[26] The AI statistic is particularly alarming when considering the ease with which malign actors can now quickly create large influence campaigns in any language online. There is a distinct likelihood that these campaigns will become more sophisticated and believable in the future as technologies, such as deepfakes, improve.

A large majority of U.S. users are worried by the threats posed by AI, with one 2023 study from Morning Consult and Twitter showing 70% are concerned about its ability to spread misinformation. The same proportion are troubled by its use by foreign powers

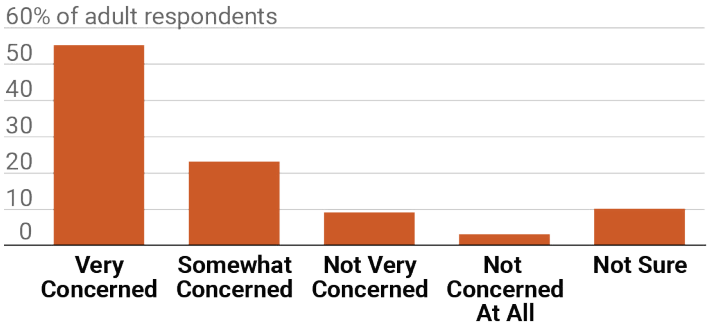
Scoring AI and Human-Generated Disinformation



Source: OECD

Concerns About AI Propaganda

Survey results of adults in the United States from 2023



Source: Statista

against U.S. interests, and 68% are worried about the creation of deepfakes.[27] Research undertaken by YouGov in the same year shows 78% of U.S. adults are either "very" or "somewhat" concerned about AI's use in spreading political propaganda,[28] making it imperative for policymakers to take a proactive stance in tackling these concerns.

Data around the numbers of Americans who regularly fact-check is limited. The available information on the topic is generally either out of date, based on low sample sizes, or analyzes populations beyond the U.S. Nevertheless, there is evidence to suggest that U.S. citizens:

1. Have low confidence in their fact-checking abilities: A Pew study in 2020 found that 71% of people held low confidence in their ability to check information relating to COVID-19.[29]
2. Are often unable to locate the source of fake news: A survey of 3,446 people in 2019 found that 52% of respondents thought a fake video from Russia showed "strong evidence" of election fraud during the 2016 Democratic Party primaries. In addition, only three people were able to locate the true origin of the video.[30]
3. Visit untrustworthy websites regularly: A survey found 44% of people visited untrustworthy sites during the 2016 U.S. presidential election campaign. The authors defined such websites as "lack[ing] the news media's editorial norms and processes for ensuring the accuracy and credibility of information."[31]
4. Are more likely to trust fake news that aligns with their political views: A 2022 study of U.S. Democrats found that demand for fact-checking in a political newsletter rose when it contained information from Fox News. However, fact-checking did not have a significant impact on demand for the newsletter where information from MSNBC was included.[32]
5. Hold differing views of fact-checking: Conservative Republicans hold less favorable views toward fact-checkers, while people interested in and knowledgeable about politics tended to be more favorable.[33] Similar results have been found among Europeans. The data suggests those most at risk of believing fake news could be on the right and/or less engaged with the political process, although this conclusion is hotly debated.

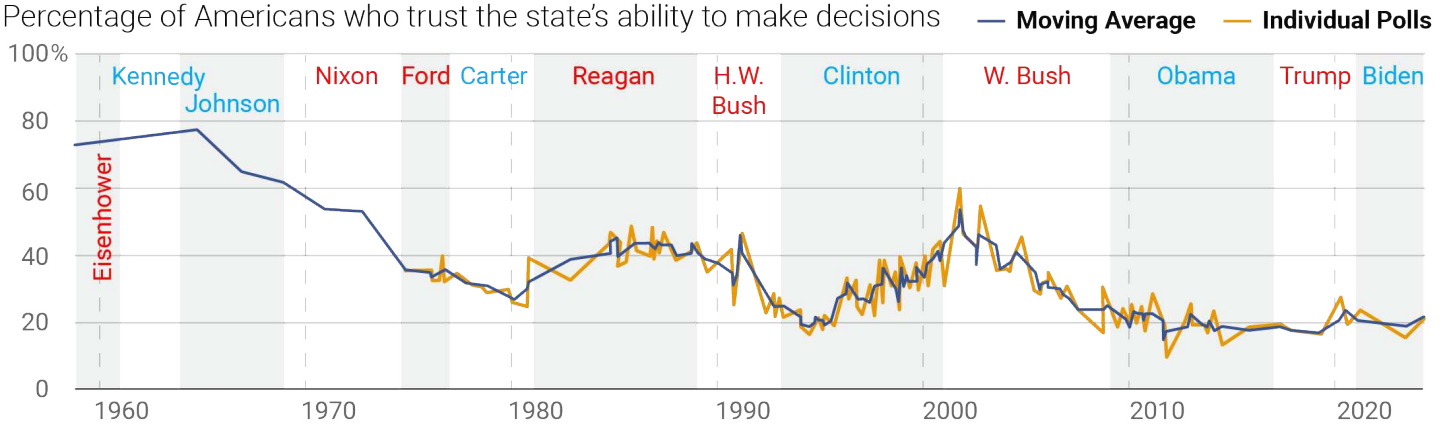
Taken together, these studies paint a picture of an American public ill at ease with differentiating truth from fabrication online. U.S. policymakers need to ensure the public is aware of the power of AI, or the outlook could become even more concerning.

The biggest threat of foreign influence campaigns is the ability to undermine trust in government and potentially stoke civil unrest. In 1964 trust in the U.S. government was at an all-time high. That sentiment underwent an alarming decline in over the next four decades, reaching historic lows in 2011.[34] That decline is not just a U.S. phenomenon. Distrust in government institutions internationally is a trend well-acknowledged by the United Nations[35] and the OECD.[36] It is difficult to draw a direct line between fake news from international influence campaigns and this trend, but it would be hard to argue that Spamouflage, or the alleged Russian-backed influence campaign called Doppelganger, do not add fuel to this fire in the U.S.

Another public policy challenge is the power of foreign influence campaigns to use fake news to fan the flames of quickly emerging national crises when information is scarce. For example, during the 2024 United Kingdom riots, or both the Pennsylvania and Florida assassination attempts on Donald Trump, fake news from a myriad of sources spread quickly. The power social media platforms hold in these cases is significant. Meta has an escalation process for restricting accounts of high-profile users

Government Trust Falls to an All-Time Low

Percentage of Americans who trust the state's ability to make decisions



Source: Pew Research

during periods of civil unrest, given their potential to supercharge the spread of fake news.[37] In 2021, the company indefinitely suspended Trump's Facebook and Instagram accounts following his praise for people involved in the Jan. 6, 2021, assault on the U.S. Capitol and the alleged risks this posed for further violence. The suspension, which was later reduced to two years on the advice of Meta's Oversight Board,[38] was ultimately lifted in January 2023 with "guardrails" and heightened repercussions for further violations. The restrictions were removed as presidential candidates geared up for their respective party conventions in 2024.[39]

Social media platforms walk a tightrope: For a pro-Trump Republican, the removal of a post about immigration that violates community guidelines might be considered censorship, but for a Democrat the same act might be viewed as a responsible reaction to inflammatory messaging. Oftentimes, moderating content involves a subjective assessment of the information in question, an assessment that Meta CEO Mark Zuckerburg recently called out as all too often being "politically biased", when he removed human fact checkers and replaced them with community moderation.[40] It can also include a more objective assessment of whether content violates a platform's user policies, which will have been established by consensus among a group of colleagues with subjective views.

Censorship arguments have divided U.S. lawmakers, society, and the social media platforms themselves. Platforms should not get Section 230 protection , which sees them given immunity for content published by users, if they censor online speech. Therefore, it is incumbent on all sides to find agreement in a unified goal: Tackling state-backed influence campaigns and fake news should be the objective, and achieving this requires close collaboration between the public and private sector. As a first step, Federal Communications Commission Chairman Brendan Carr, should undertake a review with platforms to understand how their policies are implemented in practice, including at times of national crisis.

The Double-Edged Sword

Technology's Role in Spreading Fake News

Beijing-linked organizations have been accused of using sophisticated technologies such as Synthesia[41] and CapCut[42] to create fake videos and OpenAI tools to undertake intelligence analysis.[43] OpenAI's Sora and Google's Veo 2,[44] generation models that create sophisticated moving images from language prompts and photos uploaded from a user, have the power to further supercharge the ubiquity of misleading footage originating abroad.[45] Research from the CCSC shows the stark reality of the growing problem. The organization analyzed 151 global elections held in 2023 and 2024, concluding 41 had interference from generative AI. By comparison, there was only a single case between 2021 and 2023. Examples included creating and spreading disinformation and harassing politicians. China constituted a "high number" of these threat activities between 2023 and 2024, and it was assessed as "almost certain" that the country "leverage[s] generative AI to spread disinformation narratives" and "very likely" they will continue.[46] Gary Marcus, AI expert and professor emeritus at New York University, described the stark potential of AI

tools to spread misinformation which in the worst case scenario could "lead to an accidental war that escalates and becomes a nuclear war."[47]

In 2023, the Australian Strategic Policy Institute uncovered a huge campaign of pro-China AI-generated YouTube videos it called " Shadow Play." At the time of publication, the campaign included "at least" 30 channels, over 4,500 videos, 120 million views and 730,00 subscribers."[48] Fake news from China is not confined to the most popular social media platforms; Spamouflage-linked accounts have also been detected on Bluesky and Mastodon. Closer to home , a disgruntled ex-employee of a Baltimore school was charged with spreading an audio deepfake falsely depicting the school's principal making racist comments.[49] This case study has stark implications for the use of AI tools: Their ability to be used by non-specialists, their relative sophistication compared with only a few years ago, and their potential for generating community-level division. If such methods can be instigated by actors at home, it emphasizes their ability to be employed by an increasing number of untrained actors abroad.

The acquisition of sophisticated technology from overseas could enhance the ability of China-backed actors to spread fake news. However, U.S. authorities have tightened their grip on exports that help develop AI. The Foreign Direct Product Rule (FDPR), first established in 1959, has become crucial over the last decade in efforts to limit sensitive U.S. exports. In 2019, the Bureau of Industry and Security took action against Huawei, and then in 2022 wider controls were put in place on other Chinese companies limiting the transfer of code, electronics, chips, and supercomputing capabilities.[50] In the final days of the Biden presidency, the FDPR was further deployed to stop exports to a further 140 entities, with new controls on semiconductor manufacturing and software tools and the high-bandwidth memory crucial to training AI.[51] Alongside the U.S., other allies, including the United Kingdom,[52] the Netherlands,[53] and Japan[54] have passed rules with various success. When FDPR and international action is taken, technology companies often halt their dealings with Beijing. These moves have significant implications for China's ability to develop its AI sector and therefore create new technologies for propagating fake news.

