

Defending American Democracy in the Digital Age: Recommendations Report



ASU **Walter Cronkite**
School of Journalism
and Mass Communication
Arizona State University

MCCAIN
INSTITUTE

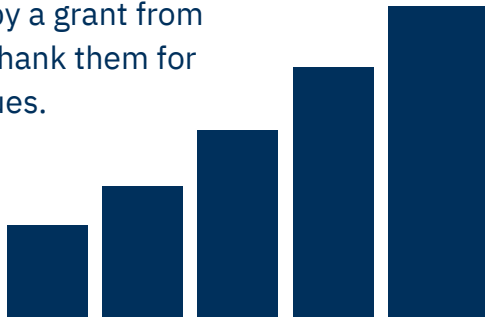
Arizona State University.



Table Of Contents

About the Task Force Conveners.....	Page 3
Executive Summary.....	Page 5
Top Line Recommendations.....	Page 9
Definitions.....	Page 10
Threat Posed by MDM.....	Page 12
Foreign Threats.....	Page 13
MDM and Voter Suppression.....	Page 17
Decline of Local News.....	Page 20
Social Media and MDM.....	Page 24
Threat of Generative AI.....	Page 26
Recommendations.....	Page 28
Acknowledgments.....	Page 50

The task force and recommendations report are made possible by a grant from The John S. and James L. Knight Foundation and Microsoft. We thank them for their generosity, support, and leadership on these important issues.





About the Task

Force Conveners

The McCain Institute

The McCain Institute at Arizona State University (ASU) is a nonpartisan organization inspired by Senator John McCain and his family's dedication to public service. It is part of Arizona State University and based in Washington, D.C. The McCain Institute's programs defend democracy, advance human rights and freedom, and empower character-driven leaders. Its unique power to convene leaders across the global political spectrum enables the McCain Institute to make a real impact on the world's most pressing challenges. Its goal is action, not talk, and like Senator McCain, the McCain Institute is fighting to create a free, safe, and just world for all.

Senator John McCain built a legacy on advancing human freedom and security in the face of adversity. Steadfast in his principles and beliefs, Senator McCain approached every problem by seeking common ground with his political opponents on the other side. "Our political differences, no matter how sharply they are debated, are really quite narrow in comparison to the remarkably durable national consensus on our founding convictions," Senator McCain famously stated. The McCain Institute honors Senator McCain's example, working in the arena with local and global groups in a nonpartisan fashion to convene, educate, and act to benefit all Americans and the world we share.



About the Task

Force Conveners

Walter Cronkite School of Journalism and Mass Communication

The Walter Cronkite School of Journalism and Mass Communication is widely recognized as one of the nation's premier professional journalism and mass communications programs. Rooted in the time-honored values that characterize its namesake – accuracy, responsibility, objectivity, and integrity – the school fosters excellence and ethics among students as they master the professional skills they need to succeed in the digital media world of today and tomorrow.

Located on Arizona State University's Downtown Phoenix campus in a state-of-the-art media complex – with additional locations in Los Angeles and Washington, D.C. – the Cronkite School leads the way in media education with its innovative teaching hospital model, for which it has received international acclaim.

Arizona PBS, one of the nation's largest public television stations, operates out of the Cronkite School building on the ASU Downtown Campus. Arizona PBS serves as a hub for the Cronkite School's immersive learning experiences and a testing ground for new approaches in journalism. All students gain hands-on experience in tools and techniques across news, strategic communications, emerging media, and more while cultivating a spirit of collaboration and innovation.



Executive Summary

Propaganda is not a new phenomenon. Urban legends, rumors, propaganda, and gossip have spread far and wide, across geographic regions, religions, and cultures, for generations. Our ability to share and relate to stories is part of what makes us human. It's how we warn each other of threats. It's how we survive. But the digital age has allowed for the rapid scale and spread of purposefully misleading information that seeks to cause harm. Increasingly, we have seen malign actors, foreign and domestic, use complex disinformation campaigns as a tool to disrupt our democratic process, sow discord throughout the United States, and undermine trust and confidence in the media and our institutions.

The First Amendment to our constitution emphasizes our right to share ideas, opinions, stories, and experiences stating, "Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." This amendment alone serves as a pillar through which democracy, and humanity as a whole, can live our values and thrive. Yet, it's the very freedom that's most exploited.

We had previously hoped that technology could and would be used to strengthen democracy by broadening the information-sharing ecosystem, allowing us to relate across global divides. Theoretically, it was supposed to advance freedom of thought, bolster the transparency of the laws and rules to which we abide, and allow us to make informed consent about our own liberties. It's clear that the opposite has occurred. Not only is the world more divided than it ever has been, but few are able to gauge fact from fiction or truth from reality.

This is especially unsettling in the shadows of a world in conflict, as 64 countries hold democratic elections in 2024, further risking the survival of our own self-governance.



Per Senator McCain,

“It is more important than ever to strengthen our defenses against foreign interference in our elections. Unfortunately, U.S. laws requiring transparency in political campaigns have not kept pace with rapid advances in technology, allowing our adversaries to take advantage of these loopholes to deceive millions of American voters with impunity.”

In other words, the very technology we created to bridge global communication gaps is being used as a tool for control, undermining the democracies we’ve vowed to safeguard.

In an effort to determine how best to protect our global, democratic institutions, maintain our First Amendment rights, and secure access to free and open information sources, Arizona State University’s McCain Institute and Walter Cronkite School of Journalism and Mass Communication have created the Task Force on Defeating Disinformation Attacks on U.S. Democracy.





The Task Force includes disinformation experts, journalists, academic researchers, technologists, and civil society members – names and bios of our Task Force members can be found at the end of this report. Over the last year, our Task Force has met with other experts, policy makers, industry leaders from technology and social media companies including Meta, Wikimedia, Microsoft, and OpenAI to better understand the threats posed by Mis-, Dis-, and Malinformation (MDM) and how best to protect our democracy from those threats.

“The U.S. is at a critical juncture as it faces internal and external assaults on its democracy. It’s going to take all Americans – on the right, left, and center – to defend our freedom.”

– Dr. Evelyn Farkas,
Executive Director of the McCain Institute

“A healthy democracy... relies on the free flow of reliable, accurate information. The Cronkite School has worked for years to provide resources to improve digital media literacy and help the public recognize the dangers of misinformation.”

– Dr. Battinto L. Batts Jr.,
Dean of the Walter Cronkite School of Journalism and Mass Communication

Building on the legacies of Senator McCain and Walter Cronkite – often touted as “the most trusted man in America” – our Task Force has developed actionable recommendations for policymakers and the tech industry, our team aims to encourage unified action against MDM threats.



To do this, we first must recognize that there is not one simple solution. Federal and state legislation, ethical journalism, fact-checking, media literacy campaigns, content moderation, and even algorithmic transparency are not enough. There must be collective action. We must work together to bridge the divide.

The recommendations included in this report are applicable across sectors and geared toward federal and state governments as well as the private sector. They are not exhaustive, but they are intended to address several key issues that we've determined require immediate attention and resources in order to spur action.

MDM impacts all of society; thus, the Task Force's recommendations are nonpartisan and are focused on strengthening our republic, protecting our democratic values, and developing a well-informed citizenry that is able to engage in safe and civil discourse without the influence of malign actors in the face of global information threats.





Top Line Recommendations for Federal, State, and Local Policymakers:

Invest in Media Literacy: Develop media literacy programs to equip individuals with skills to identify misinformation and foster informed engagement.

Prebunking and Accuracy Nudges: Use prebunking strategies and accuracy prompts to proactively counteract misinformation and encourage critical evaluation of content.

Tax Incentives: Provide tax credits to sustain local journalism, essential for informed communities and democracy.

Increased Transparency: Ensure online political ads have the same transparency and disclosure as traditional media, including public databases and clear disclaimers.

Nationwide Election Information: Establish a centralized 311 hotline for accurate, local voting information to combat misinformation.

Algorithmic Transparency: Mandate social media algorithm transparency to understand content prioritization and reduce disinformation.

User Validation: Implement optional, free ID verification to distinguish genuine accounts from fake ones, enhancing trust.

Coordinate the U.S. Government Response for a New Era of “Cold War”: Organizations across the national security community of the United States need to be reviewed for their efficacy in meeting the disinformation challenge to the West.

Misinformation, Disinformation, and Malinformation Explained

Misinformation: False information that is created or shared without the inherent intent of causing harm. ¹

Disinformation: False or misleading information that is created with the intent to cause harm, influence a portion of the public or specific groups, mislead, or manipulate.²

Malinformation: Information that is based on facts but used out of context in an attempt to manipulate, mislead, and cause harm. Malinformation is different from disinformation because malinformation relies on partially true or factual information. Disinformation, on the other hand, is intentionally false.³

1. "Foreign Influence Operations and Disinformation." Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation>

2. Ibid.

3. Ibid.





Under the DISARM framework (Disinformation, Subversion, Attribution, Resilience, and Manipulation), various tactics of **Information Manipulation and Interference** include, but are not limited to:

- **Fabricated Content:** Completely false information fabricated to mislead or deceive.
- **Manipulated Content:** Genuine information or imagery distorted or misrepresented to sensationalize or mislead.
- **Imposter Content:** False representation of genuine sources or entities to deceive audiences.
- **Misleading Content:** Information presented as factual when it is not, aimed at misleading the public or specific groups.
- **False Context:** Accurate information presented with misleading contextual details to alter its meaning or impact.
- **Satire and Parody:** Humorous but false stories presented as genuine, potentially confusing audiences.
- **False Connections:** Incorrect associations made between content and supporting elements to mislead or confuse.
- **Sponsored Content:** Paid advertising or PR presented as impartial or editorial content, misleading audiences about its origin or purpose.
- **Propaganda:** Deliberate dissemination of biased or misleading information to influence attitudes or manipulate public opinion.
- **Error:** Mistakes in reporting or dissemination by reputable sources, which can inadvertently contribute to misinformation.

