*Statement of*

**NINA JANKOWICZ**

***Disinformation Fellow***

***Woodrow Wilson International Center for Scholars***

***Science and Technology Innovation Program***

**BEFORE THE**

**UNITED STATES HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE**

***Concerning***

# "Misinformation, Conspiracy Theories, and 'Infodemics': Stopping the Spread Online"

**October 15, 2020**

### *Introduction*

Chairman Schiff and distinguished Members of the Committee, it is an honor to testify before you today on the degradation of our information ecosystem and its exploitation by malign actors, both foreign and domestic. This is a threat that is dismantling our democracy. As Americans exercise their democratic rights during this election season, it is critical the nation is informed about how this phenomenon works and how it might blunt their voice and their vote.

I came to study this problem through the lens of Russian foreign influence operations. I began my career at the National Democratic Institute, a frequent target of Russian disinformation campaigns thanks to its support of democratic activists in the country. Under a Fulbright Public Policy Fellowship, I worked as a strategic communications adviser to the Ukrainian Ministry of Foreign Affairs on the front lines of Russia's information war. I spent the last three years researching how our allies in Central and Eastern Europe dealt with Russian online aggression long before the United States even recognized it as a threat; the result is my book, *How to Lose the Information War*.[1] Given that title, you will not be surprised that my work has led me to an unsettling conclusion: **not only have the U.S. Government and social media platforms all but abdicated their responsibility to stop the threat of *foreign* disinformation over the past four years, *domestic* disinformation now runs rampant. It is amplified in the media, online, in the halls of Congress, and from the White House itself. It does our adversaries' work for them, leaving us vulnerable to continued manipulation and leaving our democracy imperiled.**

Today I will outline several examples that exemplify the trends in the information space since 2016. They hold several important morals for policymakers. First, disinformation is a threat to democracy, no matter where it comes from or who it benefits, and until our government recognizes this, we cannot hope to counter it. Second, social media platforms' structures and business models incentivize the spread of disinformation; until these business models change, we will continue to play a never-ending game of Whack-a-Troll. Third, these campaigns have stark implications for women and minorities' participation in democracy. Finally, I will discuss what I view as the most urgent -- and undervalued -- policies necessary to improve the health of our online information ecosystem.

### *Trend 1: Authentic Voices and Information Laundering*

The threat of foreign disinformation has never been about cut-and-dry "fake news." As I laid out in testimony before the Senate Judiciary Committee in 2018, and as my book describes in great detail, Russian disinformation seizes on our societal fissures -- including racism, economic inequality, and divisive political battles -- to further discord in America, turn Americans against

[1] Nina Jankowicz, *How to Lose the Information War: Russia, Fake News, and the Future of Conflict* (London: Bloomsbury/IBTauris, 2020).

one another, drive distrust in the government, and encourage disengagement both from the traditional information ecosystem and the democratic process.[2]

The most successful disinformation exploits real grievances in a given society. Increasingly, thanks to growing public awareness about disinformation and basic actions the social media platforms have taken to crack down on networks of inauthentic accounts, malign actors are investing more in information laundering: the use of authentic local voices or organizations to conceal the origin of and lend legitimacy to a given malign narrative.[3,4,5]

Perhaps the most well-known example of information laundering from the past four years (and one that this committee knows intimately) is the nexus of conspiracy theories related to Ukraine, the 2016 election, and Vice President Joe Biden. These unsubstantiated and misleading narratives, promoted by self-interested and corrupt individuals seeking power and personal gain by currying favor with the Trump administration, were endorsed by the President's advisers, treated as fact by portions of the media, and legitimized within the halls of Congress.[6,7] Individuals that served as sources for the theories have since been discredited, sanctioned, and revealed to have active connections to Russian intelligence services. While these theories were amplified in part on social media, they were mainstreamed by powerful individuals with connections to the President, underlining that disinformation is not only a problem for social media companies to combat, but a problem that requires the active recognition of politicians and the American public. Until our elected officials recognize that disinformation knows no political party and its ultimate victim is democracy, we cannot hope to make progress in countering it.