However, U.S. policymakers need to analyze the effectiveness of the FDPR. Chinese companies and researchers can continue to make progress in their ability to spread fake news by circumventing technology bans.[55] ByteDance rents Nvidia chips via Oracle's U.S.-based operations, and there is a possibility Alibaba and Tencent may do the same.[56] Likewise, semiconductor intermediary dealers enable businesses in China to get around the controls by selling to the domestic market from third countries.[57] In addition, China has boosted subsidies to chip makers , restricted sales of critical minerals to the United States, and launched an antitrust investigation into Nvidia.[58] All the while companies based in the country, including Huawei, continue to make progress in their development of advanced semiconductors. Chinese large language models (LLMs) saw significant improvements in 2024, with the strongest ones produced by companies like DeepSeek, Alibaba, 01.AI and Zhipu AI, often with lower training cost than their US competitors.[59,60] If U.S. policymakers want to tackle the increasing role of AI in spreading fake news, it needs to review its response to these wider export and technology issues.

On taking office, Trump revoked Biden's executive order on AI,[61] claiming it hinders innovation,[62] replacing it with a new policy aimed at promoting "human flourishing, economic competitiveness, and national security."[63] Among a number of goals, the previous presidential order instructed the federal government to undertake work to "establish the authenticity and provenance of digital content," established chief AI officers in large agencies, and tasked providers of Infrastructure as a Service (IaaS) providers to submit to the Secretary of Commerce a report when a "foreign person transacts [with them] to train a large AI model with potential capability that could be used in malicious cyber-enabled activity." Goals such as these may have allowed federal authorities to identify fake news more easily and ensure state-backed actors are not using U.S. IaaS products to train AI technologies that enable this activity. Speaking at the Paris AI Summit in February 2025, JD Vance further reset U.S. government AI policy with a speech describing the technology's "revolutionary applications" to "free expression."[64] As part of its new action plan, the Trump administration will need to consider how a replacement mechanism can strike a balance by

Nick Clegg, president for global affairs at Meta, testifies during the Senate Select Intelligence Committee hearing titled "Foreign Threats to Elections in 2024 - Roles and Responsibilities of U.S. Tech Providers," on Capitol Hill on Sept. 18, 2024. (Tom Williams / CQ-Roll Call, Inc. via Getty Images)

defending new U.S. technologies, ensuring national security, and promoting free speech.

Technology's Role in Combating Fake News

While Meta's former President of Global Affairs Nick Clegg pointed out it's still "early days for the spread of AI-generated content,"[65] public and corporate enthusiasm for generative AI tools has led to their quick development. This has created a huge amount of new content and the potential for orders of magnitude more. To realistically combat the potential flood of AI-generated false content, the quality and number of defensive AI tools able to mitigate fake news needs to match the number and sophistication of the ones creating it.

Social media companies have a long history of utilizing AI classifiers to categorize huge amounts of content according to specific attributes to ensure it does not break community rules. However, when it comes to detecting fake news, the work of these classifiers often still needs to be completed by human review.[66] For example, a classifier might identify a post as misinformation, but what happens if the misinformation becomes factual truth later? Or what if a post is a joke from one user to another, or might be literally false but clearly understood by reasonable people as satire?

One solution can be found in the growing number of technologies that help uncover online information with dubious provenance. For example, the Coalition for Content Provenance and Authenticity (C2PA) standard, an alliance between Adobe, Arm, Intel, Microsoft, and Truepic, has created a specification for a cryptographically sealed manifest showing users' edits that have been made to photos, videos, and audio clips on the web.[67]

Another solution from Google called SynthID embeds a digital watermark directly into AI-generated images, audio, text, or video.[68] In the first of its kind, SynthID had been rolled into the Gemini LLM with watermarks generated alongside the response. This stands in contrast to traditional detection of AI-generated text that has taken place after it has been created. Researchers at Google found that SynthID has minimal impact on computational power and enables "better detectability"[69] than other watermark technology. Google has since released the solution as open-source code.

Efforts such as C2PA, SynthID, and social media platforms' periodic attempts to remove fake news may not be able to stem the tide. In addition to these solutions, no AI-enabled fact-checkers, from organizations such as U.K.-based Full Fact and Germany-based Factinsect, have received the levels of funding and public engagement needed to tackle the

spread of large quantities of fake news online. Much of the fact-checking around the 2024 presidential election continued to take place manually.[70] The idea of moving to an AI-first approach in the short term is implausible. However, public understanding and interaction with tools like C2PA, SynthID, and fact-checkers needs to increase significantly if U.S. policymakers want to tackle fake news seriously.

Foreign actors may not want to implement new transparency measures such as SynthID into their own LLMs. There is also an inherent risk that LLMs themselves are trained on data that itself includes fake news. In China alone, there were reportedly over 180 government-approved LLMs in 2024,[71] but the total number created by Chinese actors is likely to be much higher and growing all the time.

Three solutions might be appropriate as an interim solution while the adoption of defensive AI tools gathers momentum:

1. Better utilization and more research and development around retrieval-based approaches, where a record is kept of known AI-generated text, or post-hoc detection systems, which can detect such text after creation.
2. A meta-analysis to establish and quantify in a more robust way the scale of the problem. For example, social media platforms could introduce dashboards showing the levels of information being published that does not include visible watermarks, or which has edited provenance. This approach would become increasingly beneficial as watermarks are rolled out, while also showing users the existing underutilization of these technologies to date. Eventually these dashboards and meta-analyses must be as easily accessible to the consumer as the generative tools, avoiding the need to rely on experts, law enforcement, or academia for information.
3. Better access to platform APIs to allow researchers access to the data that may help analyze the impact of fake news. The European Commission's request for information from Meta, to ensure it is complying with the Digital Services Act's (DSA) requirement to give researchers easy, real-time access to data that might improve transparency around malicious online political content, is a first step toward international action.[72] U.S. policy makers should consider how they are pushing companies towards best practice too.

Inspiration should also be sought from Bill Gates, who is among the world's most affected targets of conspiracy theories.[73] The former Microsoft CEO has been the subject of many fake news campaigns, notably in relation to health, climate, and vaccine rollouts. For example, in 2024 a story that he had funded research into genetically engineered cattle ticks gained traction online. Gates has his own dashboards that scrape platforms for mentions of conspiracies in relation to him. Information is given on the percentage change in mentions of each inaccurate claim, as well as their reach.[74] They allow him to drill down into the detail of an individual post and track its origins. Such solutions are not out of reach: Many social media monitoring technologies track online conversation, including Sprout Social, Hootsuite, and Brandwatch. These tools can be used to identify authorship, discover who has shared posts, and analyze public sentiment[75] toward the content. Taken together these abilities can deepen the public's understanding of fake news on their social media feeds. For example, a user might be more skeptical of content that had been posted and spread from China with a negative tone toward the United States. Social media platforms could do more to ensure this information is available to users without having to use one of these third-party providers.

Academia is also leading on a number of initiatives to stop the propagation of fake news. SimPPL, a research collective from the Massachusetts Institute of Technology, creates open-access tools and new research to boost online transparency. The team has delivered an engineering framework to visualize social media interactions, evaluated the impact of LLMs in online hate speech, analyzed Chinese actors' online activity with Meta, and undertaken analysis of Reddit algorithms' ability to direct users toward fake news. They are currently undertaking a project to evaluate LLMs' propensity to share fake news and the implications of deepfakes on election integrity.[76] Is That True?, a project from the University of São Paulo, has created a chatbot on Telegram and a web-based app to help users detect fake news. The team claims over a 95% accuracy on training data and 70% accuracy on real world news.[77] The platform was

trained using the LIAR dataset, which helps develop fake news detection machine-learning algorithms.[78] Finally, researchers from Arizona State University have created a new audio deepfake detection method that measures biosignals like the vibration of vocal cords in the throat and mouth. These are then compared to the speech acoustics of the recording to confirm a common human origin with an error rate of less than 0.004%. Once recorded, audio is watermarked or cryptographically signed, confirming its genesis is authentically human and not AI.[79]

U.S. policymakers should recognize the importance of this work in repelling fake news from China and elsewhere by ensuring it is well-funded. In addition, the latest technologies that have passed peer review should be quickly incorporated into the approach of both government agencies and social media platforms to ensure powerful new technologies are not confined to academic "ivory towers." Given the fast-moving nature of developments in the sector, the government needs to improve its active engagement with the academic community tackling fake news. Ultimately, if this battle is to be won, U.S. policymakers need to embrace these new and existing technologies with the same enthusiasm the public has given to generative AI.

Social Media Algorithms

Each algorithm is a powerful unique technology. Platforms understandably need to provide users with content they find interesting, and many of their business models rely on constant user engagement. But this often traps users in "echo chambers" that reinforce a user's impression that the whole platform subscribes to their own beliefs. Often these echo chambers will contain significant amounts of fake news. This could mean that if a person is interested in conspiracy theories related to "chemtrails," there is a higher likelihood they will thereafter be shown information about alleged coverups related to 9/11, or QAnon content. Renee Diresta, a leading expert on fake news, [80] compares the effect to that of a murmuration of starlings. If one changes direction, it has a cascading effect in which the rest of the flock changes directions, too. But no one bird can see the knock-on effect it is having.[81] In the same way, an apparently innocuous share of a post or like of a page containing fake news has wider significance.

Given the power of these algorithms, more should be done to scrutinize how they work. The DSA gives EU member states the power to compel large platforms to provide access to their algorithms,[82] and the European Commission has opened investigations of both Meta's and TikTok's underlying algorithms.[83] In the U.S., the issue has been dealt with on a case-by-case basis, involving a myriad of lawsuits that challenge the algorithms used by TikTok, Google and Meta through the courts.[84] In one case against Meta, a coalition of attorneys general claim the company has set out to "purposefully addict children and teens."[85]

Following these lawsuits and the European Commission's interventions on the other side of the Atlantic, lawmakers should undertake a formal assessment. The spread of fake news online is an inherently cross-border issue; a false story seeded in China can reach U.S. users in seconds. A regulation or directive in Europe impacts users across the Atlantic. How fake news is dealt with depends on the legislative and cultural contexts of those countries, and therefore U.S. policymakers may not support Brussels' interventionist approach with legislation like the DSA. However, they should not ignore the findings of international investigations and legal mechanisms that may directly impact U.S. users too.

China's Link to U.S. Fake News

COVID-19 and Elections

The 2010-2012 Arab Spring marked a tipping point in which governments across the globe, from authoritarian regimes to democracies, realized the capability of the internet and specifically social media to deliver regime change.[86] The use of social media platforms during the protests played a multifaceted role , by making citizens "better informed, turning them into activists, facilitating public organisations and collective action, and eventually helping the development of democratic institutions that could replace autocratic regimes."[87] In the decade and a half since Mohamed Bouazizi's self-immolation catalyzed the movement, governments have responded by taking a more proactive stance in using the internet to assert their national and international geopolitical priorities. This activity covers the spectrum from truthful updates to inform the public, on to national propaganda, then

ending with some of the worst examples of fake news spread abroad.[88]

Two sets of issues have helped fuel online fake news more than any other: COVID-19 and events leading to the riot at the U.S. Capitol on Jan. 6, 2021.