The Threat Posed by MDM

We are at a critical juncture in the history of American democracy. Malevolent actors, foreign and domestic, are working to degrade our democracy, undermine our elections, and sow discord. Trust in our media and institutions is at a historic low.⁴ Exacerbated by the proliferation of false information that undermines public confidence and civic engagement, it's more common than ever for constituents to question the information they see. This has led to a number of bipartisan grievances, including the questioning of election outcomes, denial of inquiries in the midst of global health crises, and even violent action.

A recent Gallup poll underscores this profound unease amongst Americans, revealing that only 28% of U.S. adults are satisfied with the way our democracy functions. This is a significant decrease from the prior low of 35% which was measured after the January 6th attack on the U.S. Capitol.⁵ Even more concerning, a 2022 NPR/Ipsos poll found that 64% of Americans believe American democracy is in crisis and at risk of failing.⁶



The Foreign Threat

The 2016 U.S. presidential election marked a watershed moment in the use of MDM as a tool of foreign interference, notably by the Russian government. A comprehensive 2017 report by the Office of the Director of National Intelligence, drawing on assessments from the Central Intelligence Agency, Federal Bureau of Investigation, and the National Security Agency, concluded that:

“Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election. Russia’s goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.”⁷

Further intelligence briefings to the House Intelligence Committee in February 2020 confirmed ongoing Russian efforts to influence subsequent elections around the world, including our own in the coming months. By employing a range of hybrid tactics as outlined in Russia’s notorious “Active Measures” political warfare strategy dating back to the 1920s, Russian operatives continue to use data-enabled cyber, psychological, and digital marketing tactics to bolster MDM across social media platforms and news media sites.


4. Megan Brenan, “Media Confidence in U.S. Matches 2016 Record Low,” Gallup.com, February 7, 2024, <https://news.gallup.com/poll/512861/media-confidence-matches-2016-record-low.aspx>

Saad, Lydia. “Historically Low Faith in U.S. Institutions Continues” Gallup.com, March 16, 2024.

5. <https://news.gallup.com/poll/548120/record-low-satisfied-democracy-working.aspx>

6. <https://www.ipsos.com/en-us/seven-ten-americans-say-country-crisis-risk-failing>

7. <https://www.nytimes.com/interactive/2017/01/06/us/politics/document-russia-hacking-report-intelligence-agencies.html>



Knowledge of the digital infrastructure as a whole, paired with age-old PR schemes, paid advertising, promoted posts, and personal marketing data, enables them to run influential, multi-faceted campaigns, formulated to impose new assumptions in the minds of their targeted audiences (see “Reflexive control”). The 2016 operation alone reached over 126 million Facebook and Twitter users, with even more spanning Instagram, YouTube, Telegram, WhatsApp, Reddit, and decentralized channels like 4chan, 8chan, and dark web forums. As data-enabled AI tools like OpenAI, Google’s Gemini, and Microsoft’s Copilot continue to evolve, they will reach far more.

Russia’s MDM attack on America was and is not sophisticated. In fact, they only spent about \$300k on the overall 2015–2016 election cycle, as opposed to the combined \$1.5 billion spent by the presidential candidates. The spending has not increased substantially since. While evolving technical capabilities in global communication systems help spread malign narratives faster, their success has little to do with newly developed tactics or even special tools. Everything they use is open source and commercially available to anyone who knows how to run a digital marketing campaign, examine competitive business data and/or interpret user behavior analytics.

Thus, they were, and still are, able to reach millions of Americans, just as a social media influencer is able to reach you with a product. By interacting with the platforms in ways that promote engagement based on user preferences and behavior patterns, carefully constructed narratives can be brought to the top of any target audience’s news feeds and disseminated amongst their network of peers. If that message does well, it will grow, making its way across other platforms and media conglomerates, adding to its false validity. This includes all forms of media.


In one particular 2016 example, a Facebook page titled “Heart of Texas” grew in popularity amongst Texas secession enthusiasts, encouraging withdrawal from the union. With over 250,000 followers, it reached more people than the official Texas Democrat and Republican Facebook pages combined.⁸

The information on the page prompted a “Stop Islamification of Texas” protest at the Islamic Center in Houston on May 21, 2016, and a “Save Islamic Knowledge” rally at the same place and time, which escalated into a larger confrontation. The Texas Tribune notes, “Russians managed to pit Texans against each other for the bargain price of \$200,” which is all that was spent on this particular audience.

By exploiting hot button issues like “abortion, LGBTQ rights, gun rights, immigration, nationalism, race, religion, terrorism, and other socio-economic touchpoints like class, education, and by exploiting cultural and spiritual ideologies,”⁹ the Kremlin-linked Internet Research Agency (IRA) – whose name has since changed – continues to successfully, and inexpensively, divide Americans across political fault lines, resulting in polarization, conflict, and voter suppression.



8. <https://www.washingtonpost.com/news/democracy-post/wp/2017/10/17/how-the-russians-pretended-to-be-texans-and-texans-believed-them/>
9. https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/09/Uncover.Kim_v.5.0905181.pdf



While Russia is infamous for its long-standing narrative attack strategy, it is not alone in its pursuit of information dominance. China, Iran, Brazil, North Korea, and many others, in addition to numerous global citizen groups at home, and overseas, have also been attributed to global information campaigns to further sway elections, sow discord, and undermine Western democracy through the simple use of commercial marketing tools, and a little bit of cognitive psychology.

The implications of foreign information manipulation and interference (FIMI) extend far beyond political campaigns, posing a broader threat to global security and the state of democracy as a whole. This has prompted NATO to establish a new “deterrence baseline,” aimed at combating information campaigns of global operational risk through increased candid communication and transparency, similar to McCain’s “Straight Talk Express.”

Like NATO, we believe that addressing this multifaceted challenge requires robust defense strategies, international cooperation, transparency, and a nuanced approach that includes deterrence measures to increase the costs for adversaries engaging in such activities.





MDM and Voter Suppression

Voter suppression refers to various strategies and tactics used to prevent or discourage certain groups of people from voting, thereby influencing the outcome of an election. These tactics can be overt or covert and can be implemented through legal means, administrative measures, or through misinformation and intimidation.

Digital platforms play a crucial role in modern voter suppression tactics. Echoing the dissemination of a political campaign, constituent groups of interest can be easily microtargeted with tailored MDM using data analytics. Far-reaching campaigns can spread through advertisements, posts, and messages designed to play on the fears and biases of specific demographic groups.

Astroturfing, the creation of fake grassroots movements or organizations that appear to be driven by community members but are actually orchestrated to spread specific narratives and misinformation, further exacerbates the issue. This is in addition to robocalls and mass texts, which serve as a popular tool for anyone's political campaign.

During the 2016 U.S. Presidential Election, Russia's IRA used social media platforms to suppress voter turnout among African Americans and other minority groups. In the 2018 Georgia Gubernatorial Election, claims of voter suppression included the purging of voter rolls, long lines at polling stations, and strict voter ID laws that disproportionately affected minority communities.

The 2020 election, coinciding with the COVID-19 pandemic, created a perfect storm for MDM campaigns aimed at voter suppression. Election officials and state governments struggled to manage voting amidst the pandemic, often changing voting rules or postponing elections at the last minute, perpetuating misinformation narratives about the integrity and security of voting by mail.



Research has shown that voting by mail does not advantage one party over another. However, in states where party leaders discouraged mail-in voting, voter turnout declined.

Republican pollster Paul Bentz noted that Trump “effectively suppressed a portion of his own base of support.”

Trump’s stance on voting methods has shifted since then. In April 2024, he wrote on Truth Social,

“ABSENTEE VOTING, EARLY VOTING, AND ELECTION DAY VOTING ARE ALL GOOD OPTIONS. REPUBLICANS MUST MAKE A PLAN, REGISTER, AND VOTE!”

This represents a significant change from his previous posts, such as after the 2022 midterm elections when he wrote,

“YOU CAN NEVER HAVE FAIR & FREE ELECTIONS WITH MAIL-IN BALLOTS – NEVER, NEVER, NEVER.”





On the other side of the aisle, Democrat Congresswoman Katie Porter (CA-D) claimed that California elections were “rigged”:

“Big money does influence our elections... Outcomes are manipulated and distorted when you have people coming in spending millions and millions of dollars at the last minute and that money is not disclosed until after the election.”

Additionally, Georgia governor candidate Stacey Abrams claimed that the election was “stolen”, suggesting that election laws were “rigged”, and that it was “not a free or fair election.”

These claims from Democrats and Republicans alike are equally damaging to our democracy and citizen’s trust in institutions.

Beyond voter suppression tactics, both foreign and domestic actors have spread MDM to make Americans question the integrity of elections by pushing cross-party narratives about how the elections have been rigged. The “big lie” (also part of the Active Measures playbook as outlined by Thomas Rid in his New York Times bestseller, “Active Measures”) that the 2020 election was stolen from Trump has been particularly effective among specifically targeted Republican voter groups, significantly undermining Republicans’ confidence in elections.

A 2022 Gallup poll revealed that only 40% of Republicans were confident in the integrity of elections, compared to 85% of Democrats. A 2023 poll by the Associated Press-NORC Center for Public Affairs Research found that while 7 in 10 Americans believe Biden was elected legitimately, 57% of Republicans view Biden as an illegitimate president. This confidence gap is the largest recorded by Gallup since 2004.

The Decline of Local News

One of the most effective defenses against MDM is nonpartisan journalism. However, since 2004 we've lost 57% of local journalists.¹⁰ On average, 2.5 newspapers close per week and more than half of all U.S. counties have limited access to local news. Over the next five years it is estimated that an additional 228 counties are at risk of becoming news deserts.¹¹ This decline in local journalism has had a profound impact on voters' knowledge of their representatives and local civic affairs. For example, according to research by Danny Hayes and Jennifer L. Lawless, coverage of local politics dropped by 56% between 1999 and 2017.¹² According to the nonprofit Rebuild Local News, the percentage of voters who could name their mayor fell from 70% in 1966 to just 40% in 2016.¹³

In addition to the decline of local news, a PEN America study found that “only 14 percent of journalists reported that their newsrooms had a dedicated in-house fact-checking team to monitor and debunk dis/mis/mal-information.”¹⁴ Newsrooms with limited resources may not be fully equipped to address MDM's increasing impact on major news stories.