Another instructive example of foreign interference through authentic local voices is the hijacking of activist groups to drive partisan rancor. On July 4, 2017, Russia's Internet Research Agency (IRA) targeted a flash mob in front of the White House, where progressive groups planned to protest the President, gathering in full colonial garb to sing parodies of songs from the musical *Les Miserables*. A criminal complaint filed in the Eastern District of Virginia in 2018 revealed the IRA "contact[ed] the Facebook accounts for three real US organizations to inquire about collaborating with these groups on an anti-President Trump 'flash mob' at the White

[2] Nina Jankowicz, "Testimony before the U.S. Senate Committee on the Judiciary concerning 'Election Interference: Ensuring Law Enforcement Is Equipped to Target Those Seeking to Do Harm,'" June 18, 2018.
[3] Boris Toucas, "Exploring the Information-Laundering Ecosystem: The Russian Case," Center for Strategic and International Studies, August 31, 2017.
[4] Kirill Meleshivich and Bret Schafer, "Online Information Laundering: The Role of Social Media," German Marshall Fund/Alliance for Securing Democracy, January 9, 2018.
[5] Joan Donovan and Brian Friedburg, "Source Hacking: Media Manipulation in Practice," Data & Society, September 4, 2019.
[6] Scott Shane, "How a Fringe Theory About Ukraine Took Root in the White House," *The New York Times*, October 3, 2019.
[7] Zoe Tillman, "Trump's Campaign Was Talking About The Conspiracy Theory That Ukraine Was Involved In The DNC Hack Back In 2016," *BuzzFeed News*, November 2, 2019.

House."[8] The IRA spent $80 to promote the flash mob, targeting the event to individuals "within 30 miles of Washington, DC, including significant portions of the Eastern District of Virginia," reaching an estimated 29,000 to 58,000 people.[9] I interviewed one of the organizers of the flash mob, who had no idea the IRA had infiltrated his group, and credits the protest's high turnout and visibility to the IRA-purchased advertising.[10]

A similar tactic was employed in the recently-uncovered PeaceData operation, a campaign run by IRA-affiliates targeting left-leaning social media users. Using a handful of fake accounts with artificial intelligence-generated profile pictures, the malign actors behind PeaceData identified American freelance journalists and commissioned them to write articles for the site reflecting well-known anti-establishment narratives.[11] Rather than use a large network of inauthentic accounts to amplify the PeaceData content, the malign actors shared it in left-wing Facebook Groups, including those targeting environmentalists, Social Democrats, and Julian Assange supporters.

These cases exemplify how our informational adversaries do not always necessarily create disinformation narratives wholecloth, but instead manipulate preexisting polarization and tension on both sides of the political spectrum, sometimes with the witting or unwitting participation of local groups. As one of the organizers of the *Les Mis* flash mob told me, "If you can weight the sides, you can really pull at the fabric of society. You can pull it apart."

***Trend 2: Platforms Create Conspiracy Convergence***

The use of local actors and information laundering makes cracking down on disinformation through content moderation alone much more difficult, given First Amendment protections. It also highlights how social media platforms' current incentive structures are weaponized. Foreign and domestic disinformers take advantage of them to seed malign narratives, achieve virality, and contribute to conspiracy convergence, when adherents of one theory are exposed to and encouraged to spread others.

During the 2018 Midterm Elections, I uncovered a small astroturfing operation associated with an independent U.S. Senate candidate in Massachusetts.[12] Using a handful of fake accounts which cross-posted material in favor of their candidate on pro-Donald Trump, anti-Elizabeth Warren Facebook groups, the operation attempted to give the guise of grassroots support for its candidate. Groups provided the perfect vector for this operation; members were already segmented by interest and affinity, and in the aftermath of the Cambridge Analytica scandal and

[8] United States v. Elena Alekseevna Khusyanynova, 1:18-MJ-464 (E.D. Va 2018), 24.
[9] Ibid.
[10] Nina Jankowicz, "How an Anti-Trump Flash Mob Found Itself in the Middle of Russian Meddling," POLITICO Magazine, July 5, 2020.
[11] Ben Nimmo et al, "IRA Again: Unlucky Thirteen," Graphika, September 1, 2020.
[12] Nina Jankowicz, "Shiva Ayyadurai's Senate Campaign Was Being Promoted By Fake Facebook Accounts," *BuzzFeed News*, October 2, 2018.

revelations about Russian interference, Facebook was beginning to prioritize closed and private spaces on its platform in response to user demand.