Beijing-linked actors' role in spreading fake news during the height of the pandemic and afterward are well-researched.[89,90] In the early stages of the crisis, accounts linked to China downplayed its seriousness, called the virus' origins into question, proposed unscientific treatments, and questioned the efficacy of FDA-approved vaccines. In one piece of analysis over the course of nine months, the Associated Press and the Atlantic Council's Digital Forensic Research Lab found examples including the People's Daily, the country's official newspaper, "highlighting speculation" that the U.S. military brought it to China[91] and the foreign ministry broadcasting a conspiracy video claiming the virus was a U.S. biological weapon.[92] The impact on people's behavior of fake news during the pandemic is less understood, but sources including the World Health Organization and individual physicians have claimed material impacts.[93,94] By June 2020, online misinformation had inspired over a dozen people to swallow disinfectant, believing it would prevent infection. Disinformation also arguably led to unnecessary panic buying.[95] Other theories, including that powerful elites had intentionally planned the outbreak,[96] or that the threat had been exaggerated to damage Trump,[97] were also common online narratives.

While China did not attempt to explicitly influence the 2020 presidential election , the vote marked the start of a Spamouflage "breakout" of China linked-actors, according to researchers at Graphika. [98] Spamouflage was quick to react to the attack on the U.S. Capitol, with the network promoting footage of the riot with mentions of "civil war."[99] One video with links to China claimed to show someone burning ballots in Virginia, footage that was shared by Eric Trump in a post that received 1.2 million views.[100] Much of the content was amplified, perhaps unknowingly, by the official accounts of Chinese diplomats who may have been influenced by traditional media. For example, in the runup to the vote, a Chinese news website was accused of splicing "Hunter Biden material with easily provable false information,"[101] while other

Democratic Rep. Eric Swalwell reacts to a GOP member's post on X utilizing A.I. generated imagery during a House Judiciary Committee hearing about open border policies on Sept. 10, 2024, in Washington, D.C. (Tom Brenner / Getty Images)

outlets painted the attack as a result of "U.S. Society's severe division."[102]

Most recently, a September 2024 Graphika report found evidence of a Chinese "state-linked" influence operation ahead of the 2024 presidential election,[103] marking a departure from the NIC's assessment of the 2020 vote.[104] The report found that Spamouflage-linked accounts had "seeded and amplified content denigrating Democratic and Republican candidates, sowing doubt in the legitimacy of the U.S. electoral process, and spreading divisive narratives about sensitive social issues including gun control, homelessness, drug abuse, racial inequality, and the Israel-Hamas conflict."[105] A Microsoft analysis of Storm 1376 – its term for Spamouflage – found attempts to push "key issues that divide U.S. voters" in the runup to the vote by posing contentious questions on controversial domestic issues.[106]

To understand behaviors indicative of the Spamouflage network, we can assess the "Three As": activity, anonymity, and amplification, a method often used to identify bot networks.[107] These attributes can be tracked with analysis of social media networks.

On the basis of such research, Spamouflage accounts tend to feature:

1. **Activity:** Posts are often made either in inaccurate English or in Chinese. Often the content attacks Western political figures, mentions divisive issues in other countries, or promotes conspiracy theories. Additional content often describes Chinese politics and society in positive terms. Cultural references including important national symbols, events, and locations are often posted. Sometimes accounts are operated by a central actor that is automating activity. These accounts have standardized posting schedules or a quantity of posts far exceeding the rate of a normal human user.
2. **Anonymity:** Profiles can feature vague or nonexistent biographical information, making it impossible or difficult to identify the author. Sometimes profile pictures include a Chinese national emblem or an inauthentic image of a person who does not appear to be of Han Chinese ethnicity.
3. **Amplification:** Accounts with the above activity and anonymity features tend to repost each other, follow each other (so-called "follow back" behavior) and engage with prominent accounts from social media influencers and high-profile political figures in the West. Much of the content can be unoriginal and shared across multiple accounts.

On Nov. 5, 2024, accounts displaying these characteristics pushed narratives discrediting the presidential election result and amplifying anxiety about potential violence. One described the vote as a "money-burning war" in reference to the fact that U.S. elections are among the most expensive in the world.[108] After the election, a prominent post featured a cartoon from an influential pro-China artist showing Trump and Kamala Harris as puppets controlled by corporations. Others posts ridiculed Harris, claiming she was "dog-walked" by Trump.

Showing the Link

Microsoft analysis shows that China employs over 230 state media employees and affiliates who "masquerade as independent social media influencers across all major Western social media platforms."[109] This has parallels to a recent Russian campaign, uncovered by the Department of Justice and other agencies,[110] that paid western influencers to spread propaganda , which they claim they were doing unwittingly.[111] In the same way, the DOJ, FBI and wider intelligence community needs to publicly demonstrate how the Chinese state is directly responsible for fake news, rather than private Chinese citizens or entities.

This can be done with direct attribution using IP addresses or indirect attribution using geotagging or cookies. Other techniques, such as analyzing the Three As, have proved helpful. Despite these methods , the Chinese government routinely denies accusations that it runs influence campaigns targeting other countries. When accused of an online influence operation during the 2024 presidential campaign, a Chinese Embassy spokesperson said: "China has no intention and will not interfere in the U.S. election, and we hope that the U.S. side will not make an issue of China in the election."[112] When the nonprofit Network Contagion Research Institute accused TikTok of presenting information to users that gave an unequally positive view of China, a Washington-based embassy spokesperson issued a similar denial, saying the report "has no factual basis and is full of prejudice and malicious speculation."[113] Questioning the factual basis of research is a common response from Chinese embassies when responding to accusations.[114]

On the face of it, China can point to its own tough domestic laws on the spread of fake news by citing numerous pieces of legislation.[115] The Cyberspace Administration of China bans AI-generated images and video without a watermark. The Economist points out that while the Chinese Communist Party tackles "genuine misinformation," they also "label anything that contradicts the party line as such."[116]

TikTok

While national security concerns are paramount, there is also a public interest in understanding the link between China and fake news in more detail. Nowhere is this more reasonable than with the example of TikTok, which as of 2024 has around 170 million U.S. users. The bill that would ban the app in the U.S. has thrust the issue into the spotlight.[117] During TikTok CEO Shou Zi Chew's appearance before Congress in March 2023, U.S. Sen. Ted Cruz highlighted China's 2017 National Intelligence Law, which sets out that "all organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national

> "In exerting control over Chinese parent companies through formal legal means and, more frequently, the informal business culture that surrounds the PRC's legal framework, the PRC can access information from and about U.S. subsidiaries and compel their cooperation with PRC directives."
>
> **Kevin Vorndran**, assistant director of the FBI's Counterintelligence

intelligence work secrets they are aware of."[118] Chinese laws such as these are often given as evidence that Beijing is able to implement foreign influence operations through direct engagement with its society, a power that has no equivalent in the U.S.

In *TikTok v. Garland*, the case brought by the social media giant to challenge the bill, the DOJ laid out the risks posed by the app. But much of the government's July 2024 filing to the Court of Appeals for the District of Columbia was redacted.[119] Lawyers cited national security concerns for the withheld information.[120] A similar point was made by U.S. Rep. Josh Gottheimer, who drafted an earlier bill to ban TikTok, when he said, "we have seen evidence [about TikTok] in a classified setting."[121]

Currently, users understand only the broad nature of the connection. For example, in the July 2024 filing, Kevin Vorndran, assistant director of the FBI's Counterintelligence Division, laid out[122] the undetailed argument government officials often make in public forums:

> "In exerting control over Chinese parent companies through formal legal means and, more frequently, the informal business culture that surrounds the PRC's legal framework, the PRC can access information from and about U.S. subsidiaries and compel their cooperation with PRC directives. In contrast, in the United States, U.S. subsidiaries are generally treated as U.S. persons and afforded robust legal and constitutional protections."

David Newman, principal deputy assistant attorney general of the National Security Division of the DOJ,[123] concurred in the same filing, mentioning laws that "blur the line" between the public and private sector in a way that was "very different" to the way private companies operate in the U.S.

While public statements such as those from the FBI and DOJ are helpful to an extent to understand the nature of Chinese influence, when we look at the insufficiencies of TikTok's proposals to placate[124] the federal government, we are literally reading between the lines of a heavily redacted document.[125] The intelligence community needs to publicly demonstrate more clearly how the Chinese state is directly responsible for fake news, rather than Chinese citizens or private entities.

FARA

China's Global Television and its Xinhua News Agency and network were required[126] to register as foreign principals[127] under the Foreign Agents Registration Act (FARA),[128,129,130] and did so in 2019 and 2021 respectively. The law was introduced in 1938 to combat the rise of German propaganda before World War II.[131] As the DOJ looks to FARA as a tool to counter propaganda from abroad, we can perhaps look at it as a tool to tackle fake news too. The lines between state-sponsored propaganda and fake news are often blurry. Arguably, the two can in many instances be one and the same: Some of the content published by Chinese social media accounts that have spread falsehoods about Maui wildfires and the federal government's poisoning of other countries' water supplies[132] might fit into the definition of "political activities" under FARA.[133]

In September 2024, an alleged agent of Beijing, Linda Sun, was indicted on charges of violating FARA as part of her work with New York Gov. Kathy Hochul.[134] We

might need to consider the real possibility of Chinese-backed individuals being charged under FARA for online influence campaigns too.

A precedent has been set by Russia's attempt to influence U.S. political life through online activity. The day after the news about Sun broke, two RT employees were indicted under FARA related to "a $10 million scheme to create and distribute content to U.S. audiences with hidden Russian government messaging."[135] In coordinated government action, 10 individuals and two entities were sanctioned[136] and 32 internet[137] domains were seized as part of an investigation into the Russian Doppelganger program. This follows the 2018 grand jury indictment of 13 individuals as part of then-Special Counsel Robert Mueller's work on Russian interference during the 2016 presidential election.[138] The charges against the individuals were not formally dropped[139] and they have not been extradited by Moscow. The possibility that Beijing-backed individuals will face similar charges is perhaps the next milestone following China's well-known attempts at what the DOJ describes as "state-sponsored"[140] hacking as well as other infiltration attempts.[141] Given the experience with Doppelganger, U.S. policymakers should ready themselves for a similar moment with regards to Spamouflage so they can formulate a quick and effective response.