While Americans have traditionally had high confidence in their local news, Americans' confidence in mass media – newspapers, TV, and radio – is at a record low. A Gallup poll from 2023 found that 32% of Americans have a great deal/fair amount of confidence in mass media, while a record high 39% of Americans say they have no confidence in mass media at all.¹⁵ This declining trust –combined with the decrease in local coverage – has led people to seek news from outside the traditional mainstream media – including from content creators on social media. The reliability and credibility of this information varies widely since it is not held to the same ethical standards as professional journalism.

10. <https://www.poynter.org/commentary/2024/how-ai-could-sap-or-save-local-news/>


11. <https://www.medill.northwestern.edu/news/2023/more-than-half-of-us-counties-have-no-access-or-very-limited-access-to-local-news.html>

12. Hayes, Danny, and Jennifer L. Lawless. “The Great Gutting of US Newspapers.” Chapter. In *News Hole: The Demise of Local Journalism and Political Engagement*, 15–40. Communication, Society and Politics. Cambridge: Cambridge University Press, 2021.

13. <https://www.rebuildlocalnews.org/how-the-fcc-could-help-save-local-news/>

14. <https://pen.org/report/hard-news-journalists-and-the-threat-of-disinformation/>

15. <https://news.gallup.com/poll/512861/media-confidence-matches-2016-record-low.aspx>



According to NewsGuard, engagement with “generally unreliable” sites grew from 8% in 2019 to 17% in 2020.¹⁶ NewsGuard works with journalists and editors to produce a reliability rating based on nine journalistic criteria. Unreliable sites can fall into one of two categories: proceed with caution, meaning the website is unreliable “because it fails to adhere to several basic journalistic standards” or proceed with maximum caution which applies to websites that severely violate basic journalistic standards.¹⁷

The decline in confidence in traditional media, coupled with digital advertising and promoted posts on social media, has significantly increased the reach of unreliable sites. Another byproduct of shrinking local journalism is pink slime outlets, a name borrowed from low-quality meat. These pink slime sites “are familiar yet misleading – masquerading as the digital equivalent of traditional, well-trusted, locally-based newspapers, but actually promoting political, ideological, and commercial interests in strategically significant locations.”¹⁸ Pink slime sites are made to look like local news sites, yet they are closer to a propaganda outlet than a news organization aimed at advancing a particular agenda and engaging in pay-to-play news stories.

Podcasts are a growing source of news for Americans. While only 29% of podcast listeners say keeping up with current events is a major reason they listen to podcasts, listeners have a very high level of trust in the news they do hear. Nearly 90% of those who hear news on a podcast expect the news to be mostly accurate.¹⁹ This stands in stark contrast to Americans’ trust in traditional media as well as social media. An earlier poll found that only 39% of social media users believed news they read on social media was largely accurate.²⁰

16. <https://www.newsguardtech.com/special-reports/special-report-2020-engagement-analysis/>

17. <https://www.newsguardtech.com/ratings/rating-process-criteria/>

18. https://www.cjr.org/tow_center/pink-slime-journalism-and-a-history-of-media-manipulation-in-america.php

19. <https://www.pewresearch.org/journalism/2023/04/18/podcasts-as-a-source-of-news-and-information/>

20. <https://www.pewresearch.org/journalism/2021/01/12/news-use-across-social-media-platforms-in-2020/>

What's even more interesting, "just one-in-five listeners say the podcasts they listen to are connected to a news organization, while almost three times that amount (59%) say they are not."²¹ The confidence podcast listeners have in the news they are hearing from non-news organizations may make them vulnerable to MDM if the podcasts they listen to knowingly or unknowingly spread false or misleading information. The long-form conversational nature of podcasts makes it easy for false or misleading information to get lost in the conversation.

Analysis by the Brookings Institute of more than 8,000 episodes of political podcasts found that more than one-tenth of the episodes shared potentially false information. Due to the popular nature of podcasts, the flagged episodes "collectively received more than 100 million views, likes, or comments."²²

To illustrate the potential impact MDM can have on podcast listeners, Joe Rogan's "The Joe Rogan Experience" boasts an estimated 11 million listeners per episode, which is nearly four times as many people that tune into prime-time cable news shows.²³ Podcasters and their guests have a massive reach. This presents both an opportunity for MDM to spread, as well as an opportunity to educate listeners with factual information.



21. <https://www.pewresearch.org/journalism/2023/04/18/podcasts-as-a-source-of-news-and-information/>

22. <https://www.brookings.edu/articles/the-challenge-of-detecting-misinformation-in-podcasting/#ftn1>

23. <https://www.washingtonpost.com/politics/2021/05/03/joe-rogan-told-his-millions-listeners-not-take-his-anti-vaccine-advice-seriously-is-it-too-late/>

News reporters and journalists obtain their information through various means. They rely on sources, including government officials, experts, eyewitnesses, and documents. The process involves fact-checking, verifying information from multiple sources, and adhering to journalistic ethics and standards. However, the decline in resources and dedicated fact-checking teams has made this process more challenging.

As explained in "Trust Me, I'm Lying" by Ryan Holiday, media manipulation tactics can exploit these challenges. Holiday describes how marketers and propagandists can plant false stories in low-tier blogs, which are then picked up by larger outlets, eventually gaining widespread credibility. This manipulation highlights the vulnerabilities in the media ecosystem, where the pressure to publish quickly can lead to the spread of misinformation.

Understanding the decline of local news and the mechanics of how journalists obtain and verify information is crucial in addressing the challenges posed by MDM. Strengthening local journalism, improving fact-checking resources, and educating the public about media and data literacy are essential steps in combating the spread of misinformation and ensuring a well-informed electorate.





How Social Media Helps Spread MDM

Social media has inarguably changed the world. It has brought people closer together and driven us apart. Grassroots activists have used social media to drive revolutionary change while despots have used it to crush dissent. It has also been the largest catalyst for the rapid spread of MDM online and into mainstream news networks and local media

According to researchers at the Massachusetts Institute of Technology (MIT), “falsehoods were 70% more likely to be retweeted than the truth.”²⁴ One explanation for this is that people are attracted to new and interesting information, and we like to be, or appear to be, “in the know.” Researchers from MIT found that “false news is more novel, and that novel information is more likely to be retweeted.”²⁵ This inclination towards novelty plays into the hands of those who spread MDM, as false information often appears more engaging and interesting than the truth, especially when designed to reach the people whose data suggests they’ll bite.

Social media algorithms are designed to identify and promote content that is likely to keep people on their platforms and maximize engagement. If false information generates more engagement and shares, platforms will push that content to more people, further spreading the MDM. By prioritizing engagement metrics above accuracy, these algorithms facilitate the dissemination of MDM.

The reward-based structure encourages users to share content that garners high levels of engagement, often leading to a cycle where users repeatedly share MDM to maintain or increase their engagement levels.

Unlike traditional media, which undergoes – at least some – editorial oversight and fact-checking, social media platforms lack rigorous content verification processes and are protected from being held accountable for the content posted on their platforms by Section 230 of the Communications Decency Act (CDA).²⁶ Section 230(c)(1) states, “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” This essentially means that companies such as Meta or YouTube cannot be held liable for the content their users post. There has been significant debate among academics and politicians regarding the need to reform, protect, or repeal Section 230.²⁷



Most of the algorithms used by social media focus on engagement likes, watches, clicks, reposts, etc. to determine what content to recommend to users. The posts with more engagement get pushed to the front of users' feeds which allows for more engagement. The challenge with this system is that it will often promote MDM and other divisive content that attracts engagement both from users who believe the information and those who are pushing back against it. This helps drive more views and engagement to the MDM content, thereby helping grow its reach.

Some researchers are exploring alternatives to the engagement model that will base recommendations not on engagement but on how users' determine the content's value. The theory is, by focusing on the value of the content and how it made users feel vs. solely adjusting algorithms based on likes, comments, shares, etc. companies can create a more useful algorithm that drives high-value content.²⁸ If researchers are able to collaborate with social media companies to study values-based recommender systems, and companies adjust how their algorithms work, we may be able to cut down on the promotion of highly-divisive and MDM-laden content.

The speed and ease with which unregulated information can be shared on these platforms mean that falsehoods can go viral before they can be debunked. Furthermore, the anonymity and reach provided by social media enable anyone in the world to disseminate false information widely without immediate accountability. Still, there is no solution as to "who" gets to decide what that accountability might look like.

These tactics are not limited to marketers but are also employed by those spreading MDM to exploit the weaknesses in the digital news ecosystem. The emphasis on engagement over accuracy, combined with the echo chamber effect, allows false information to proliferate rapidly. The decline in traditional journalism and the complex dynamics of the digital information ecosystem underscore the challenges we face as the technologies continue to evolve.

24. Soroush Vosoughi et al. ,The spread of true and false news online. *Science*359,1146-1151(2018).

25. Soroush Vosoughi et al. ,The spread of true and false news online. *Science*359,1146-1151(2018).

26. <https://www.congress.gov/bill/104th-congress/senate-bill/652/text>

27. Ibid.

28. <https://www.wired.com/story/platforms-engagement-research-meta/>




The Threat of Generative AI

Within two months of its launch, ChatGPT, the generative artificial chatbot, hit 100 million monthly users, a milestone that took popular streaming platform Netflix three and a half years to reach.²⁹ The rapid advancement in generative AI over the last few years has been astounding. Clunky chatbots quickly evolved to be able to write entire articles, create realistic images, and even produce high-quality videos from simple text prompts.

As AI continues to improve, it will become more difficult to differentiate between human-generated and AI-generated content. In fact, one study showed readers preferred AI-generated content over content written by humans.³⁰ It will also become more difficult to identify fake or manipulated content.

