

**The Subcommittee on Elections of the Committee on House Administration
Hearing on “A Growing Threat: Foreign and Domestic Sources of Disinformation”
July 27, 2022**

Chairman Butterfield and Members of the Committee, thank you for the opportunity to testify today.

My name is Jiore Craig. I am the Head of Digital Integrity at the Institute for Strategic Dialogue (ISD) where I oversee our work around elections. ISD is a not-for-profit think-tank focused on countering extremism, disinformation, and hate worldwide.

I have spent nine years as a public opinion researcher examining how foreign and domestic actors use social media during elections to deceive their publics. My experience includes hundreds of elections in the United States and more than a dozen other countries, including in Central and Western Europe, Central Africa, Southeast Asia, the Caribbean, Australia, and Latin America.

I appreciate the Committee taking time to understand how the threat of foreign and domestic disinformation puts the American public at risk. I hope you will take one big point away from my testimony today: disinformation targeting voters remains a significant threat – not only to our own citizens, but to citizens in democracies worldwide. We will only counter it effectively if we look at the systems, policies, product features, and business models that drive the actions of social media companies and those sourcing disinformation, instead of merely chasing after the false or pernicious content that specific disinformation campaigns promote.

Domestic and foreign sources of disinformation targeting Americans

The disinformation marketplace is made up of state-sponsored foreign actors, foreign and domestic commercial actors, and ideologically driven domestic actors seeking political power and control. It is impossible to know the precise breakdown of foreign vs. domestic disinformation efforts. Our inability to know this is due in large part to a lack of transparency on the part of the social media platforms.

However, ISD’s work to date suggests domestic disinformation targets Americans at a higher volume and frequency than foreign campaigns. Research also suggests that the domestic sources of disinformation enable the success of many foreign efforts as both rely on exploiting cultural tensions and partisan rhetoric.

Much domestic disinformation is well-resourced, references real world people and events, and deliberately uses social media product features like targeted advertising, recommendation systems, and “explore” feeds that are opt-in by default to seed disinformation.

Consider the following report of domestic disinformation: research found a website purporting to represent an organization which lacked meaningful contact information called “Protect My Vote”. In 2020, “Protect My Vote” ran a digital ad campaign with more than 150 paid ads on Facebook; their aim was to erode trust in mail-in voting in target battleground states with high concentrations of voters of color. Some of the paid posts featured an image of LeBron James and falsely claimed he had expressed concerns about the safety of mail-in voting. [Facebook eventually removed the page](#) for engaging in voter suppression tactics. This example features tactics common to many successful disinformation campaigns, including misleading organization names, the

unauthorized use of trusted messengers, spurious linkages of unrelated issues, hidden sources of advertising funds as well as Facebook's election policies and advertising model in action.

Foreign sources of disinformation can be state-sponsored actors promoting state-interests via overt, semi-covert or fully covert activity; or ideological groups with no single geographic home who are sharing tactics across borders; or it can come from commercial actors available for hire based overseas. Recent research from my ISD colleagues and others points to several state-sponsored attempts to promote foreign interests among American audiences, including attempts from Russia, China, and Iran. Additional research suggests commercial and ideological Spanish-language disinformation is moving across borders from Central and South America.

Anyone can decide to pursue disinformation tactics for profit, and anyone can hire commercial actors to use disinformation tactics to influence an election. The online presence of such commercial actors can be as anonymous and profitable as laws and platform policies allow.

Foreign commercial actors often use unethical tactics to inflate metrics, such as the view count on a video. In some cases, they may employ rooms full of internet savvy young people, paid by the hour, to run accounts that appear native to the target country. These troll farms may post on both sides of a culturally sensitive debate, such as around race, identity, or crime, to elevate the issue or create a sense of conflict.

In many cases, foreign disinformation actors, whether they are state-sponsored or commercial, try to hitch a ride on homegrown narratives. That is, they play on divisive issues or controversy originating in the United States. The success of their campaign often requires the willing or unwilling participation of Americans to help spread the disinformation.

Disinformation tactics in foreign elections

Electoral disinformation has become a global enterprise, and each election serves as a petri dish for experimenting and learning from fellow disinformation entrepreneurs' global experiences. Already this year voters in Australia, France, Germany, and Colombia were targets of electoral disinformation. The disinformation tactics in each case often borrowed from playbooks in other countries.

In May, [ISD's research](#) highlighted how Australian voters were targeted with disinformation claiming Dominion voting machines, which had baselessly been tied to vote manipulation in the US, would be used in Australia and might lead to fraud. This claim was pushed across social media platforms including Facebook and Telegram despite Australian law forbidding the use of voting machines all together. [Recent French elections saw](#) the same disinformation claim around Dominion voting machines where most votes are cast with paper ballots.

Facebook and Twitter made statements about their commitment to fighting electoral disinformation ahead of both the French and Australian elections. Yet the actual policies of both companies still fall short of stopping disinformation at the source.

Content vs. Systems

In our country and in other democracies, there is understandably an intense focus on the content of electorally-focused disinformation efforts. But this focus on content can obscure the role of systems at play in enabling disinformation. Recent reporting demonstrates that [the way these companies make business decisions about what to show Americans around elections has a significant impact on how successful disinformation campaigns are in reaching Americans.](#) Those sourcing disinformation are experts in maximizing social media product features and loopholes to achieve their ends. This is why it is so important to focus on the systemic aspects of social media companies, such as their business models or product features, geopolitical and commercial interests.