Part of the solution could be found in requiring certain agents[142] of foreign principals to flag their accounts and posts on social media. Under the terms of the act, the DOJ requires any activity undertaken within the U.S. to be reported. In recent opinions, the government has been expansive in its view on what this means, in one case saying this element was met because a foreign principal's online account was "clearly viewable in the United States."[143] Prior to the presidential election the DOJ promised to provide "more specific" guidance on labelling social media posts.[144] Attorney General Pam Bondi should build on this record by considering how her office can use the Act further. In a February 2025 departmental memo after taking office, she called for FARA to be used for "alleged conduct similar to more traditional espionage by foreign government actors," which suggests she may take an approach that does not recognize its potential for countering fake news.[145] An ambitious move would be for the new administration to instead propose social media companies proactively label suspected foreign-origin social media accounts under FARA with a precautionary principle-style approach. The user could later challenge the decision under a dispute resolution mechanism if they had been wrongly labeled.

Protecting First Amendment Rights

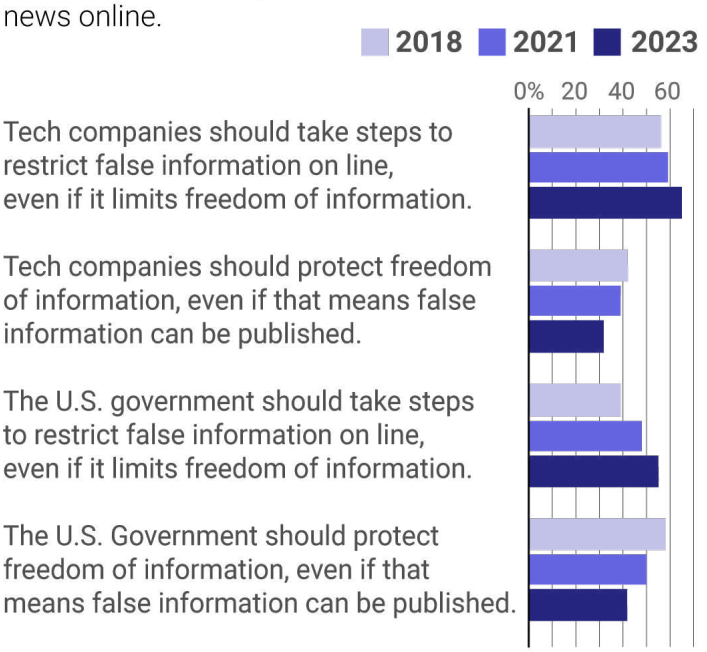
The countering of fake news from abroad must take First Amendment considerations into account. There should be a focus on checking facts without policing opinions. It is a common argument that the Bill of Rights applies to foreign nationals for conduct that takes place in the United States. The question arises whether foreign actors spreading fake news via U.S. servers therefore enjoy the protections afforded under the First Amendment.

During the *Murthy v. Missouri* case, which was decided by the Supreme Court in June 2024, the Biden administration argued it was legitimately liaising with platforms to tackle the spread of misinformation in relation to COVID-19 and elections. Then-Missouri Attorney General Eric Schmitt saw it differently, arguing government officials were "coerc[ing]" or "significantly encourage[ing]"[146] social media companies to remove views they disagreed with. This aligns with the views held by the new Trump administration. Speaking at the Munich Security Conference, Vice President J.D. Vance described how the previous administration "threatened and bullied" platforms to "censor so-called misinformation."[147] As a first step, U.S. Attorney General Pam Bondi disbanded the FBI's Foreign Influence Taskforce, which led much of the work to liaise with platforms. In her February 2025 memo, Bondi justified the decision due to the need to "free resources to address more pressing priorities, and end risks of further weaponization and abuses of prosecutorial discretion."[148]

Despite the U.S. Supreme Court's 6-3 decision favoring the Biden administration in *Murthy v. Missouri*, the issue is not settled because the majority said states had failed to establish standing[149] to sue the government as they were not able to identify "any specific speakers or topics that they have been unable to hear or follow" as a result of government action.[150]

Restricting False Information

Percentage of Americans who trust tech companies and the state's ability to make decisions about false news online.



Source: Statista

However it is notable that while the July 2024 preliminary injunction, which started the legal process toward the Supreme Court in *Murthy v. Missouri*, effectively halted much government liaison with social media companies, Judge Terry Doughty included exceptions[151] for national security, security threats, criminal efforts to suppress voting, and foreign attempts to influence elections. This exception for issues pertaining to international influence is telling. Foreign influence should warrant special treatment. Nevertheless, what constitutes international influence is inherently complex and requires close liaison and exchange of expertise between intelligence agencies and platforms. Despite this there remain important and legitimate voices who, as described in Supreme Court Justice Samuel Alito's dissent in *Murthy v. Missouri*, believe the government was putting "unrelenting pressure" on platforms "to suppress Americans' free speech."[152]

There is a risk international influence could increase dramatically if a heavy-handed attitude to fake news is now taken. U.S. lawmakers need to work out an approach that recognizes the complexity involved in analyzing sources of fake news, which could originate as part of a foreign influence campaign or have been seeded by domestic actors. This approach needs to balance the robust protection of the First Amendment with an equally robust defense against foreign influence. Ultimately, U.S. lawmakers need to decide a complex trade-off about whether they agree or disagree with a blanket right to free speech even when U.S. users are spreading fake news that has been seeded as part of a foreign influence campaigns. This is particularly true given research from Pew shows growing public approval for tech companies and government to limit false information online, even if it means limits to freedom of information.[153,154]

Recommendations

Throughout this report, several recommendations have been made specifically in relation to managing the spread of fake news from China. To summarize, U.S. policymakers should:

1. Recognize that Spamouflage is the largest cross-platform covert influence operation in the world.
2. Take the threat of Spamouflage more seriously given recent influence attempts during the 2024 presidential election, rising geopolitical competition with Beijing, and the growing technological sophistication of Chinese actors.
3. Use the precedent set by Russian online campaigns such as Doppelganger as a guide to what the future might hold for the threat posed by Spamouflage.
4. Demonstrate more readily the link between Spamouflage actors and the Chinese state. The DOJ's operation to expose the Russian government-sponsored disinformation campaign in 2024 could serve as a guide.[155]
5. Ensure the government has understood properly the limitations of the FDPR in limiting China's AI development and undertake work to close loopholes.

In addition, this report makes recommendations that have broader implications for managing the spread of fake news from all state-backed actors. To summarize, U.S. policymakers should:

1. Account for the U.S. public's difficulty in discerning truth from fake news and how to properly fact-check claims made online.
2. Work with social media platforms to understand the implementation of their user policies, particularly during times of national crisis.
3. Take a balanced approach that both supports the First Amendment and ensures platforms and agencies are able to counter international influence campaigns.
4. Consider how Trump's invalidation of Biden's executive order on AI and Bondi's disbandment of the FBI's Foreign Influence Task Force might impact the federal government's ability to counter the spread of fake news.
5. Encourage the private sector to develop defensive tools and technologies that can detect and stop the issue. These include access to public dashboards that give metrics on the provenance of posts, support to organizations developing technologies such as AI fact-checkers and watermark technologies, and pushing platforms to give wider access to data on fake news for users and researchers. These tools should be embraced with as much vigor as the public has given to generative AI.
6. Improve engagement with and funding for the academic communities studying fake news and the technologies that can tackle it. Task government agencies to rapidly incorporate the latest peer-reviewed tools into their attempts to counter fake news.
7. Undertake a formal review of findings following recent lawsuits against big tech companies in the U.S. and European Commission action in Brussels.
8. Consider how existing legislation such as FARA might be used to tackle fake news.

Finally, three additional detailed recommendations described below further support transparency, improve awareness of fake news, and help emerging platforms address the problem.

A State-Funded Fact-Checking Panel

U.S. work to combat fake news has been led by the Cybersecurity and Infrastructure Security Agency (CISA) and other partners such as the FBI. During election cycles, the National Association of Secretaries of State (NASS) and the Election Assistance Commission (EAC) also play a role. In 2020, a process was put in place[156] that allowed U.S. election officials who spot fake news to report it directly to the Elections Infrastructure Information Sharing and Analysis Center, a partnership among the CISA, the Center for Internet Security, and the Election Infrastructure Subsector Government Coordinating Council.

In the United Kingdom, the Counter Disinformation Unit was established in 2019 and makes referrals to platforms in cases of state-backed disinformation campaigns.[157] In France, VIGNIUM was established in 2021 to detect and deter foreign influence campaigns.[158] In Australia, the Electoral Commission established a register of "prominent pieces of disinformation"[159] during the 2022 federal election. In the EU, the DSA means that large platforms could face fines of up to 6% of their annual turnover if they do not take action to prevent manipulation of elections and disinformation.

When it comes to state-backed influence campaigns, intelligence organizations often discuss, analyze, and counter fake news away from public view in direct collaboration with platforms. Much of this secrecy is understandable due to national security concerns. But in the U.S., this gives rise to concerns about the implications for free speech, as seen in the case of *Murthy v. Missouri*.

A problem in virtually all jurisdictions is that organizations seeking to tackle fake news and foreign influence campaigns are spread across a myriad of different departments and agencies with different interests, roles, and responsibilities. At the same time, private sector fact-checking organizations often use different methodologies, lack public awareness, or are accused of being politically biased. The process of uncovering fake news therefore needs a figurehead organization with better public engagement, clearer transparency, political buy-in from both Republicans and Democrats, long-term funding certainty, and complete impartiality.

One solution could be a state-funded fact-checking panel researching the most egregious cases of

fake news propagation. Like many existing private sector fact-checking organizations, it could publish its findings, which would include the true sources of information and clarifications. To ensure neutrality, it might need to sit separately from the three branches of government. Membership of such a panel could be drawn from the public, legal experts, data analysts, Republican and Democratic lawmakers, issue-specific experts, and fact-checking organizations. The panel could hear cases brought from lawmakers, the government, platforms, and users, including those related to foreign influence campaigns. Once the panel's findings were made public, it would be up to the wider system to act.

The panel should be as transparent as Meta's Oversight Board, which publishes all its decisions[160] and recommendations[161] online for public scrutiny. However, the Board's role differs from that of the proposed panel in a number of key ways: It makes binding decisions on cases related to the Meta's user policies and proactive nonbinding recommendations to the company too, including in relation to misinformation. But the investigative nature of the board, the expertise of its members, its ability to hear diverse cases from different sources, and its transparent approach have made it a success.

The panel should be tasked with checking facts behind stories, not individual opinions. For example, Trump's claim that he won the September 2024 presidential debate, despite a flash poll suggesting Harris was more successful,[162] would not be a topic for the panel. However, his claim that migrants in Springfield, Ohio, were eating dogs, or comments in early 2025 about President Zelensky of Ukraine's approval ratings, might be.[163] Likewise, Joe Biden's claim that he "inherited" a 9% inflation rate on taking office,[164] or Kamala Harris' assertion that Trump would sign a "national abortion ban," or that unemployment was at its "worst since the 1930s" during Trump's previous tenure, could also be issues for analysis.[165] Fact-checking around milestone events, such as presidential debates, times of national crisis, and major speeches would be particularly important.