Last year, an AI-generated image of an explosion at the Pentagon went viral on social media and was even reported by some foreign news agencies before eventually being confirmed as a hoax.³¹ While this was an example of a more sophisticated cheapfake, there is growing concern about the potential influx of deepfake techniques that can manufacture convincing images, videos, and audio recordings of things that did not happen or were not said.

A Senate Select Committee on Intelligence report on the active measures used by Russia to influence the 2016 election stated that deepfake techniques, while still new, “are being perfected at a pace that eclipses the effort to create the technology for detecting and mitigating fraudulent media content.”³²



Just this year, during the 2024 New Hampshire presidential primary, a robocall using AI voice cloning to impersonate President Biden told Democrats not to vote in the Democratic primary.³³ That example is just the tip of the iceberg of what could come. Imagine campaigns or foreign adversaries running deepfakes of candidates endorsing policies antithetical to their platform or saying something so offensive or uncharacteristic it could sway votes.

The integration of AI into the information ecosystem is deeply connected to the data that trains these models. AI systems, including generative AI, are trained on vast datasets, much of which is derived from user-generated content on social media and other digital platforms. The same data is used to target interest groups and encompass the same patterns and behaviors that feed social media algorithms, determining the information users are exposed to. Consequently, the biases, inaccuracies, and manipulative content that permeate social media also influence AI training data, reinforcing and potentially amplifying existing issues.

Machine learning models, the backbone of AI, rely heavily on the quality and diversity of their training data. If the data contains false or misleading information, the AI is likely to replicate and spread these inaccuracies. This feedback loop between social media and AI can significantly enhance the reach and impact of MDM, making it harder to discern truth from deception.

If AI-generated deceptive content becomes too difficult to detect, it can pose a significant threat to public trust. This erosion of trust could not only undermine confidence in democratic institutions but also leaves individuals vulnerable to manipulation, potentially resulting in disruptions to the electoral processes and other critical aspects of society.

29. <https://www.journalofdemocracy.org/articles/how-ai-threatens-democracy/>

30. <https://www.forbes.com/sites/rogerdooley/2023/12/04/humans-prefer-ai-generated-content/?sh=4fdd9f295cf6>

31. <https://www.npr.org/2023/05/22/1177590231/fake-viral-images-of-an-explosion-at-the-pentagon-were-probably-created-by-ai>

32. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

33. <https://www.nytimes.com/2024/02/27/us/politics/ai-robocall-biden-new-hampshire.html>



Recommendations

Invest in Media Literacy and Critical Thinking Training

Americans are inundated with content from a variety of sources. In fact, Americans see between 50 and 400 branded advertisements per day. Cable news, online news sites, social media, podcasts, YouTube, blogs, and independent journalists provide an endless stream of information that shapes narratives and opinions.

Effective media literacy and critical thinking skills are essential to navigate this landscape and mitigate the impact of deceptive content on democratic processes. A significant majority of Americans (72% surveyed) believe media literacy skills can be helpful in identifying misinformation, disinformation, and malinformation (MDM). In a 2022 survey by Media Literacy Now, analysts found that 84% of Americans support requiring schools to provide media literacy education, and 90% support requiring lessons in critical thinking.

There is a growing body of research indicating that media literacy and critical thinking training effectively stem the spread of MDM. One study found that 73.3% of respondents who received media literacy training could identify fake news stories and information, compared to only 46.4% of those without such training.³⁵

Some states have already started investing in media literacy education in schools. At least 19 states have enacted legislation mandating media literacy requirements for K–12 students, although the level of instruction varies. An additional nine states have pending media literacy legislation.³⁶

Robust media literacy programs are critical not only for identifying misinformation but also for fostering informed civic engagement. By equipping individuals from different age groups, backgrounds, and demographics with the ability to critically assess information, communities can better safeguard against threats to electoral integrity posed by false narratives and deceptive tactics. Successful initiatives underscore the importance of tailored educational strategies. States like Massachusetts and Washington have implemented comprehensive media literacy frameworks that integrate critical thinking into K–12 curricula, aiming to empower students from diverse backgrounds with the skills needed to discern reliable sources and verify information.



Programs should go beyond traditional media sources and focus on the mediums many Americans are getting their news from today, including YouTube videos and podcasts. Special attention should also be paid to generative AI. The more people are familiar with new and emerging technologies, the better equipped they will be to identify when these technologies are being used deceptively.

34. Daniel Milo and Katarína Klingová. "Countering Information War: Lessons Learned from NATO and Partner Countries." GLOBSEC Policy Institute. 2016
https://www.globsec.org/sites/default/files/2017-09/countering_information_war.pdf

35. Dame Adjin-Tettey, Theodora. "Combating Fake News, Disinformation, and Misinformation: Experimental Evidence for Media Literacy Education." *Cogent Arts & Humanities* 9, no. 1 (2022).

36. https://medialiteracynow.org/wp-content/uploads/2024/02/MediaLiteracyNowPolicyReport2023_publishedFeb2024b.pdf



RECOMMENDATIONS

I. Federal:

A. Congressional Funding: Allocate new funding and educational grants to states aimed at enhancing media literacy programs at the K–12 level. This funding should be flexible to support curriculum development, teacher training, and the integration of digital literacy tools tailored to emerging technologies and evolving platforms.

B. Department of Education Initiative: Partner with nonprofits and academic institutions to develop model curricula and online resources for teens and adults. Implement a train-the-trainer model to scale up teacher and civic leader proficiency in media literacy education, ensuring widespread adoption of best practices across schools and community centers nationwide.

II. State:

A. Legislative Mandates: States without existing media literacy requirements should enact legislation mandating media literacy and critical thinking training in K–12 education. This legislative action should ensure comprehensive coverage across all educational institutions, addressing varying levels of instruction to meet diverse community needs.

B. Financial Support: State legislatures should appropriate additional funds to expand media literacy initiatives beyond schools, facilitating programs in public libraries, community centers, and senior facilities. Prioritize support for vulnerable communities, including veterans, minorities, and non-English speakers, who are disproportionately targeted by MDM.



Social Media Companies Should Expand Prebunking and Accuracy Nudges to Inoculate Users Against MDM

While media literacy training can be used as an effective tool to combat malign information campaigns, not everyone will receive adequate media literacy training, let alone learn about the cyber implications of the personal data that’s used to power them, leaving millions susceptible to MDM. Therefore, it’s crucial that we take an integrated approach to employ tested and effective tactics to curb information threats effectively.

Prebunking is a proactive approach to preemptively combat MDM by forewarning users about potential misinformation and providing them with factual information. For instance, during election cycles, prebunking could involve prominently displaying accurate Election Day information to counter false claims attempting to suppress voter turnout.

Prebunking draws from social psychology’s **inoculation theory**, likening the process to building “mental antibodies” against misinformation. Just as vaccines prepare the body to resist infections, prebunking prepares individuals to resist misleading information, making them less susceptible in the future.

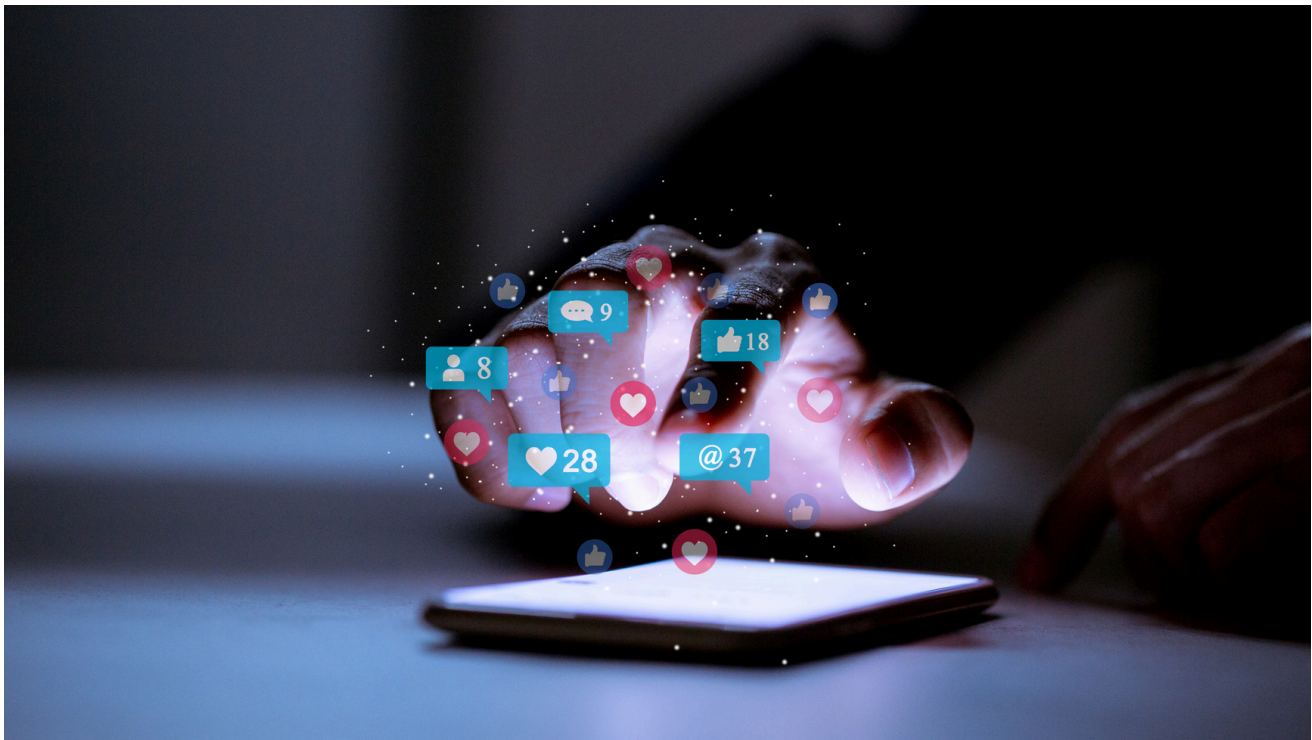
While prebunking is most effective when users receive these messages before encountering MDM, it can still inoculate individuals after exposure, reinforcing their resistance.