There are two key reasons that a focus on disinformation *content* often eclipses disinformation *systemic forces*. First, most of us primarily experience disinformation as content. Voters, journalists, and researchers have extremely easy access to disinformation on a day-to-day basis. It is much harder to obtain information about the hidden *systems* that enable such disinformation - like who is paying for the content, who is making money from a person engaging with content, or whether the accounts sharing content are neighbors, foreign citizens, or fake accounts. This opacity is no accident. Social media companies are intentionally not transparent with much of this information. And while there have been a few improvements, in terms of social media companies sharing systemic information, they are worse in many other ways following increased scrutiny of platform transparency.

The second reason the conversation tends to focus on content rather than systemic dynamics is because many stakeholders in the disinformation marketplace want to center free speech protections naturally evoked in a debate focused on content – First Amendment protections in the US, or similar protections in many other countries. Unfortunately, this approach does not protect free speech – which should be defended at all costs – but instead helps stakeholders avoid a conversation about systems, like social media business models and product features, which if examined would likely lead to further protections for speech and help to defend First Amendment rights. Until then, these systems enable them and others to profit from disinformation campaigns.

If we stay focused on content and not on systems, those spreading disinformation for ideological or political gain can continue using social media to take full advantage of the product features enabling their successful campaigns.

I urge those trying to understand how disinformation targets Americans to shift their focus away from content alone and toward the systems moving disinformation into Americans' newsfeeds. A focus on such systemic dynamics is essential to hold social media companies and disinformation bad actors accountable. We cannot just debate which meme is more rooted in fact. We need to debate which systems at play in disinformation should change to end the downward spiral of trust that Americans have started to have in their own democracy, and even more important, in each other.

Trust in Elections, Democracy, and Each Other

Disinformation campaigns vary. But most of them share a common target: trust. The initial goal for architects of many disinformation campaigns is to build trust, or to destroy trust.

[According to Pew Research](#), nearly 70% majority of Americans use social media platforms, like Meta-owned Facebook, to keep up with friends and family or explore personal interests. Social media's expansive reach makes it a perfect place to go after the public's trust.

Foreign and domestic disinformation sources aim to gain trust by blending in on social media. They disguise themselves as local media websites or use fake accounts posting with references to local sports teams or using informal language specific to certain communities. Other times, disinformation does not make claims at all, but rather asks repeated questions designed to plant a seed of doubt about a person, politician, media outlet, or institution.

At the heart of most disinformation campaigns is an attempt to control. When people feel their trust has been broken, they tend to grow insecure, when people are insecure, they grow defensive. And when they are defensive for a long time, people get tired and ultimately easier to influence or even control.

Voters' views on the spread of disinformation

A recent Data for Progress survey suggests an 86% majority of American likely voters believe social media plays a very or somewhat significant role in the spread of false information from person to person. A 66% majority also believe social media CEOs profit from election lies and conspiracies. To curb the threat of disinformation, social media platforms need to be held accountable. We need not make them the arbitrators of truth in elections. But we can ensure they do not profit from foreign and domestic actors' use of their product features to disrupt American elections.

Solutions

ISD works together with partners in the US on solutions to the systems propping up election disinformation including evidencing policy debates through our Digital Policy Lab (DPL), tracking the disinformation marketplace around elections through our Digital Analysis Unit, and mitigating its harm through education, violence prevention, and communication work with trusted local messengers, stakeholders, and communities to build resilience against the threat of disinformation.

The Digital Policy Lab is an intergovernmental network of policy officials from Five Eyes and European countries including representation from the European Commission and regulators essential to digital policy. In 2021, ISD's DPL initiated a new cycle of discussions on the theme "A Democratic Internet: Systemic Approaches to Combatting Online Harms." To kick-off this cycle, a session on the range of harms impacting the integrity of elections provided an overview to the complex threat environment, from extremism, targeted harassment of politicians and election workers, to disinformation and conspiracy theories. These conversations help evidence ongoing debates in the European Union, especially around the recent Digital Services Act which takes a systems approach to platform regulation in contrast to previous EU legislation focused on content.

Additional Resources

ISD: [Elections 2022: The French Information Ecosystem put to the Test](#)
ISD: [“US-imported” voter fraud claims on the rise on Facebook in the lead up to elections in Australia](#)
ISD: [Anatomy of a Disinformation Empire: Investigating NaturalNews](#)
ISD: [Hoodwinked: Coordinated Inauthentic Behaviour on Facebook](#)
ISD: [Reply All: Inauthenticity and Coordinated Replying in Pro-Chinese Communist Party Twitter Networks](#)
BBC Panorama: [How misogynistic hate benefits from algorithms and propels through social media](#)
Washington Post: [Facebook removes page using image of LeBron James over ‘voter suppression tactics’](#)
Washington Post: [Disinformation campaign stokes fears about mail voting, using LeBron James image and boosted by Trump-aligned group](#)
New York Times: [Facebook Struggles to Balance Civility and Growth](#)
Pew Research: [Social Media Usage in 2021](#)
Data for Progress: [Voters Believe Social Media Companies Profiting From Conspiracies and Lies Are Driving Divisions in America](#)
The Verge: [Meta reportedly plans to shut down CrowdTangle, its tool that tracks popular social media posts](#)
Dr. Safiya Umoja Noble: [Algorithms of Oppression: How Search Engines Reinforce Racism](#)
Brookings: [Disinformation Threat to Diaspora Communities in Encrypted Chats](#)