The panel's research would also help the wider system understand if the author was spreading misinformation or disinformation. For foreign influence campaigns this would be an important distinction given many state-backed actors would know the information they are spreading to be untrue. The panel would need the resources to move quickly, for example during periods of civil unrest, but also space to undertake longer investigations for complex or high-profile cases. It could operate with a digital first approach, with members of the public having the ability to vote on content to be reviewed.

A Government-Led Awareness Campaign

Government has a rich history of promoting information campaigns aimed at improving the lives of citizens by promoting smoking cessation, healthier eating, and the wearing of seatbelts. Examples include the Centers for Disease Control and Prevention's "Tips from Former Smokers" campaign,[166] the Department

Maricopa County election workers prepared for another onslaught of conspiracy theories in the 2024 by bulking up security and giving public tours of their ballot tabulation facility, (Patrick T. Fallon / AFP / Getty Images)

of Health and Human Services' "Risk Less. Do More" vaccines campaign,[167] the National Highway Traffic Safety Administration's "Click it or Ticket" seatbelt campaign[168] and the Department of Agriculture's "MyPlate" healthy eating campaign.[169] There have also been campaigns involving partnerships between the government and private sector, such as those focused on combating sexual assault on college campuses[170] and raising awareness of the impacts of illegal narcotics.[171]

The communications campaign to tackle fake news, however, has been a complex and overlapping effort by a range of government and nongovernment actors. Prior to the 2020 election, CISA operated a "rumor control"[172] and the NASS ran a #TrustedInfo2020 campaign. Four years later, the campaign was renewed, and other activity, such as an FBI and CISA joint public service announcement in September 2024, published a number of recommendations.[173] The impact of these campaigns in tackling fake news and increasing public understanding is unclear. They also have a wide variety of different messaging strategies, products to assist users in combatting the spread of fake news, and target audiences. This creates an unnecessarily complex set of messages for the public.

Drawing upon the experience of NASS, EAC and CISA, the U.S. government could act to bring together divergent strands into a single aligned campaign encouraging the public to do their own research. It could be targeted toward a number of "supersharers" who are responsible for spreading the majority of misinformation.[174] Given that fake news touches a range of policy areas and departmental portfolios, this campaign might have to be led directly from the White House. Alternatively, new remit could be given to the FCC as part of its broader responsibility for strengthening the nation's communications infrastructure.

The campaign could focus on the concept of prebunking,[175] which makes people aware of fake news before they encounter it, equipping them with the tools, techniques, and skeptical mindset needed to face these challenges in their day-to-day lives. One approach to making this message resonate would be to gamify the concept of prebunking.[176] U.S. authorities could build on the work undertaken by scientists at the University of Cambridge, who found that playing an interactive game called Bad News exposed participants to "weakened doses" of misinformation techniques that made the them subsequently "rate fake news as significantly less reliable after the intervention."[177] They found that this so-called "inoculation effect" of playing the game remained "stable" for at least three months.[178] Inspiration could be sought from a publicly available game drawing upon these learnings called Go Viral!, which was built by a team at Cambridge with the U.K.'s Cabinet Office in order to tackle misinformation in relation to COVID-19.[179]

Support for New Platforms

Virtually all online information platforms that claim to minimize the influence of algorithms on the user are small, with notable exceptions like Bluesky , Signal, and Mastodon. There are a myriad of other networks that claim to prioritize unfiltered content, including BeReal, Vero, Diaspora, and trustcafe.io. Some allow users to subscribe to feeds, effectively allowing them to opt out of receiving content. Others show users a stream of content, for example in chronological order, meaning they could view information from diverse sources, or only allow engagement between friends, or are messenger apps, for which in both cases the user has the power to engage with people or organizations of their own choosing. Despite the existence of these challenger brands, the biggest social media networks in the U.S. rely on algorithms to deliver a personalized experience. Eliminating algorithmic content entirely would destroy their business models.

By the same token, social networks that prioritize user choice in the content they view can be at an inherent financial disadvantage, but Bluesky, Signal and Mastodon show that strong user bases can be built. These networks are often organized around closed communities such as a Signal group, or a Mastodon private server. Bluesky allows users to select their own algorithm.[180] While fake news can appear on these networks, its spread can be contained to an extent by the walls users themselves organize around their communication and their ability to actively select the content that is shown to them.

Regardless of whether a new platform prioritizes algorithms or not, support needs to be given to new entrants that set tackling of fake news as their core mission. A new company could automatically label digitally altered content during sensitive election periods, as mandated by California's new deepfake law.[181] Or it could provide users with easily accessible dashboards showing the spread of fake news, or metrics on which posts have been shared by whom. If both sides of the aisle agree that fake news can damage society, they need to support new companies that allow users to avoid the worst echo chambers. This could also be achieved through better signposting to government support – for example with loans guaranteed by the Small Business Administration, state-level grant programs,[182] federal grant programs,[183] and tax credits.

Another approach might be to put in place a voluntary open algorithm commitment, in much the same vein as the AI commitment published by the previous White House administration, which major companies like Google, Anthropic, and OpenAI signed.[184] This commitment could outline guarantees such as to develop algorithms in a more transparent manner and prioritize research on societal risks. This would assist both the government and public in understanding how fake news could spread on social media. In addition, the executive branch could run a red-teaming exercise of algorithms, like the ones run with AI companies to analyze AI risks in 2023.[185] This exercise could identify algorithms that are most effective in stopping the spread of fake news and this would produce powerful learnings for both established and new platforms. Finally and importantly, all lawmakers should actively speak up in support of new emerging platforms as powerfully as they have in condemning the spread of fake news.

Sam Douglas-Bate is an expert on misinformation and disinformation in the modern age. Prior to establishing ForgeFront, a policy and futures consultancy, he worked for the UK Government at the FCDO and Cabinet Office. An accredited data analyst, he has led complex projects in the public and private sector related to technology, security and defence.

Endnotes

1 Watson, A. (2024, April 17). Frequency of seeing false or misleading information online among adults in the United States as of April 2023, by age group. statista. https://www.statista.com/statistics/1462057/false-news-consumption-frequency-us-by-age/

2 Wendling, M. (2024, November 3). Whirlwind of misinformation sows distrust ahead of US election day. BBC. https://www.bbc.com/news/articles/czj7eex29r3o

3 Federal Bureau of Investigation. (2024, November 4). Joint ODNI, FBI, and CISA Statement [Press Release]. https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-110424

4 Office of the Director of National Intelligence. (2024, November 1). Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts [Press Release]. https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/4014-pr-28-24

5 National Intelligence Council. (2021). Foreign Threats to the 2020 US Federal Elections (Report No. ICA 2020-00078D). https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

6 Microsoft Threat Intelligence. (2024, April 4). Same targets, new playbooks: East Asia threat actors employ unique methods. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/east-asia-threat-actors-employ-unique-methods#section-master-oc526b

7 https://scontent.fbrs4-1.fna.fbcdn.net/v/t39.8562-6/10000000_878173163681285_2523028760863660247_n.pdf?_nc_cat=100&ccb=1-7&_nc_sid=b8d81d&_nc_ohc=G7cDZGZRyN0Q7kNvgHL7iZJ&_nc_zt=14&_nc_ht=scontent.fbrs4-1.fna&_nc_gid=AGoDLE2OIiO8M66x4mjml2A&oh=00_AYAyy9ydEaaHzlNil5PDwyRpA6-EQitOOH4yJIy21E2oKA&oe=6736D308

8 The next American president will be a China hawk. (2024, October 10). The Economist. https://www.economist.com/united-states/2024/10/10/the-next-american-president-will-be-a-china-hawk

9 Cybersecurity & Infrastructure Security Agency. (2024, October 25). Joint Statement by FBI and CISA on PRC Activity Targeting Telecommunications [Press Release]. https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-prc-activity-targeting-telecommunications

10 Li, J. (2019, August 27). Conflict Mediation with Chinese Characteristics: How China Justifies Its Non-Interference Policy. Stimson https://www.stimson.org/2019/conflict-mediation-chinese-characteristics-how-china-justifies-its-non-interference-policy/

11 Permanent Mission of the People's Republic of China to the United Nations and Other International Organizations. (2023). US Hegemony and Its Perils. https://archive.is/uQSsg

12 U.S. Department of State. (2023, March 14). The Kremlin's Never-Ending Attempt to Spread Disinformation about Biological Weapons. https://www.state.gov/the-kremlins-never-ending-attempt-to-spread-disinformation-about-biological-weapons/

13 Bing, C., & Schectman, J. (2024, June 14). Pentagon ran secret anti-vax campaign to undermine China during pandemic. Reuters. https://www.reuters.com/investigates/special-report/usa-covid-propaganda/

14 Graphika. (2024). Pro-China Accounts Leverage Cartoons to Target Philippines, Blame US for South China Sea Disputes. https://launch.graphika.com/pro-china-cartoons-south-sea?utm_campaign=Industry%20Drip&utm_medium=email&_hsenc=p2ANqtz-_8nVNDJ04OdFS2wEFSj_ztLm042deM-6uvmhTYH0z5ZWNOShaJVWGvKJQBTCKRlKGL_w-WJkmBRJbJlIyOOwG1ixJ_KwHjPHjUd6nSg9uG3PYoIYc&_hsmi=314730085&utm_content=314730085&utm_source=hs_automation

15 Watts, C. (2024, October 23). As the U.S. election nears, Russia, Iran and China step up influence efforts. Microsoft. https://blogs.microsoft.com/on-the-issues/2024/10/23/as-the-u-s-election-nears-russia-iran-and-china-step-up-influence-efforts/

16 Thomas, E. (2024, April 1). Pro-CCP Spamouflage campaign experiments with new tactics targeting US. Institute for Strategic Dialogue. https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-campaign-experiments-with-new-tactics-targeting-the-us/

17 Thibaut, K. (2024, November 4). Trends in China's US election interference illustrate its longer game. DFRLab. https://dfrlab.org/2024/11/04/china-us-election-interference/

18 Turnnidge, S. (2024, October 17). Amazon Alexa users given false information attributed to Full Fact's fact checks. Full Fact. https://fullfact.org/online/amazon-echo-misleading-voice-assistant/

19 Canadian Centre for Cyber Security. (2025, March 6). Cyber Threats to Canada's Democratic Process: 2025 Update. https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2025-update

20 U.S. Department of Justice. (2025, March 5). Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns. https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global

21 Jinping, X. (2019, January 25). Political Bureau of CPC Central Committee, 12th collective study session [Speech transcript]. The State Council of the People's Republic of China. https://www.gov.cn/xinwen/2019-03/15/content_5374027.htm