Accuracy nudges represent another effective strategy in which reminders about the importance of accuracy enhance the quality of information shared on social media platforms. Despite people’s ability to discern truth from falsehood, social media dynamics often prioritize factors like partisan alignment over accuracy, leading to the inadvertent sharing of misinformation.

Research has shown that “simply reminding people about the concept of accuracy improves the quality of information-sharing on both sides of the political aisle.”³⁷

One of the reasons MDM is able to spread so rapidly on social media is that “while people are often able to tell truth from falsehood... they nonetheless share false and misleading content because the social media context focuses their attention on factors other than accuracy (e.g., partisan alignment). As a result, they get distracted from even considering accuracy when deciding whether to share news — leading them to not implement their preference for accuracy and instead share misleading content.”³⁸



37. <https://news.cornell.edu/stories/2024/04/accuracy-nudges-decrease-misinformation-sharing-left-right>

38. Pennycook, G., McPhetres, J., Zhang, Y., Lu, J. G., & Rand, D. G. (2020). Fighting COVID-19 Misinformation on Social Media: Experimental Evidence for a Scalable Accuracy-Nudge Intervention. *Psychological Science*, 31(7), 770-780.



RECOMMENDATIONS

I. Federal:

- A.** Establish a bipartisan commission or task force dedicated to studying and recommending policies that enhance the transparency and accountability of social media platforms in combating MDM. This commission should include experts in digital media, ethics, and data privacy to develop guidelines that ensure algorithms prioritize accuracy and integrity in content dissemination.
- B.** Congress should pass legislation requiring social media companies to adopt standardized practices for transparency in content moderation algorithms. This includes disclosing how algorithms prioritize content and ensuring that these algorithms prioritize accuracy and reliability over engagement metrics.

II. State:

- A.** Encourage state legislatures to develop and fund initiatives that promote digital literacy and critical thinking skills among residents of all ages. This includes partnerships with educational institutions and community organizations to integrate media literacy into school curricula and adult education programs.
- B.** Establish state-level grants or tax incentives to support local journalism initiatives that focus on investigative reporting and community engagement. Strengthening local journalism is essential for providing accurate, context-rich information that counters MDM and fosters informed civic participation.

III. Private Sector:

- A.** Social media companies should invest in collaborative research efforts with independent researchers and academic institutions to continuously improve prebunking and accuracy nudges. By sharing data and insights, these collaborations can refine strategies that effectively inoculate users against misinformation while respecting user privacy and autonomy.



Tax Incentives to Support Local Journalism

Local journalism is dying. On average, 2.5 newspapers close per week, and more than half of all United States counties have limited access to local news.³⁹ According to the nonprofit organization Rebuild Local News, between “1999 and 2017, coverage of local politics dropped by 56%.”⁴⁰

This lack of local reporting directly affects our democracy. Communities that have less local news have lower voter turnout, less competitive races, more uninformed voters, less civic engagement, more government corruption and waste, and more polarization.⁴¹ Often times, it is the communities of color, immigrant, and non-English speakers who are disproportionately affected by this.

Local news outlets have struggled to compete in the modern media age. Creative solutions are needed to ensure communities across the country have access to nonpartisan and trustworthy local news.

39. <https://www.medill.northwestern.edu/news/2023/more-than-half-of-us-counties-have-no-access-or-very-limited-access-to-local-news.html>

40. <https://www.rebuildlocalnews.org/research-on-local-news/>

41. <https://www.rebuildlocalnews.org/research-on-local-news/>



RECOMMENDATIONS

I. Federal:

- A.** Introduce federal tax incentives for individuals who subscribe to local newspapers or donate to nonprofit news organizations. These incentives could take the form of tax credits or deductions, encouraging direct financial support for local journalism and ensuring its sustainability.
- B.** Establish a federal grant program specifically aimed at supporting local journalism initiatives that serve underserved communities, including communities of color, immigrants, and non-English speaking populations. These grants should prioritize projects that enhance diversity and inclusivity in local news coverage.

II. State:

- A.** Enact state-level tax credits for small businesses that advertise with local newspapers and media outlets. This initiative would stimulate local advertising revenue, providing critical financial support to sustain local journalism efforts across different states.
- B.** Create state-funded subsidies or matching grants to bolster funding for investigative journalism and community reporting in areas where local news coverage is sparse or declining. These subsidies should prioritize projects that promote transparency, accountability, and community engagement.

III. Private Sector:

- A.** Media organizations and tech companies should establish partnership programs with local news outlets to provide technological and editorial support. These collaborations could include funding for digital transformation, audience development strategies, and innovative storytelling techniques aimed at revitalizing local journalism.



Increased Transparency for Online Political Ads

Political advertisements can be ubiquitous, especially ahead of elections. It is estimated that over \$10 billion will be spent on political ads in the 2024 election cycle.⁴² Increasingly, campaigns are spending more on online advertisements that can be found on social media sites, YouTube videos, and streaming platforms. The issue is that the law that requires transparency for political ads on TV, print, and radio currently does not apply to internet and digital ads.

In 2002, when Senators John McCain and Russ Feingold led the effort to pass the Bipartisan Campaign Reform Act, commonly known as the McCain-Feingold Act, into law the internet was not nearly as omnipresent as it is today and, thus, was not considered in the restrictions.

We know foreign adversaries and other malign actors exploit these loopholes and use online advertising to target voters in an attempt to influence our elections. The now re-branded IRA used promoted posts and paid advertisements to influence millions of Americans ahead of the 2016 elections, which reportedly reached over 126 million Facebook users alone.⁴³

In 2024, we ask Congress to close this loophole and ensure online political advertising is transparent and funded by legal means.

42. <https://www.nbcnews.com/politics/2024-election/political-ad-spending-2024-expected-shatter-10-billion-breaking-record-rcna104402>
43. <https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html>



RECOMMENDATIONS

I. Federal:

A. Congress should pass comprehensive legislation that mandates the same disclosure requirements and transparency standards for online political advertisements as those applied to TV, radio, and print ads. This legislation should encompass ads from candidates, issue ads, and ads sponsored by unaffiliated Political Action Committees (PACs). Additionally, stringent measures should be implemented to prohibit foreign governments, entities, and individuals from running online political ads aimed at influencing U.S. elections.

B. Establish a federal regulatory body or empower an existing agency to oversee and enforce compliance with the new transparency laws for online political advertising. This body should maintain a publicly accessible database of all online political ads, including details on ad content, funding sources, targeting criteria, and audience demographics. Enhanced monitoring and reporting mechanisms should be implemented to ensure transparency and accountability in digital political campaigns.

II. State:

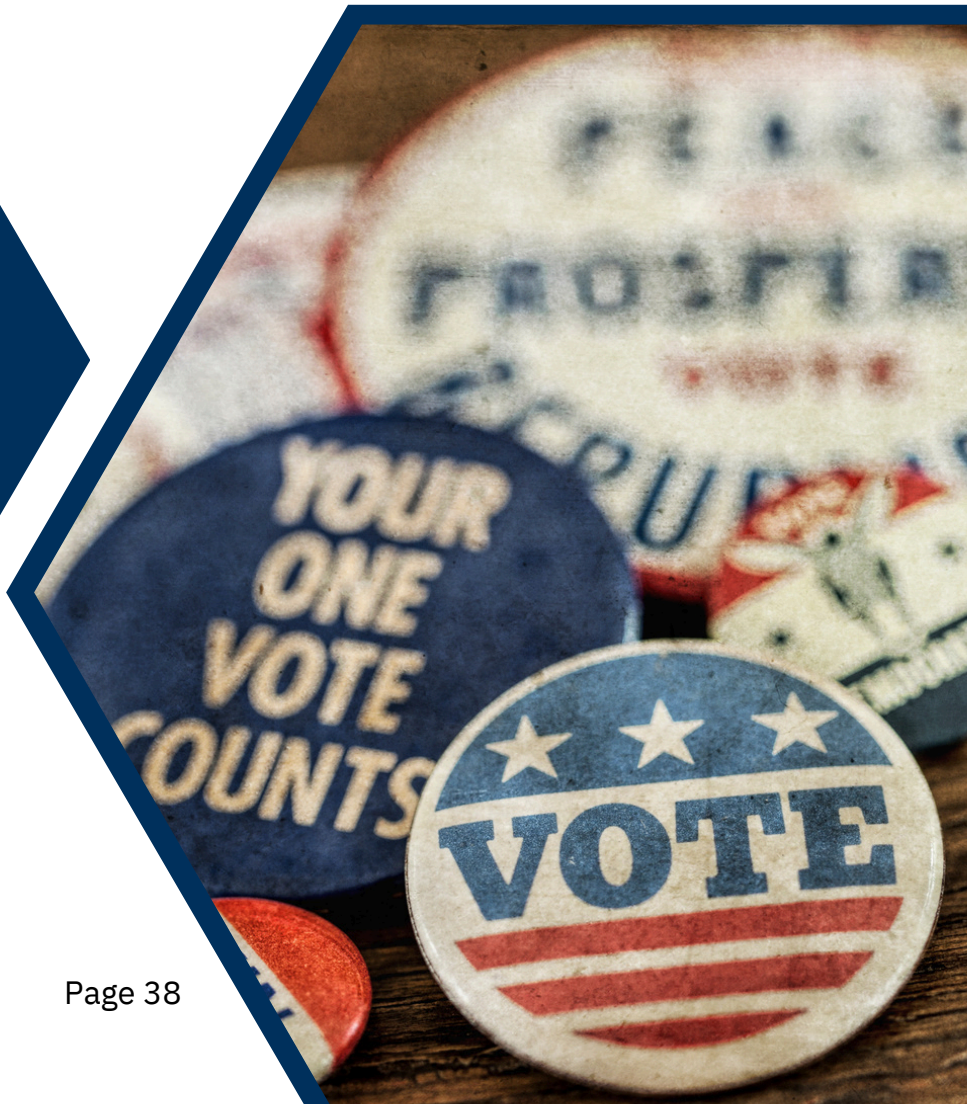
A. State legislatures should enact legislation that mirrors federal requirements for transparency in online political advertising. This includes mandating disclosure of funding sources, sponsorship details, and targeting criteria for all digital political ads that specifically reference candidates or issues relevant to state elections.