Facebook's reliance on groups as a core part of its platform experience has only increased since 2018. Now, as a default platform setting, members of groups receive notifications about content posted in their groups, and that content is prioritized in their news feeds. They are also recommended content from groups "similar" to those of which they are already a member. Over the course of this year, as Americans searched for information and answers about the coronavirus pandemic, groups have become a fertile ground for seeding and amplifying disinformation and have led to the convergence of conspiracies and malign disinformation that has had serious effects on public health, public safety, and the democratic process. As my fellow panelist Cindy Otis and I found in June, conspiracies ran rampant across groups on the platform, taking advantage of the recommendation algorithm to cross-pollinate between communities and indoctrinate new members.[13] And in my own hometown in New Jersey, a gym owner who reopened his business despite a stay-at-home order became an unwitting medical freedom celebrity after he shared his plans to a "Reopen NJ" Facebook group.[14] His "cause" quickly traveled across the platform and was seized upon by "similar" groups, including some that believed the coronavirus pandemic was a political hoax.

Facebook has recently taken harsh action against the QAnon conspiracy, banning all accounts related to the movement across all of its platforms.[15] It is an encouraging step, but QAnon is only one of the pollutants affecting the health of the information ecosystem and our democracy. As the 2020 election season draws to a close, unsubstantiated allegations of voter fraud and ballot harvesting continue to gain prominence on the platform. For example, a recently-debunked domestic disinformation campaign accusing Rep. Ilhan Omar of voter fraud boasts over one million interactions across about 60,000 public Facebook posts in the past month.[16] Of the top 50 most-interacted-with posts, all but one endorse the conspiracy. Only a post from *Newsweek* with about 4,600 interactions and 14 shares casts doubt on it while the top post about this disinformation narrative boasts 80,000 interactions and over 24,000 shares.[17]

Facebook has also shifted its approach to political advertising ahead of the election, putting all political and issue-based ads on pause after November 3 and placing a "votes are still being counted" announcement at the top of users' news feeds to fend off premature declarations of victory.[18] While turning off political advertising in the aftermath of the election will hamper the ability of some disinformers to target damaging narratives to select audiences, it will do little to

[13] Nina Jankowicz and Cindy Otis, "Facebook Groups are Destroying America," *WIRED*, June 17, 2020.
[14] Nina Jankowicz, "How an Anti-Shutdown Celebrity is Made," *The Atlantic*, October 3, 2020.
[15] Ben Collins and Brandy Zadrozny, "Facebook Bans QAnon Across its Platforms," NBCNews, October 6, 2020.
[16] Maggie Astor, "Project Veritas Video Was a 'Coordinated Disinformation Campaign,' Researchers Say," *The New York Times*, September 29, 2020.
[17] CrowdTangle Team (2020). CrowdTangle. Facebook, Menlo Park, California, United States.
[18] Guy Rosen, "Preparing for Election Day," Facebook, October 7, 2020.

address the problem as a whole.[19] Ads are not the major vector of disinformation on the platform; organic content is. The most successful content spread by Russian IRA operatives in the 2016 election was amplified this way. The Oxford Internet Institute found that "IRA posts were shared by users just under 31 million times, liked almost 39 million times, reacted to with emojis almost 5.4 million times, and engaged sufficient users to generate almost 3.5 million comments," all without the purchase of a single ad.[20]

The policy also leaves aside the most obvious source of disinformation: high-profile, personal accounts to which Facebook's Community Standards seemingly do not apply. President Trump pushes content—including misleading statements about the safety and security of mail-in-balloting—to nearly 30 million users on his page alone, without accounting for the tens of millions who follow accounts belonging to his campaign or inner circle.

Facebook's decision -- and its lack of action on other misleading and false content on the platform -- also underlines another fundamental error in its thinking and misalignment in its incentive structures: disinformation campaigns do not begin and end on November 3. They are built over time, trafficking in emotion and increased trust, in order to undermine not just the act of voting but the democratic process as a whole. When our information ecosystem gets flooded with highly salient junk that keeps us scrolling and commenting and angrily reacting, civil discourse suffers. Our ability to compromise suffers. Our willingness to see humanity in others suffers. Our democracy suffers. But Facebook profits.