22 2023内容科技发展报告（简版）. (2024, April 8). 人民网研究院. http://yjy.people.com.cn/n1/2024/0408/c458741-40211694.html

23 Beauchamp-Mustafaga, N., Green, K., Marcellino, W., Lilly, S., & Smith, J. (2024). Dr. Li Bicheng, or How China Learned to Stop Worrying and Love Social Media Manipulation: Insights Into Chinese Use of Generative AI and Social Bots from the Career of a PLA Researcher. RAND. https://www.rand.org/pubs/research_reports/RRA2679-1.html

24 Tuquero, L. (2023, December 5). How generative AI could help foreign adversaries influence U.S. elections. Politifact. https://www.politifact.com/article/2023/dec/05/how-generative-ai-could-help-foreign-adversaries-i/

25 Huang, C., Silver, L., & Clancy, L. (2024, May 1). Americans Remain Critical of China. Pew Research Center. https://www.pewresearch.org/global/2024/05/01/americans-remain-critical-of-china/

26 OECD. (2024). The OECD Truth Quest Survey: Methodology and findings (Report No. 369). OECD iLibrary. https://www.oecd-ilibrary.org/docserver/92a94c0f-en.pdf?expires=1731328150&id=id&accname=guest&checksum=6FA6F3167F0A1E74366E3CC0410C674F

27 Thormundsson, B. (2024, May 14). Share of adults in the United States who were concerned about issues related to artificial intelligence (AI) as of February 2023. statistia. https://www.statista.com/statistics/1378220/us-adults-concerns-about-artificial-intelligence-related-issues/

28 Statista. (2024, September 16). Concerns among adults in the United States about the spread of political propaganda through artificial intelligence (AI) as of August 2023. https://www.statista.com/statistics/1471069/us-adults-ai-generated-political-propaganda/

29 Gottfried, J. (2020, May 28). Around three-in-ten Americans are very confident they could fact-check news about COVID-19. Pew Research Center. https://www.pewresearch.org/short-reads/2020/05/28/around-three-in-ten-americans-are-very-confident-they-could-fact-check-news-about-covid-19/

30 Breakstone, J., Smith, M., Wineburg, S., Rapaport, A., Carle, J., Garland, M., & Saavedra, A. (2019). Students' Civic Online Reasoning: A National Portrait. Stanford History Education Group. https://stacks.stanford.edu/file/druid:gf151tb4868/Civic Online Reasoning National Portrait.pdf

31 Guess, A. M., Nyhan, B., & Reifler, J. (2020). Exposure to untrustworthy websites in the 2016 U.S. election. Nature Human Behavior, 4(5), 472-480. https://doi.org/10.1038/s41562-020-0833-x

32 Chopra, F., Haaland, I., & Roth, C. (2022). Do people demand fact-checked news? Evidence from U.S. Democrats. Journal of Public Economics, 205(1), 104549. https://doi.org/10.1016/j.jpubeco.2021.104549

33 Lyons, B., Mérola, V., Reifler, J., & Stoeckel, F. (2020). How Politics Shape Views Toward Fact-Checking: Evidence from Six European Countries. The International Journal of Press/Politics, 25(3). https://doi.org/10.1177/1940161220921732

34 Pew Research Center. (2024, June 24). Public Trust in Government: 1958-2024. https://www.pewresearch.org/politics/2024/06/24/public-trust-in-government-1958-2024/

35 United National Department of Economic and Social Affairs. (2021). Trust in public institutions: Trends and implications for economic security (Report No. 108). United Nations. https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2021/08/PB_108.pdf

36 OECD. (2023). Trust in government. https://www.oecd.org/en/data/indicators/trust-in-government.html?oecdcontrol-3122613a85-var3=2023

37 Meta. (2023, January 30). Restricting accounts of public figures during civil unrest. https://transparency.meta.com/en-gb/enforcement/taking-action/restricting-accounts-by-public-figures/

38 Oversight Board. (2021, May 5). Oversight Board Upholds Former President Trump's Suspension, Finds Facebook Failed to Impose Proper Penalty. https://www.oversightboard.com/news/226612455899839-oversight-board-upholds-former-president-trump-s-suspension-finds-facebook-failed-to-impose-proper-penalty/

39 Clegg, N. (2023, January 25). Ending Suspension of Trump's Accounts With New Guardrails to Deter Repeat Offenses. Meta. https://about.fb.com/news/2023/01/trump-facebook-instagram-account-suspension/

40 https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/

41 Lyons, J. (2023, February 11). Let's play a game: Deepfake news anchor or real person?. The Register. https://www.theregister.com/2023/02/11/deepfake_news_anchors/

42 Microsoft Threat Intelligence. (2024, April 4). Same targets, new playbooks: East Asia threat actors employ unique methods. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/east-asia-threat-actors-employ-unique-methods#section-master-oc526b

43 OpenAI. (2024, February 14). Disrupting malicious uses of AI by state-affiliated treat actors. https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/

44 https://deepmind.google/technologies/veo/veo-2/

45 OpenAI. (n.d.). Sora. https://sora.com/

46 Canadian Centre for Cyber Security. (2025, March 6). Cyber Threats to Canada's Democratic Process: 2025 Update. https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2025-update

47 From Babbage from The Economist: Gary Marcus: a sceptical take on AI in 2025, 15 Jan 2025 https://podcasts.apple.com/gb/podcast/babbage-from-the-economist/id508376907?i=1000684121035&r=1920

48 Keast, J. (2023). Shadow Play: A pro-China technology and anti-US influence operation thrives on YouTube (Report No. 77). Australian Strategic Policy Institute. https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-12/Shadow%20Play.pdf?VersionId=1_.62RpM_chdUdpm7I0da34yOfAvR0t6

49 Spring, M. (2024, October 5). The racist AI deepfake that fooled and divided a community. BBC. https://www.bbc.co.uk/news/articles/ckg9k5dvlzdo

50 Export Compliance Training Institute. (2022, December 20). Understanding the Foreign Direct Product Rule. https://www.learnexportcompliance.com/understanding-the-foreign-direct-product-rule/

51 Bureau of Industry and Security. (2024, December 2). Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications [Press Release]. https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced

52 Morrison Foerster. (2024, March 14). UK Expands Export Controls to Semiconductor and Other Emerging Technologies. https://www.mofo.com/resources/insights/240314-uk-expands-export-controls-to-semiconductor

53 Pan, C. (2024, September 16). China hit hard by new Dutch export controls on ASML chip-making equipment. South China Morning Post. https://www.scmp.com/tech/tech-war/article/3278535/china-hit-hard-new-dutch-export-controls-asml-chip-making-equipment

54 Perozo, E. (2024, September 2). China threatens to retaliate after Japan imposes export regulations. Investment Monitor. https://www.investmentmonitor.ai/news/china-threatens-to-retaliate-after-japan-imposes-export-regulations/

55 Benaich, N., & Air Street Capital. (2024). State of AI Report 2024 (Report No. 7). https://www.stateof.ai/

56 Benaich, N., & Air Street Capital. (2024). State of AI Report 2024 (Report No. 7). https://www.stateof.ai/

57 Benaich, N., & Air Street Capital. (2024). State of AI Report 2024 (Report No. 7). https://www.stateof.ai/

58 Sherman, N. (2024, December 11). Nvidia targeted by China in new chip war probe. BBC. https://www.bbc.co.uk/news/articles/cx2vkd90mk8o

59 https://www.bbc.co.uk/news/articles/c5yv5976z9po

60 Benaich, N., & Air Street Capital. (2024). State of AI Report 2024 (Report No. 7). https://www.stateof.ai/

61 Exec. Order No. 14,110, 3 C.F.R. 75191-75226 (2023). https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

62 Republican Party. (2024, July 8). 2024 GOP Platform Make America Great Again!, 9. https://prod-static.gop.com/media/RNC2024-Platform.pdf?_gl=1*1kwqi4o*_gcl_au*MjMzMjk5Mzc5LjE3MzMzNjQ1ODI.&_ga=2.79801364.2029520348.1734397581-53960822.1733364582

63 https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

64 https://youtu.be/64E9O1Gv99o?t=68

65 Clegg, N. (2024, February 6). Labeling AI-Generated Images on Facebook, Instagram and Threads. Meta. https://about.fb.com/news/2024/02/labeling-ai-generated-images-on-facebook-instagram-and-threads/

66 Meta. (2024, April 2). How fact-checking works. https://transparency.meta.com/en-gb/features/how-fact-checking-works/

67 Coalition for Content Provenance and Authenticity. (n.d.). Overview. https://c2pa.org/

68 Google DeepMind. (n.d.). SynthID. https://deepmind.google/technologies/synthid/

69 Dathathri, S., See, A., Ghaisas, S., Huang, P., McAdam, R., Welbl, J., Bachani, V., Kaskosoli, A., Stanforth, R., Matejovicova, T., Hayes, J., Vyas, N., Merey, M. A., Bowen-Cohen, J., Bunel, R., Balle, B., Cemgil, T., Ahmed, Z., Stacpoole, K., ...Kohli, P. (2024). Scalable watermarking for identifying large language model outputs. Nature, 634(1), 818-823. https://www.nature.com/articles/s41586-024-08025-4

70 AFP Fact Check. (n.d.). US Elections 2024. https://factcheck.afp.com/list/US-elections-2024

71 Jiang, B. (2024, April 13). More than 600 million on mainland now use LLMs amid rapid growth in GenAI adoption: report. South China Morning Post. https://www.scmp.com/tech/tech-trends/article/3274328/more-600-million-mainland-now-use-llms-amid-rapid-growth-genai-adoption-report

72 European Commission. (2024, August 16). Commission sends request for information to Meta under the Digital Services Act [Press Release]. https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-2

73 Wakefield, J. (2020, June 5). How Bill Gates became the voodoo doll of Covid conspiracies. BBC. https://www.bbc.co.uk/news/technology-52833706

74 Neville, M. (Writer & Director). (2024, September 18). Truth or Consequences? (Season 1, Episode 2) [TV series episode]. In Marson, E., & Roger, C. (Executive Producers), What's Next: The Future with Bill Gates. Netflix. https://www.netflix.com/watch/81680795.

75 Bannister, K. (2018, February 26). Understanding Sentiment Analysis: What It Is & Why It's Used. Brandwatch. https://www.brandwatch.com/blog/understanding-sentiment-analysis/

76 SimPPL. Research. (n.d.). https://simppl.org/research

77 Prototypes for Humanity. (n.d.). #2024 Is That True?. https://www.prototypesforhumanity.com/project/is-that-true/

78 Deeplake. (n.d.). LIAR Dataset. https://datasets.activeloop.ai/docs/ml/datasets/liar-dataset/#:~:text=LIAR%20Dataset%2C%20is%20a%20new,%2C%20party%2C%20and%20past%20date.