B. Establish a state-level regulatory body or commission dedicated to overseeing and enforcing transparency requirements for online political advertising. This body should collaborate with the federal regulatory body and associated federal agencies and online platforms to monitor compliance with disclosure rules, investigate complaints of non-compliance, and ensure that state-specific regulations are effectively implemented to safeguard electoral integrity at the local level.



III. Private Sector:

A. Online ad platforms and vendors should proactively enhance transparency measures for digital political ads. This includes implementing clear and prominent disclosures within the ad units themselves, such as identifying the sponsoring entity and clarifying the funding source. Platforms should also develop and enforce identity validation policies that prevent misuse of their advertising systems for political influence campaigns, employing advanced algorithms and human oversight to detect and block suspicious activities.





Create a Nationwide 311 for Election Information

Free and fair elections are one of the main pillars of democracy. Regardless of political affiliation, state, or electoral district, Americans value our elections. One of the most detrimental impacts of MDM on American democracy is spreading false information about elections and candidates in an effort to suppress the vote of specific communities.

It should be easy for voters to quickly find out if they are registered to vote, when the next election is, and where to cast their ballot. Unfortunately, if someone does a quick internet search the results are mixed between issue advocacy organizations, nonprofits, as well as federal, state, and local government websites – including for states that are not where the voter resides.⁴⁴ Voters should not have to wade through a labyrinth of search results to find simple, accurate information.

Regardless of whether a voter is targeted for election-related MDM and wants to check a claim or simply wants to find out basic information about the next election, there should be an easy way for them to access those answers.

A centralized hotline that can debunk MDM and help voters know when and where to vote could greatly improve confidence in elections. There has been a nationwide adoption of 911 as the emergency services number, and many cities and municipalities across the country use 311 for local government information.

44. <https://cdt.org/insights/only-1-in-4-election-websites-uses-the-gov-domain-thats-a-problem-and-an-opportunity/>

RECOMMENDATIONS

I. Federal, State, Local:

A. Congress, state, and local governments should collaborate to create a centralized 311 (or similar) hotline for voters to get reliable, accurate, and local voting information. This hotline could be used by voters to answer questions about upcoming elections and also debunk/pre-bunk reported instances of MDM.

II. Federal:

A. Allocate federal funding to support the implementation and maintenance of the nationwide 311 hotline. This funding should prioritize technological enhancements and staffing to manage inquiries, ensuring prompt and accurate responses to voter queries and MDM concerns.

B. Enact federal legislation mandating the comprehensive inclusion of verified election information in the 311 hotline database. This legislation should ensure consistent updates and transparency across federal, state, and local electoral processes, enhancing public trust in election integrity.





III. State:

A. State governments should establish formal partnerships with the nationwide 311 hotline to ensure seamless integration of state-specific voting information. This collaboration should include regular updates on election laws, polling locations, and registration deadlines tailored to each state’s requirements.

B. States should also allocate resources to expand outreach and education campaigns that promote the use of the 311 hotline among voters. These initiatives should target diverse communities, including minority groups and non-English speakers, to ensure equitable access to accurate election information and combat misinformation effectively.

IV. Private Sector:

A. Tech companies and digital platforms should collaborate with government agencies to enhance the technological infrastructure of the nationwide 311 hotline. This partnership should focus on deploying AI and data management solutions to improve the hotline’s functionality and accessibility for users seeking verified election information.



Improve Algorithm Transparency

Social media companies gather a significant amount of data from their users, and they use this data to inform what we see while on their apps and websites. These meticulously crafted algorithms monitor user engagement with posts, videos, other sites, and applications to tailor future content recommendations in an effort to keep you on the site or app longer.⁴⁵

Whether you see a funny cat video, a conspiracy theory, or political advertisements depends on your daily interactions with the technology you're connected to and the data it collects from those interactions, to help the algorithm determine what will keep your attention the longest. Recently, whistleblowers like Francis Haugan have pulled back the curtain, leaking documents that indicated the company was aware of extremism and disinformation on its platform and chose to continue promoting that content by refusing to change, regulate, or acknowledge public concerns about the abuse of their private data, because it kept people on the platform and boosted profits.⁴⁶

While social media companies and their algorithms are not necessarily the driving force behind growing partisanship, polarization, and extremism in the United States, researchers suggest there is empirical evidence that it is a “key factor.”⁴⁷ This is due to the predictive analytics they employ to serve information to users based on their digital dust.

45. <https://georgetownlawtechreview.org/social-media-algorithms-why-you-see-what-you-see/GLTR-12-2017/>

46. <https://nytimes.com/2021/10/03/technology/whistle-blower-facebook-frances-haugen.html>

47. <https://www.brookings.edu/articles/how-tech-platforms-fuel-u-s-political-polarization-and-what-government-can-do-about-it/>

RECOMMENDATIONS

I. Federal:

A. Congress should enact legislation requiring social media companies to provide transparency into their algorithms and the data collected from users. This legislation should enable academic researchers, journalists, and nonprofit organizations to access algorithmic data to study their impacts on user behavior, polarization, and the spread of misinformation. Protections like deanonymization and decryption should be included to safeguard user privacy and data security. Additionally, provisions should protect researchers from legal actions aimed at stifling research into algorithmic influence on online misinformation and polarization.

B. Federal agencies should allocate research grants to fund independent research on the impacts of social media algorithms. These grants would support studies exploring alternative algorithmic approaches that prioritize accuracy, diversity of viewpoints, and mitigating the spread of misinformation.





RECOMMENDATIONS

II. State:

A. States should establish oversight commissions tasked with monitoring and reporting on the use of algorithms by social media platforms operating within their jurisdiction. These commissions would ensure compliance with federal transparency requirements and investigate local impacts of algorithmic content curation.

B. State legislatures should also enact accountability policies – outside of the protections of Section 230 of the Communications Decency Act – requiring social media companies to publish annual reports detailing how algorithms influence content distribution. These reports should include metrics on content moderation, diversity of viewpoints, and efforts to mitigate misinformation and extremist content.

III. Private Sector:

A. Social media companies should proactively collaborate with academic researchers and nonprofit organizations to facilitate independent audits of their algorithms. This collaboration should prioritize user privacy and data protection while enabling external scrutiny of algorithmic decision-making processes.

B. Social media companies should also partner with independent researchers to study alternative recommender algorithms that maximize high-value content while maintaining user engagement



Limited Real ID Verification on Social Media

The concept of the blue check on Twitter, introduced in 2009, was initially thought to distinguish official accounts from parody or impostor accounts, enhancing user trust and authenticity. Unlike traditional identity verification methods, however, this symbol wasn't based on user identification or documentation. It was based on marketing metrics.

Factors such as media mentions, the volume of relevant sources discussing them, on-platform engagement metrics, off-platform engagement metrics, market value, and audience reach played pivotal roles in determining verification status. This approach focused more on influence and visibility as assessed by algorithms, rather than simply follower count or user validation.

This broader approach inadvertently created opportunities for misuse. Malicious actors, including entities like the Internet Research Agency (IRA), exploited verified accounts to amplify misinformation and manipulate user perceptions. By leveraging the credibility associated with verified status, these actors could significantly impact public opinion and trust in online content.

Despite the ongoing use of ranking and authority systems to gauge content relevance and user influence, platforms have since revised their verification processes. These revisions reflect a recognition of the need for greater scrutiny and clarity in how verified status is assigned and maintained.



RECOMMENDATIONS

I. Federal:

- A.** Congress should collaborate with social media platforms to establish standardized, transparent criteria for verification. This should include clear metrics based on user identity, credibility, and authenticity, rather than ambiguous measures like off-platform relevance. Legislation could mandate regular audits and public reporting on verification practices to ensure accountability and mitigate misuse.
- B.** Federal agencies, such as the FTC, should be empowered to enforce regulations that protect users from deceptive practices involving verified accounts. This could involve fines or sanctions for platforms that fail to uphold transparent and fair verification standards.

II. State:

- A.** State legislatures should consider legislation that incentivizes platforms to adopt rigorous verification processes and penalizes misuse of verified status. Tax incentives or regulatory benefits could be offered to platforms that demonstrate proactive measures to combat misinformation and safeguard user trust.
- B.** Attorneys general in each state should collaborate to investigate and prosecute cases of fraud or deception involving verified accounts. State-level enforcement can complement federal efforts by addressing localized instances of misuse.



III. Private Sector:

A. Social media companies should enhance their verification procedures to prioritize user identity verification and reduce the risk of misuse. This includes implementing real-time monitoring and verification checks, possibly through partnerships with reputable third-party verification services.

B. An alternative solution is for social media companies to offer a free real ID check and verification status for users who wish to have a verified account. This ID verification process could be executed in partnership with a third-party company such as ID.me. Social media companies could still offer paid subscription models to access additional features. A free ID verification process would not only allow everyday users of the platform to verify their identity but also restore the ability to clearly identify notable figures, from journalists to celebrities, making the spread of dis/misinformation from imposter accounts much more difficult.



Coordinate the U.S. Government Response For a New Era of ‘Cold War’

Organizations across the national security community of the United States, including the White House itself, need to be reviewed for their efficacy in meeting the disinformation challenge to the West. This starts with empowering a special assistant to the president to coordinate efforts to counter malign foreign influence targeting the U.S. government, institutions, and citizens. The person in this role will also ensure that the White House communicates to Congress the need for any new authorizations and appropriations to sufficiently fund and equip executive agencies and departments. The administration also must provide the diplomatic leadership required for an international response to the common challenge posed by Russian, Chinese, and other adversarial interventions in the democratic processes of the West, as well as the sovereign independence of smaller countries around the world. Finally, the next administration must ensure the effectiveness of the U.S. government’s own international media agencies to tell our story and be a beacon for those craving truth and objectivity in the face of state-controlled media.