In the first week of October alone, the presidential candidates and their running mates have bought more than $12.5 million worth of Facebook advertising.[21] In 2019, Facebook generated 98 percent of its revenue -- a whopping $69.7 billion -- from ads.[22] And that is leaving aside Facebook's most valuable asset: us, its users. The platform has an economic incentive to keep us scrolling through our news feeds, reacting, sharing, and commenting, as it adds more to the data profiles that will make its advertising services so valuable to its customers. It will continue to feed us the most engaging, and therefore most enraging content, because that is how it keeps us hooked and keeps providing us, its product, to advertisers. That emotional content is manipulative at best and disinformation at worst.

### *Trend 3: Effects on Women and Minorities*

Given that today's hearing features a brilliant all-female panel, I would be remiss if I did not mention the fact that disinformation campaigns often target women and minorities to the

[19] Nina Jankowicz, "Facebook's 'Kill Switch' Solves the Wrong Problem," *WIRED*, August 21, 2020.

[20] Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François, "The IRA, Social Media and Political Polarization in the United States, 2012–2018," Working Paper 2018.2. Oxford, UK: Project on Computational Propaganda.

[21] According to the Facebook Ad Library, October 12, 2020.

[22] Rishi Iyengar, "Here's how big Facebook's ad business really is," CNN Business, July 1, 2020.

detriment of our democracies. We know, for instance, that the Internet Research Agency disproportionately targeted Black voters during its 2016 operation in an attempt to suppress the Black vote.[23] My own research has identified several instances in which the Kremlin has targeted women in democratizing nations in Eastern Europe with sexualized disinformation campaigns meant to undermine their credibility and drive them from participation in public life.[24] This trend also exists in the United States, driven by domestic actors. For instance, in an ongoing Wilson Center project tracking the use of gendered and sexualized disinformation against female politicians in the 2020 election, my team has observed an increase in individuals spreading malicious, false, sexualized narratives against Senator Kamala Harris ahead of Election Day. On the night of the recent Vice Presidential Debate, instances of hashtags containing sexualized disinformation or violence against Senator Harris on platforms Parler and 4Chan increased 631 percent and 1078 percent, respectively. These campaigns -- whether beginning in Russia or within our own borders -- are meant to affect American women and minorities' participation in the democratic process, and it is a trend Congress and social media platforms should seek to ameliorate and every American should categorically reject.

The embrace of disinformation by domestic political groups and its all-but-unchecked proliferation on social media means that foreign adversaries do not need the creativity or brute force they required to fuel their 2016 campaigns; today, they need only sit back and watch, regurgitating and amplifying what is already endemic to our society. Nineteen days before voting closes in the 2020 election, I believe we are far more vulnerable to online disinformation -- from both foreign and domestic sources -- than ever before.

### *Solutions*

We will not repair our information ecosystem before November 3, but Congress should continue to raise awareness among the American people about its ailing health and legislate to improve it. The following are the most urgent changes to pursue:

### Social Media Platforms

1. **Pursue more consistent and equitable enforcement of Terms of Service,** inclusive of public figures and world leaders; if leaving content up due to "newsworthiness," increase on-platform friction including through interstitials and overlays that provide context and facts to users before they interact with misleading or false content. Twitter is the best example of a platform moving in the right direction in this context, but the U.S. political environment would be better served by more transparency and equity around its enforcement of these measures.

[23] U.S. Senate Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 Election, Volume 2: Russia's Use of Social Media with Additional Views," 116th Congress, First Session, Report 116-XX.
[24] Nina Jankowicz, "How Disinformation Became a New Threat to Women," *Coda Story*, December 11, 2017.

2. **Increase transparency and oversight of closed online spaces** such as Facebook groups; limit the size of private and secret groups, mandating that groups above a certain threshold be set to public. Introduce regular human review of groups included in recommendation algorithms to identify potential viral vectors of disinformation.

3. **Make changes to user interfaces that make reporting malign content and harassment more intuitive and more widespread** and include reporting options for election/democracy-related disinformation, health disinformation, and information that may pose an imminent threat to public safety. Inform and educate users on the use of these tools; actively enforce terms of service against users to attempt to brigade or spam these functions.