79 Federal Trade Commission. (2024). OriginStory: Authenticating the human origin of voice at the time of recording. https://www.ftc.gov/system/files/ftc_gov/pdf/OriginStory-Abstract.pdf

80 See Invisible Rulers: The People Who Turn Lies into Reality.

81 Federal Trade Commission. (2024). OriginStory: Authenticating the human origin of voice at the time of recording. https://www.ftc.gov/system/files/ftc_gov/pdf/OriginStory-Abstract.pdf

82 Regulation (EU) 2022/2065. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) https://www.eu-digital-services-act.com/Digital_Services_Act_Article_69.html

83 Goujard, C., & Volpicelli, G. (2024, May 16). EU hits Meta with new probe over 'addictive' algorithms harming children. Politico. https://www.politico.eu/article/meta-hit-with-new-eu-probe-over-addictive-algorithms-harming-children/

84 Poritz, I. (2024, October 24). Meta, Google, TikTok Must Face Schools' Addiction Claims. Bloomberg. https://www.bloomberg.com/news/articles/2024-10-24/social-media-giants-must-face-school-districts-addiction-claims

85 New York State Attorney General. (2024, March 14). Attorney General James Champions Legislation to Protect Kids from Addictive Social Media Feeds in National USA Today Op-Ed [Press Release]. https://ag.ny.gov/press-release/2024/attorney-general-james-champions-legislation-protect-kids-addictive-social-media

86 Howard, P. N., & Hussain, M. M. (2013). Digital Media and the Arab Spring. In Howard, P. N., & Hussain, M. M. (Eds.), Democracy's Fourth Wave? Digital Media and the Arab Spring (pp. 17-34). Oxford Studies in Digital Politics. https://ora.ox.ac.uk/objects/uuid:05e13455-3e16-478b-b0b3-f75b58ef489c/files/m047d301ca586576dc9ba2eea1833ee0

87 Smidi, A., & Shahin, S. (2017). Social Media and Social Mobilisation in the Middle East: A Survey of Research on the Arab Spring. India Quarterly, 73(2), 196-209. https://www.jstor.org/stable/48505308

88 Schiffrin, A. (2017). Disinformation and Democracy: The internet transformed protest but did not improve democracy. Journal of International Affairs, 71(1), 117-126. https://www.jstor.org/stable/26494367

89 Kurlantzick, J. (2020, September 10). How China Ramped Up Disinformation Efforts During the Pandemic. Council on Foreign Relations. https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic

90 Wendler, J. R. (2021). Misleading a Pandemic: The Viral Effects of Chinese Propaganda and the Coronavirus. Joint Force Quarterly, 104(1). https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2884217/misleading-a-pandemic-the-viral-effects-of-chinese-propaganda-and-the-coronavir/

91 Kinetz, E. (2021, February 15). Anatomy of a conspiracy: With COVID, China took leading role. AP News. https://apnews.com/article/pandemics-beijing-only-on-ap-epidemics-media-122b73e134b780919cc1808f3f6f16e8

92 Ibid

93 Coldewey, D. (2024, May 30). Misinformation works, and a handful of social 'supersharers' sent 80% of it in 2020. TechCrunch. https://techcrunch.com/2024/05/30/misinformation-works-and-a-handful-of-social-supersharers-sent-80-of-it-in-2020/

94 World Health Organization. (2021, April 27). Fighting misinformation in the time of COVID-19, one click at a time. https://www.who.int/news-room/feature-stories/detail/fighting-misinformation-in-the-time-of-covid-19-one-click-at-a-time

95 Caceres, M. M. F., Sosa, J. P., Lawrence, J. A., Sestacovschi, C., Tidd-Johnson, A., Rasool, M. H. U., Gadamidi, V. K., Ozair, S., Pandav, K., Cuevas-Lou, C., Parrish, M., Rodriguez, I., & Fernandez, J. P. (2022). The impact of misinformation on the COVID-19 pandemic. AIMS Public Health, 9(2), 262-277. https://doi.org/10.3934/publichealth.2022018

96 Schaeffer, K. (2020, July 24). A look at the Americans who believe there is some truth to the conspiracy theory that COVID-19 was planned. Pew Research Center. https://www.pewresearch.org/short-reads/2020/07/24/a-look-at-the-americans-who-believe-there-is-some-truth-to-the-conspiracy-theory-that-covid-19-was-planned/

97 Uscinski, J. E., Enders, A. M., Klofstad, C., Seelig, M., Funchion, J., Everett, C., Wuchty, S., Premaratne, K., & Murthi, M. (2020). Why do people believe COVID-19 conspiracy theories?. Harvard Kennedy School (HKS) Misinformation Review. https://doi.org/10.37016/mr-2020-015

98 Nimmo, B., Hubert, I., & Cheng, Y. (2021). Spamouflage Breakout. Graphika. https://graphika.com/reports/spamouflage-breakout

99 Nimmo, B., Hubert, I., & Cheng, Y. (2021). Spamouflage Breakout. Graphika. https://graphika.com/reports/spamouflage-breakout

100 Hundreds of fake Twitter accounts linked to China sowed disinformation prior to the US election – report. (2021, January 28). Cardiff University News. https://www.cardiff.ac.uk/news/view/2491763-hundreds-of-fake-twitter-accounts-linked-to-china-sowed-disinformation-prior-to-the-us-election,-with-some-continuing-to-amplify-reactions-to-the-capitol-building-riot-report

101 Rogin, J. (2020, October 29). There's Chinese interference on both sides of the 2020 election. The Washington Post. https://www.washingtonpost.com/opinions/global-opinions/theres-chinese-interference-on-both-sides-of-the-2020-election/2020/10/29/49f90dfe-1a2c-11eb-82db-60b15c874105_story.html

102 Eisenman, J., & Grizzell, H. (2021, March 24). Beijing's Schadenfreude Over the Capitol Riots Conceals Deep Anxiety. Foreign Policy. https://foreignpolicy.com/2021/03/24/beijing-capitol-riot-elections-xi-jinping/

103 Graphika. (2024). The #Americans. https://graphika.com/reports/the-americans

104 National Intelligence Council. (2021). Foreign Threats to the 2020 US Federal Elections (Report No. ICA 2020-00078D). https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

105 Graphika. (2024). The #Americans. https://graphika.com/reports/the-americans

106 Watts, C. (2024, April 4). China tests US voter fault lines and ramps AI content to boost its geopolitical interests. Microsoft. https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/

107 Cybersecurity & Infrastructure Security Agency. (2018, May). Social Media Bots Overview. https://www.cisa.gov/sites/default/files/publications/19_0717_cisa_social-media-bots-overview.pdf

108 Bowden, J. (2024, October 9). 2024 election to be most expensive in history with $15.8bn spent, new report reveals. Independent. https://www.independent.co.uk/news/world/americas/us-politics/2024-trump-harris-election-spending-b2626617.html

109 Watts, C. (2023, September 7). China, North Korea pursue new targets while honing cyber capabilities. Microsoft. https://blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea/

110 U.S. Department of Justice. (2024, September 4). Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere [Press Release]. https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

111 Simon, S. (2024, September 7). DOJ says Russia paid right-wing influencers to spread Russian propaganda. NPR. https://www.npr.org/2024/09/07/nx-s1-5101895/doj-says-russia-paid-right-wing-influencers-to-spread-russian-propaganda

112 Bing, C., & Paul, K. (2024, September 3). US voters targeted by Chinese influence online, researchers say. Reuters. https://www.reuters.com/world/us/us-voters-targeted-by-chinese-influence-online-researchers-say-2024-09-03/

113 ABC News. (2024, August 29). New study alleges Chinese government is using TikTok to influence U.S. users [Video]. YouTube. https://www.youtube.com/watch?v=rsZyF5efQek

114 Embassy of the People's Republic of China in the United Kingdom of Great Britain and Northern Ireland. (2023, September 14). Embassy Spokesperson on the UK Government's response to the Intelligence and Security Committee of Parliament report 'China'. http://gb.china-embassy.gov.cn/eng/PressandMedia/Spokepersons/202309/t20230915_11143290.htm

115 Zhang, L. (2020, March 2). FALQs: Spreading Rumors and Police Reprimand Under Chinese Law. Library of Congress Blogs. https://blogs.loc.gov/law/2020/03/falqs-spreading-rumors-and-police-reprimand-under-chinese-law/

116 In China, fib online and find out. (2024, October 17). The Economist. https://www.economist.com/china/2024/10/17/in-china-fib-online-and-find-out

117 Text - H.R.815 - 118th Congress (2023-2024): Making emergency supplemental appropriations for the fiscal year ending September 30, 2024, and for other purposes. (2024, April 24). https://www.congress.gov/bill/118th-congress/house-bill/815/text

118 The Economic Times. (2024, February 2). TikTok CEO denies links with Communist Party of China, says "I'm Singaporean!" | US Senate Hearing [Video]. YouTube. https://www.youtube.com/watch?v=EVDsImdq4Yg

119 TikTok Inc. v. Merrick Garland, 24-1113, (D.C. Cir. 2024). https://www.courtlistener.com/docket/68506893/01208647195/tiktok-inc-v-merrick-garland/

120 Allyn, B. (2024, August 15). TikTok fights for survival in latest filing as ban approaches. NPR. https://www.npr.org/2024/08/15/nx-s1-5077782/tiktok-survival-filing-ban-approaches

121 ABC News. (2024, August 29). New study alleges Chinese government is using TikTok to influence U.S. users [Video]. YouTube. https://www.youtube.com/watch?v=rsZyF5efQek

122 TikTok Inc. v. Merrick Garland, 24-1113, (D.C. Cir. 2024). https://www.courtlistener.com/docket/68506893/01208647195/tiktok-inc-v-merrick-garland/

123 TikTok Inc. v. Merrick Garland, 24-1113, (D.C. Cir. 2024). https://www.courtlistener.com/docket/68506893/01208647195/tiktok-inc-v-merrick-garland/

124 TikTok Inc. v. Merrick Garland, 24-1113, (D.C. Cir. 2024). https://www.courtlistener.com/docket/68506893/01208647195/tiktok-inc-v-merrick-garland/

125 TikTok Inc. v. Merrick Garland, 24-1113, (D.C. Cir. 2024). https://www.courtlistener.com/docket/68506893/01208647195/tiktok-inc-v-merrick-garland/

126 Maza, C. (2018, September 19). Why These Chinese Media Companies Have to Register As Foreign Agents. Newsweek. https://www.newsweek.com/why-these-chinese-media-companies-have-register-foreign-agents-1128649

127 According to the DoJ's website, a "foreign principal" and be: "a foreign government, a foreign political party, any person outside the United States (except U.S. citizens who are domiciled within the United States), and any entity organized under the laws of a foreign country or having its principal place of business in a foreign country. It can also include a foreign faction or body of insurgents whose legitimacy the United States government has yet to recognize. U.S. Department of Justice. (n.d.). Foreign Agents Registration Act – Frequently Asked Questions. https://www.justice.gov/nsd-fara/frequently-asked-questions

128 United States Department of Justice. (n.d.). Foreign Agents Registration Act – Browse Filings. https://efile.fara.gov/ords/fara/f?p=1381:1:5042331505515

129 Registering under FARA is not groundbreaking in itself, many organisations from allied countries - from the UK's British Tourist Authority, to Australia's New South Wales Government - are signed up. What was noticeable was the timing and the fact that these were specifically news companies. The DOJ's China decision puts Beijing on a par with Moscow, as in November 2017 two Russian outlets were given the same treatment.