Additionally, the State Department and the Intelligence Community must have the ability to both identify and call out fake news, disinformation campaigns, and other types of “active measures.” When the Soviet Union launched a campaign in the Cold War with the bogus claim that the U.S. government had engineered HIV, the virus that causes AIDS, the Reagan administration created an interagency task force — the Active Measures Working Group (AMWG) made up of personnel from State, CIA, ACDA, USIA, DOD, and DOJ to begin to counter the Soviet disinformation effort. The AMWG not only monitored and assessed Soviet disinformation campaigns but also spoke to the press about their findings, even contacting newspaper editors who were running Soviet-sponsored stories. This group also enabled U.S. government (USG) officials to confront Soviet officials directly and publicly. Remarkably, there is still no government-wide task force designed to counter Russian, Chinese, or other disinformation campaigns targeting the United States.



Ultimately, fighting foreign malign influence begins with a recognition that its use by our adversaries is a foreign policy choice they have made. They will not stop until they have achieved their goals or the price of their pursuit becomes too great to bear. American foreign policy, then, has to determine whether foreign influence in our politics and institutions is acceptable. If it is not, then it is up to policymakers to craft policies – including the offensive use of our own influence campaigns—that raise the cost on adversaries who currently act within and against Western democracies with impunity.

RECOMMENDATIONS

I. Federal:

- A.** Empower a special assistant to the president to coordinate efforts across the government to counter malign foreign influence targeting the U.S. government, institutions, and citizens.

- B.** Relaunch the Active Measures Working Group (AMWG) made up of personnel from State, CIA, ACDA, USIA, DOD, and DOJ to identify and counter foreign disinformation threats.

- C.** Encourage coordination with the NATO alliance and other close allies (Australia, Japan, South Korea, New Zealand, etc) on harmonized efforts to deter and combat cyberthreats as they pertain to the undermining of our democratic institutions. Consider the introduction of collective action against adversaries like Russia, China, Iran, North Korea, and Venezuela when the United States or one of its allies' democratic institutions are attacked.



Acknowledgments

The task force and recommendations report are made possible by a grant from the John S. and James L. Knight Foundation and Microsoft. We thank them for their generosity, support, and leadership on these important issues.

Task Force Members

This report was informed by conversations with the McCain Institute and Cronkite School for Journalism and Mass Communication's Task Force on Defeating Disinformation Attacks on U.S. Democracy. Not all members of the Task Force endorse each recommendation and every view expressed in this report.

Dr. Evelyn N. Farkas, Executive Director, McCain Institute

Dr. Evelyn N. Farkas is the executive director of the McCain Institute. She has three decades of experience working on national security and foreign policy in the U.S. executive, legislative branch, private sector and for international organizations overseas. In 2019-2020 she ran to represent New York's 17th Congressional District in the House of Representatives. Previously, she was president of Farkas Global Strategies and a senior fellow at the German Marshall Fund of the United States and the Atlantic Council and national security contributor for NBC/MSNBC. She served from 2012 to 2015 as deputy assistant secretary of defense for Russia/Ukraine/Eurasia, Balkans, Caucasus and conventional arms control. From 2010 to 2012, she was senior advisor to the Supreme Allied Commander Europe and special advisor to the Secretary of Defense for the NATO Summit. From 2001 to 2008, she served as a professional staff member of the Senate Armed Services Committee. Dr. Farkas obtained her Ph.D. from The Fletcher School.

Joan Donovan, Boston University

Joan Donovan, PhD is an Assistant Professor of Journalism and Emerging Media Studies at Boston University, where she researches social movements, knowledge production, and the internet.



Ellen Gustafson, Co-Founder and Executive Director, We the Veterans

Ellen is a proud Navy Spouse and Navy and Coast Guard Granddaughter. She is a Co-Founder and the Executive Director of We the Veterans & Military Families, a non-partisan, non-profit organization that empowers the veteran and military family community to strengthen democracy. She is also the Co-Founder of the Military Family Building Coalition, the first non-profit supporting active duty military in building their families. She previously co-founded FEED, Food Tank and co-directed the Summit Institute. Ellen is the author of "We the Eaters: If We Change Dinner, We Can Change the World," has been a Fortune Most Powerful Women Entrepreneur and given four TEDxTalks. Ellen is a member of the Board of We the Veterans Society for American Democracy and is the Executive Director and Board member of We the Veterans Foundation.

Mark Jacobson, The Partnership for Public Service

Dr. Mark Jacobson has held a variety of policymaking roles in the US government, on Capitol Hill, and in international organizations as well as serving in the US Army as a psychological operations specialist. As an academic, Jacobson specializes in the history of propaganda, political warfare, and disinformation. He is currently completing a monograph on the US use of propaganda and psychological warfare during the Korean War. He holds degrees from the University of Michigan, King's College, London, and a PhD in military history from The Ohio State University.

K. Hazel Kwon, Arizona State University

K. Hazel Kwon (PhD in Communication, SUNY-Buffalo) is a Professor of Digital Audiences and the lead researcher at the Media Information, Data and Society Lab at Walter Cronkite School of Journalism and Mass Communication. Her research interests focus on social/digital media and society, with a particular emphasis on the ways in which networked publics make sense of news events and how the problem of information disorder redefines the process of informing the public. Some of her research has been supported by DoD, NSF, SSRC, and Gates Foundation. Dr. Kwon was selected as the U.S.-Korea NextGen scholar by CSIS.



Jim Ludes, Pell Center at Salve Regina University

Dr. Jim Ludes is Vice President for Strategic Initiatives at Salve Regina University in Newport, RI, as well as Executive Director of the university's Pell Center for International Relations and Public Policy. In addition, he is executive producer and co-host of "Story in the Public Square," an eight-time Telly Award-winning, weekly, public affairs program broadcast on SiriusXM's POTUS channel as well as on public television stations across the country. With Mark Jacobson he is co-creator and co-host of the Active Measures Newsletter and Podcast.

Tom Malinowski, Former US Congressman (NJ-7)

Tom Malinowski served two terms in the House of Representatives, after winning election in 2018 in New Jersey's 7th Congressional District. He was Vice Chairman of the House Foreign Affairs Committee and a member of the Transportation and Infrastructure Committee, focusing on issues ranging from national security and the war in Ukraine, to infrastructure, clean energy, social media regulation and combatting domestic extremism. From 1994 to 2001, Malinowski served as a speechwriter for Secretaries of State Warren Christopher and Madeleine Albright, and as a Senior Director on President Clinton's National Security Council. He later served as President Obama's Assistant Secretary of State for Democracy, Human Rights, and Labor, leading America's global efforts to promote human rights. Malinowski received his B.A. in Political Science from the University of California, Berkeley and earned a Master of Philosophy from St. Anthony's College, Oxford, where he was a Rhodes Scholar.

Matt Masterson, Director of Information Integrity, Democracy Forward Team, Microsoft

Matt Masterson is the director of information integrity for the Democracy Forward Team at Microsoft. Previously he served as a non-resident policy fellow with the Stanford Internet Observatory. He served as senior cybersecurity advisor at the Department of Homeland Security, where he focused on election security issues. He previously served as a commissioner at the Election Assistance Commission from December 2014 until March 2018, including serving as the Commission's chairman in 2017-2018. Prior to that, he held staff positions with the Ohio Secretary of State's office, where he oversaw voting- system certification efforts and helped develop an online voter registration system.



Tim Roemer, Chief Security Officer, Global Market Innovators, and President & GM, ThriveDX

Tim currently serves as the Chief Security Officer for Global Market Innovators, and President & GM for ThriveDX. Previously, Tim Roemer served as Arizona's Director of Homeland Security and Chief Information Security Officer. He has been working for the State of Arizona since the beginning of Governor Doug Ducey's administration, where he most recently served as the Deputy Director of Legislative Affairs. Prior to that, Tim held a dual role as the Governor's Public Safety Advisor and the Deputy Director for the Arizona Department of Homeland Security. Prior to joining the State of Arizona, Tim admirably served in the Central Intelligence Agency for 10 years. An Arizona native, Tim graduated from Arizona State University with a Bachelor of Arts degree in Communication and a minor in Political Science.

Kristy Roschke, Arizona State University


Kristy Roschke is the director of the News Co/Lab at ASU's Walter Cronkite School of Journalism and Mass Communication. Her research and teaching are focused on media literacy, misinformation and institutional trust. She is a board member of the National Association for Media Literacy Education.

Dhanaraj Thakur, Center for Democracy & Technology

Dhanaraj Thakur is Research Director at the Center for Democracy & Technology, where he leads research that advances human rights and civil liberties in tech policy. He has been interviewed and his work quoted in several news media, including WIRED, CNN, the WSJ, the Economist, and the Guardian (UK). He holds a PhD in Public Policy from the Georgia Institute of Technology, and graduated from the London School of Economics and the University of the West Indies (Jamaica).

Brette Steele, President, Eradicate Hate Global Summit; Chair, Prevention Practitioners Network

Brette Steele serves as President of the Eradicate Hate Global Summit and Chair of the Prevention Practitioners Network. Prior to joining Eradicate Hate, Steele served as Senior Director of Preventing Targeted Violence at the McCain Institute. Steele also served as the Regional Director of Strategic Engagement for the U.S. Department of Homeland Security Office of Terrorism Prevention Partnerships and Deputy Director of the U.S. Countering Violent Extremism Task Force and Senior Counsel to the Deputy Attorney General and coordinated the U.S. Department of Justice's terrorism prevention and forensic science reform initiatives.