**Congress**

1. **Mandate increased transparency in online political advertising, and eliminate microtargeting of political ads.** Limit the targeting of online political ads to the district level. Pass the Honest Ads Act, and consider broader regulations that give social media users more context about who is targeting them, through what means, and why.

2. **Organize the federal government to respond to disinformation:** This testimony describes how disinformation is not a threat that only affects traditional national security departments and their purviews. Congress should ensure that a holistic understanding of disinformation is systematized in the operations of the federal government by providing funds to:[25]

    a. **Build capability** across the federal government so that civil servants` are trained on how to recognize and counter disinformation. This would reduce disinformers' attack surface, increase awareness across an important target audience, and ensure the government's disinformation response moves beyond discrete campaigns addressing to a specific disinformation event, and instead works toward a more holistic, proactive posture;[26]

    b. **Improve interagency coordination** to counter disinformation, including by working with the Executive Branch to designate a node within the government responsible for such overarching policy coordination. Fund domestically-oriented programs outside of the traditional national security sphere as part of this counter-disinformation package (see Item 3 below), and hold regular hearings to

[25] Nina Jankowicz and Henry Collis, "Enduring Information Vigilance: Government After COVID-19," *Parameters* 50, no. 3, Autumn 2020.

[26] The UK Government's RESIST Counter Disinformation Toolkit provides a ready-made training curriculum for government communicators and civil servants.

encourage and assess interagency coordination.

c. **Engender international cooperation:** together with the Executive Branch, encourage federal agencies to work with international organizations and their allied counterparts to multiply the impact of U.S. counter-disinformation policy, particularly in regard to foreign disinformation. Congress should also increase cooperation with allied foreign legislatures to coordinate policy responses and present a united front against foreign adversaries as well as in the tech regulation space.

3. **Invest in building a more resilient society:** In addition to the structural changes outlined above, the U.S. government must begin to make generational, citizens-based change that will address the vulnerabilities in our information ecosystem that foreign and domestic disinformers seek to exploit.

   a. **Increase media and digital literacy skills:** Fund a Department of Education program to disburse state grants for media and digital literacy training in elementary and secondary schools, universities, public libraries, and through civil-society implemented mechanisms. Grants would be awarded based on adherence to a strictly non-partisan curriculum compliant with accepted media literacy standards, and would address: critical thinking skills; an understanding of how malign actors manipulate digital platforms; basic comprehension of how social media platforms and algorithms operate; insight into emotional manipulation; cyber hygiene skills; and civic literacy as it relates to the information environment.

   b. **Support a robust public media:** The American news environment is atrophying, a trend that the coronavirus pandemic is exacerbating. Compounding the problem, the largest national outlets are largely viewed along partisan lines, according to a recent Pew study.[27] Local news outlets, trusted by more than 6 in 10 Americans, are being shuttered, replaced by misleading niche sites that serve as vectors for disinformation.[28] With the U.S. investment in public media already embarrassingly low, at about $1.35 per person per year, the Trump administration sought to allocate only $30 million for the Corporation for Public Broadcasting, down from $445 million.[29,30] The importance of public media in rural markets

[27] Mark Jurkowitz, Amy Mitchell et al, "U.S. Media Polarization and the 2020 Election: A Nation Divided," Pew Research Center, January 24, 2020.

[28] John Sands, "Local News is More Trusted than National News, But That Could Change," Knight Foundation, October 29, 2019.

[29] Rachel Abrams, "Unloved by Trump, NPR Carries On," *The New York Times,* February 16, 2020.

[30] CPB Operating Budget, Corporation for Public Broadcasting, accessed 12 October 2020.

cannot be overstated; in many cases the local NPR or PBS station is the only dedicated local media in the area.[31] Congress must invest more in our citizens' access to trustworthy information to inform their participation in democracy.

Underlying all of these recommendations must be the most basic of recognitions, without which we cannot hope to make any progress repairing our information ecosystem: any government that claims to fight disinformation originating outside its borders cannot do so while it embraces the same methods within them. Disinformation is a threat to democracy, no matter what political party it benefits or whether it is foreign or domestic in its source, and it is long past due that the United States began to address this challenge to the very foundation of our country and its values.

[31] See, for instance: CPB's explainer "Public Media Journalism," or the NPR public editor's "Working Together to Alleviate News Deserts."