130 United States Department of Justice. (n.d.). Foreign Agents Registration Act – Browse Filings. https://efile.fara.gov/ords/fara/f?p=1381:1:5042331505515

131 FARA requires agents to provide public awareness of their activities to influence public opinion and policies in the US, maintain significant records of their work, and ensure they are transparent about materials they share.

U.S. Department of Justice. (n.d.). Foreign Agents Registration Act – Frequently Asked Questions. https://www.justice.gov/nsd-fara/frequently-asked-questions

132 Microsoft. (2024, April 4). China tests US voter fault lines and ramps AI content to boost its geopolitical interests. https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/

133 Foreign Agents Registration Act of 1928, 22 U.S.C. § 11 (2009). https://www.govinfo.gov/content/pkg/USCODE-2009-title22/pdf/USCODE-2009-title22-chap11-subchapII.pdf

134 U.S. Department of Justice. (2024, September 3). Former High-Ranking New York State Government Employee Charged with acting as an Undisclosed Agent of the People's Republic of China and the Chinese Communist Party [Press Release]. https://www.justice.gov/opa/pr/former-high-ranking-new-york-state-government-employee-charged-acting-undisclosed-agent

135 U.S. Department of Justice. (2024, September 4). Two RT employees Indicted for Covertly Funding and Directing U.S. Company that Published Thousands of Videos in Furtherance of Russian Interests [Press Release]. https://www.justice.gov/opa/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published-thousands

136 U.S. Department of the Treasury. (2024, September 4). Treasury Takes Action as Part of a U.S. Government Response to Russia's Foreign Malign Influence Operations [Press Release]. https://home.treasury.gov/news/press-releases/jy2559

137 U.S. Department of Justice. (2024, September 4). Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operations Targeting Audiences in the United States and Elsewhere [Press Release]. https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

138 U.S. Department of Justice. (2018, February 16). Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System [Press Release]. https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere

139 Dilanian, K., Williams, P., & Winter, T. (2020, March 17). Why did the Justice Department drop its prosecution of 2 firms linked to a Putin associate?. NBC News. https://www.nbcnews.com/politics/justice-department/why-did-justice-department-drop-its-prosecution-2-firms-linked-n1161886

140 U.S. Department of Justice. (2024, September 18). Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers [Press Release]. https://www.justice.gov/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state

141 U.S. Department of Justice. (2024, August 23). Florida Telecommunications and Information Technology Worker Pleads Guilty to Conspiring to Act as Agent of PRC Government [Press Release]. https://www.justice.gov/opa/pr/florida-telecommunications-and-information-technology-worker-pleads-guilty-conspiring-act

142 According to the DoJ's website, the definition of an "agent of a foreign principal" is: "someone who acts as an agent, representative, employee, or servant, or otherwise acts at the order, request, or under the direction or control of a "foreign principal"" See: https://www.justice.gov/nsd-fara/frequently-asked-questions U.S. Department of Justice. (n.d.). Foreign Agents Registration Act – Frequently Asked Questions. https://www.justice.gov/nsd-fara/frequently-asked-questions

143 Kelner, R. K., Smith, B. D., & Langton, K. (2023, May 31). DOJ Releases New FARA Advisory Opinions Affecting Digital Media Platforms. Lexology. https://www.lexology.com/library/detail.aspx?g=f8213304-a9dc-4e0d-9ae9-0b39e03f3b0b

144 Hickey, A. S., Keeler, T. J., Becker, J. H., Leibner, M., & Shah, R. (2024, January 12). The US Foreign Agents Registration Act (FARA): Key Issues to Watch in 2024. Mayer|Brown. https://www.mayerbrown.com/en/insights/publications/2024/01/the-us-foreign-agents-registration-act-fara-key-issues-to-watch-in-2024

145 https://www.justice.gov/ag/media/1388541/dl

146 Murthy v. Missouri, 23-411. 2 (U.S. Sup. Ct. 2023). https://www.supremecourt.gov/opinions/23pdf/23-411_3dq3.pdf

147 https://www.youtube.com/watch?v=XPZAtf3VRWI&t=175s

148 https://www.justice.gov/ag/media/1388541/dl

149 Murthy v. Missouri, 23-411. 9 (U.S. Sup. Ct. 2023). https://www.supremecourt.gov/opinions/23pdf/23-411_3dq3.pdf

150 Murthy v. Missouri, 23-411. 28 (U.S. Sup. Ct. 2023). https://www.supremecourt.gov/opinions/23pdf/23-411_3dq3.pdf

151 Murthy v. Missouri, 23-411. 5-6 (U.S. Sup. Ct. 2023). https://www.supremecourt.gov/opinions/23pdf/23-411_3dq3.pdf

152 Murthy v. Missouri, 23-411. 5 (U.S. Sup. Ct. 2023). https://www.supremecourt.gov/opinions/23pdf/23-411_3dq3.pdf

153 Watson, A. (2023, August 16). Public opinion on government restricting false news online in the United States from 2018 to 2023. Statista. https://www.statista.com/statistics/829242/government-intervention-fake-news/

154 Watson, A. (2023, August 16). Public opinion on tech companies restricting false news online in the United States in 2018 and 2023. Statista. https://www.statista.com/statistics/829260/tech-company-intervention-fake-news/

155 U.S. Department of Justice. (2024, September 4). Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere [Press Release]. https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

156 Center for Internet Security. (n.d.). Reporting Misinformation to the EI-ISAC. https://www.eac.gov/sites/default/files/partners/EI_ISAC_Reporting_Misinformation_Sheet102820.pdf

157 United Kingdom Cabinet Office. (2023, June 9). Fact Sheet on the CDU and RRU. https://www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru

158 Secrétariat général de la défense et de la sécurité nationale. (n.d.). Une organisation au cœur de l'exécutif. https://www.sgdsn.gouv.fr/

159 Australian Electoral Commission. (2024, April 17). Disinformation register. https://www.aec.gov.au/media/disinformation-register.htm

160 Oversight Board. (n.d.). Case Decision and Policy Advisory Opinions. https://www.oversightboard.com/decision/

161 Oversights Board. (n.d.). Tracking the Implementation of Our Recommendations. https://www.oversightboard.com/recommendation-tracker/

162 Edwards-Levy, A. (2024, September 11). CNN Flash Poll: Majority of debate watchers say Harris outperformed Trump onstage. CNN. https://edition.cnn.com/2024/09/11/politics/election-poll-trump-harris-debate/index.html

163 https://www.reuters.com/fact-check/zelenskiys-latest-approval-rating-is-63-not-4-contrary-trumps-claim-2025-02-21/

164 https://www.politifact.com/factchecks/2024/may/15/joe-biden/joe-biden-wrong-that-he-inherited-9-inflatio/

165 https://www.bbc.co.uk/news/articles/cgjv3gdxv7go

166 Centers for Disease Control. (n.d.). Tips From Former Smokers. https://www.cdc.gov/tobacco/campaign/tips/index.html

167 U.S. Department of Health and Human Services. (n.d.). Risk Less. Do More. https://www.hhs.gov/risk-less-do-more/index.html

168 National Highway Traffic Safety Administration. (n.d.). Seat Belts Save Lives. https://www.nhtsa.gov/campaign/click-it-or-ticket

169 U.S. Department of Agriculture. (n.d.). Learn how to eat healthy with MyPlate. https://www.myplate.gov/

170 It's On Us. (n.d.). Home. https://itsonus.org/

171 Partnership to End Addiction. (n.d.). Home. https://drugfree.org/

172 Cybersecurity & Infrastructure Security Agency. (n.d.). Election Security Rumor vs. Reality. https://www.cisa.gov/topics/election-security/rumor-vs-reality

173 Cybersecurity & Infrastructure Security Agency. (2024, September 12). Just So You Know: False Claims of Hacked Voter Information Likely Intended to Sow Distrust of U.S. Elections [Public Service Announcement]. https://www.cisa.gov/sites/default/files/2024-09/PSA_Just_So_You_Know_False_Claims_of_Hacking_Voter_Reg_CISA_and_FBI-508_0.pdf

174 Coldewey, D. (2024, May 30). Misinformation works, and a handful of social 'supersharers' sent 80% of it in 2020. TechCrunch. https://techcrunch.com/2024/05/30/misinformation-works-and-a-handful-of-social-supersharers-sent-80-of-it-in-2020/

175 Ivan, C., Chiru, I., Buluc, R., Radu, A. Anghel, A., Stoian-Iordache, V. Arcos, R., Arribas, C. M., Ćuća, A., Ganatra, K., Gertrudix, M., Modh,K., & Nastasiu, C. (2023). HANDBOOK on Identifying and Countering Disinformation. DOMINOES Project. https://doi.org/10.5281/zenodo.7893952

176 Maertens, R., Roozenbeek, J., Basol, M., & van der Linden, S. (2021). Long-term effectiveness of inoculation against misinformation: Three longitudinal experiments. Journal of Experimental Psychology: Applied, 27(1), 1–16. https://doi.org/10.1037/xap0000315

177 https://pubmed.ncbi.nlm.nih.gov/33017160/

178 Ibid

179 Lewsey, F. (n.d.). Cambridge game 'pre-bunks' coronavirus conspiracies. University of Cambridge. https://www.cam.ac.uk/stories/goviral

180 Graber, J. (2023, May 30). Algorithmic choice. Bluesky. https://bsky.social/about/blog/3-30-2023-algorithmic-choice

181 Office of Governor Gavin Newsom, (2024, September 17). Governor Newsom signs bill to combat deepfake election content [Press Release]. https://www.gov.ca.gov/2024/09/17/governor-newsom-signs-bills-to-combat-deepfake-election-content

182 Texas Economic Development & Tourism. (n.d.). Texas Enterprise Fund. https://gov.texas.gov/business/page/texas-enterprise-fund

183 National Science Foundation. (n.d.). America's Seed Fund. https://seedfund.nsf.gov/

184 U.S. White House. (2023, July). Voluntary AI Commitments. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/

185 Mislove, A. (2023, August 29). Red-Teaming Large Language Models to Identify Novel AI Risks. United States Office of Science and Technology Policy https://bidenwhitehouse.archives.gov/ostp/news-updates/2023/08/29/red-teaming-large-language-models-to-identify-novel-ai-risks/