Rachael Dean Wilson, Managing Director, Alliance for Securing Democracy and US Elections

Rachael Dean Wilson is managing director of the Alliance for Securing Democracy (ASD) at GMF, where she leads work on US elections and political analysis. Driven by her belief that safeguarding democracy must involve all Americans, Wilson has spoken in cities across the country about the importance of building democratic resilience to autocratic efforts to undermine democracy. Wilson served in senior roles on Capitol Hill and political campaigns, and has experience in corporate communications and PR consulting. She worked for the late Senator John McCain for six years, most recently as his Senate communications director and advisor to his 2016 reelection campaign.

Other significant contributors:

Michael Baldassarro, The Carter Center; Rachel Brown, Over Zero; Anthony Demattee, The Carter Center; Stefanie Lindquist, Arizona State University; Scott Ruston, Arizona State University



McCain Institute Program Staff:

Paul Fagan, Director of the Democracy Programs, McCain Institute

Paul Fagan is the director of the Democracy Programs for the McCain Institute at Arizona State University. Previously, he served as the executive director of the Eastern Congo Initiative (ECI), an organization founded by Ben Affleck that seeks to bring the world's attention to the ongoing situation in that country but also highlight the abundant opportunities for economic and social development. Prior to joining ECI, Fagan worked at the International Republican Institute (IRI), an organization that promotes democracy worldwide by developing political parties, civic institutions, democratic governance and the rule of law.

Mike Brand, American Democracy Fellow, McCain Institute

Mike Brand is a Democracy Fellow with the McCain Institute where he supported the work of the the Task Force on Defeating Disinformation Attacks on U.S. Democracy. Mike has spent most of his career focused on mass atrocities prevention, human rights, and peacebuilding policy, advocacy, organizing, and education. He has been published in peer-reviewed journals, national and international publications, and has been quoted in international news outlets as an expert in his field. Mike is also an Adjunct Professor at Georgetown University and the University of Connecticut where he teaches courses on mass atrocities prevention and human rights.

Luke Englebert, Senior Program Coordinator, McCain Institute

Luke Englebert currently serves as the Senior Program Coordinator for the Democracy Program at the McCain Institute. Prior to rejoining the McCain Institute's staff, Luke served as a program associate for Francophone Central Africa at the International Republican Institute. Previously, Luke worked as the Counterterrorism Center program assistant at the McCain Institute and also interned with the Institute's Human Rights & Democracy program during the summer of 2017. Originally from Claremont, California, Luke graduated from the University of Redlands with a B.A. in international relations.

Additional Resources



McCain Institute:

[Defending Disinformation in the Digital Age](#)

For decades, technology has fostered the advancement of freedom, transparency, and liberty. The more technology has been employed in elections and allowed people to access information, the more democracy benefitted. Yet, over time, technology also became a tool to undermine democracy. To address these threats against American democracy, the McCain Institute and Cronkite School co-hosted an event titled “Defending Democracy in the Disinformation Age.”

[Defending American Democracy Conversations](#)

The McCain Institute has launched a series of complementary and mutually reinforcing conversations designed to advance this cause by convening key stakeholders, empowering likeminded organizations, engaging elected officials, and communicating with the public.

- [Is the Loss of Local Journalism Endangering American Democracy?](#)
- [When Local Elections are Threatened, What are the National Implications?](#)
- [Protecting U.S. Democracy’s Elections Systems and Infrastructure Against Cyber Attacks](#)
- [Courage in American Leadership: A Conversation with Congresswoman Liz Cheney](#)
- [Why Do Foreign Actors Want to Erode U.S. Democracy?](#)

[The Disinformation Economy](#)

The McCain Institute at Arizona State University (ASU) and the Carter Center released The Disinformation Economy. The latest joint report by the two organizations examines the prevalence of disinformation on over 300 ad systems and how many of these platforms facilitate the monetization of disinformation.



The Carter Center:

[Monitoring Online Political Advertising: A Toolkit](#)

During an electoral process, electoral actors, whether contestants or noncontestants, have the right to advertise political ideas in accordance with the right of expression. However, political advertising may be subject to reasonable limitations through regulations imposed by domestic law, including who can run political advertisements, when and where they may run advertisements, restrictions on advertising expenditure levels, and reporting and disclosure requirements to ensure transparency, accountability, and a level playing field.

[The Big Lie and Big Tech: Misinformation Repeat Offenders and Social Media in the 2020 U.S. Election \(PDF\)](#)

The Carter Center published “The Big Lie and Big Tech,” a new report that details the role played by “repeat offenders” – media known to repeatedly publish false and misleading information—in spreading election fraud narratives in online echo chambers during the 2020 election.

Center for Democracy and Technology:

[Women of Color Political Candidates in the US Endure Most Severe Online Abuse, Mis- and Disinformation](#)

This project examines the scale and impact of mis- and disinformation on women of color political candidates. Using a content analysis of a random selection of tweets during the 2020 election period that were in response to, or mentioned one of, a representative sample of all candidates that ran for Congress, this project codes for a range of categories including mis- and disinformation and many types of abuse.

[Learning to Share: Lessons on Data-Sharing from Beyond Social Media](#)

In this report, we look to other industries where companies share data with researchers through different mechanisms while also addressing concerns around privacy. In doing so, our analysis contributes to current public and corporate discussions about how to safely and effectively share social media data with researchers. We review experiences based on the governance of clinical trials, electricity smart meters, and environmental impact data.

[A Lie Can Travel: Election Disinformation in the United States, Brazil, and France](#)

This report examines case studies of election disinformation – and interventions aimed at combating disinformation—in the U.S., Brazil, and France.



Center on Narrative, Disinformation, and Strategic Influence at Arizona State University:

[ASU experts explore national security risks of ChatGPT](#)

This article is the first of a two-part series about the ways that AI, including large language models like ChatGPT, impacts society and how ASU researchers are addressing its opportunities and challenges.

[Can policy get smart enough for artificial intelligence?](#)

This article is the second of a two-part series about the ways that AI, including large language models like ChatGPT, impacts society and how ASU researchers are addressing its opportunities and challenges.

Cronkite School for Journalism and Mass Communication, Arizona State University:

[Is Aggression Contagious Online? A Case of Swearing on Donald Trump's Campaign Videos on YouTube](#)

This study examines empirical evidence of the contagion of offensive comments by exploring two mechanisms of swearing on YouTube: Public vs. Interpersonal.

[Gatekeeping practices of participants in a digital media literacy massive open online course \(MOOC\)](#)

Long before “fake news” dominated the conversation within and about the media, media literacy advocates have championed the need for media literacy education that provides the tools for people to understand, analyze, and evaluate media messages. Social media’s shareability can dictate how information spreads, increasing news consumers’ role as a gatekeeper of information and making media literacy education more important than ever.

[Doctors Fact-Check, Journalists Get Fact-Checked: Comparing Public Trust in Journalism and Healthcare](#)

Public trust in journalism has fallen disconcertingly low. This study sets out to understand the news industry’s credibility crisis by comparing public perceptions of journalism with public perceptions of another institution facing similar trust challenges: healthcare.

[J-guard: Journalism guided adversarial robust detection of ai-generated news](#)

The rapid proliferation of AI-generated text online is profoundly reshaping the information landscape. Among various types of AI-generated text, AI-generated news presents a significant threat as it can be a prominent source of misinformation online. To address these challenges, we leverage the expertise of an interdisciplinary team to develop a framework, J-Guard, capable of steering existing supervised AI text detectors for detecting AI-generated news while boosting adversarial robustness.



Democracy Forward Team, Microsoft:

Meeting the moment: Combating AI deepfakes in elections through today's new tech accord

The tech sector came together at the Munich Security Conference to take a vital step forward. Standing together, 20 companies announced a new Tech Accord to Combat Deceptive Use of AI in 2024 Elections. Its goal is straightforward but critical – to combat video, audio, and images that fake or alter the appearance, voice, or actions of political candidates, election officials, and other key stakeholders. It is not a partisan initiative or designed to discourage free expression. It aims instead to ensure that voters retain the right to choose who governs them, free of this new type of AI-based manipulation.

From tipping point to turning point: Charting new pathways for rebuilding local news

As part of our work to address this crisis and turn the tide in favor of more successful and sustainable local newsrooms, today we are announcing the release of a comprehensive guidebook focused on giving independent local news organizations the strategies, tools, and support they need to strengthen their sustainability. The guidebook provides a framework for understanding choices available to journalists, newsrooms, civic institutions, and community stakeholders.

Expanding our Content Integrity tools to support global elections

Microsoft announced the expansion of the private preview of its Content Integrity tools to EU political parties and campaigns and news organizations from around the world. Microsoft deeply believes that healthy democracies depend on healthy information ecosystems. Through this expansion they are delivering tools these organizations can use to help voters understand the information they encounter online.

In the digital age, democracy depends on information literacy

To help equip people to better understand and have confidence in the information they consume, Microsoft has pointed to utilizing information inoculation methods that can be scaled and disseminated. Media literacy campaigns are not designed to tell anyone what to believe or how to think; rather, they are about equipping people to think critically and make informed decisions about what information they consume.



Partnership for Public Service:

[Innovation and Technology Modernization Policy Recommendations](#)

Our government faces an array of critical and complex challenges, including protecting public health and the environment, caring for veterans, responding to natural disasters, and safeguarding our national security.

[Rebuilding Trust in Government](#)

America is experiencing a crisis in public trust in government. This lack of trust has serious implications for how the public interacts with our government and how federal agencies respond to the major challenges facing the country – both of which are critical to a healthy and vibrant democracy.

Pell Center for International Relations and Public Policy, Salve Regina University:

[The Pell Center Active Measures Newsletter Podcast](#)

Since 2018, the Pell Center has produced the Active Measures Newsletter, a weekly dive into the murky world of disinformation, influence, and information campaigns. Now, beginning Monday, April 22, 2024, the conversation continues with the debut of the Active Measures Newsletter Podcast. Released every Monday, continue the conversation with Jim Ludes and Mark Jacobson as they discuss the biggest headlines from the latest edition of Active Measures, interview special guests, and try to make sense of the campaigns happening right before everyone's eyes.

We the Veterans:

<https://vetthe.vote/>

A national campaign to recruit and educate veterans and military family members to become the next generation of poll workers.