March 2020 | No. 4

Safeguarding Digital Democracy

Digital Innovation and Democracy Initiative Roadmap

Karen Kornbluh and Ellen P. Goodman

with contributions by Eli Weiner

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington, DC Ankara Belgrade Berlin Brussels Bucharest Paris Warsaw

March 2020 | No. 4

Table of Contents

3 Executive summary

8 Introduction

10 Politically motivated disinformation campaigns

27 After tech utopianism

30 Policy roadmap for safeguarding digital democracy

The Digital Innovation and Democracy Initiative

The Digital Innovation and Democracy Initiative works to foster innovation and ensure that technology strengthens democracy. DIDI leverages GMF's transatlantic network and network of senior fellows to promote strategies for reforming policies for the digital age.

Authors

Karen Kornbluh, former U.S. Ambassador to the Organization for Economic Cooperation and Development, is Senior Fellow and Director of the Digital Innovation and Democracy Initiative at the German Marshall Fund of the United States.

Ellen P. Goodman is a professor at Rutgers Law School, where she is co-director and co-founder of the Rutgers Institute for Information Policy & Law at Rutgers Law School, and Non-Resident Senior Fellow at the German Marshall Fund.

Eli Weiner is a research assistant with the Digital Innovation and Democracy Initiative at the German Marshall Fund of the United States.

Even before a global pandemic hit, the Bulletin of Atomic Scientists announced that the Doomsday Clock had advanced for the first time ever to 100 seconds before midnight. The Bulletin cited “information warfare” as a “threat multiplier” that is reducing trust and corrupting the information ecosystem needed for democratic debate. Now the World Health Organization is warning of an “infodemic” of widespread conspiracy theories about the coronavirus, and disinformation has already been evident in the lead-up to the 2020 presidential election. Despite a clear and present danger, it is evident that our institutions are not nearly ready—neither for foreign nor domestic disinformation campaigns.

While U.S. intelligence officials have repeatedly warned lawmakers that foreign interference in U.S. elections will continue, the giant platforms that have become the new media gatekeepers—Facebook/Instagram, Twitter, and Google/YouTube—have largely been left to choose their own paths. And though the platforms say

The United States is Woefully Unprepared for Disinformation Wars

Digital Astro-Turf

Secret groups that simulate grassroots support are being increasingly weaponized to spread conspiracy theories and undermine trust in institutions

> **And yet, despite Facebook policies, users are able to spread false origin stories about the coronavirus and promote “remedies” that the FDA has said are “the same as drinking bleach”**

Personalized Propaganda

In the 2020 elections, over $1.6 billion is likely to be spent on micro-targeted ads—three times more than in 2016

> **And yet, platforms’ ad databases crashed days before elections in the United Kingdom, and still do not reveal donors**

Flooding the Zone

Not just ads or Russian trolls, but armies of domestic warriors are flooding the news cycle with fakes, memes, and rumors

> **And yet, Facebook and Google do not require paid “organizers” to disclose sponsorship**

Platform Moderation Black Box

Secret, inconsistent algorithmic recommendations and moderation decisions create loopholes for cross-platform disinformation campaigns

> **And yet, platforms are not required to provide traffic information on the 2020 elections, as they were compelled to do after 2016**

Trojan Horse Outlets

Partisan and conspiracy sites, sometimes pretending to be local news, and engagement with outlets that repeatedly share false information are on the rise

> **And yet, the platforms do not tell users that “news” stories from partisan and satire sites—like those spreading rumors that Greta Thunberg is George Soros’s niece—aren’t factual or fact checked**

they want to address election disinformation, their own rules are inconsistently applied and underenforced, leaving it to fact-checkers, journalists, and researchers to expose rule breaking as best they can. According to our research with NewsGuard, among outlets that repeatedly share false content, eight of the top 10 most engaged-with sites are running coronavirus stories.

> ***Eight out of the top ten sites promoting false information were found to be running disinformation about coronavirus, with headlines such as "STUDY: 26 Chinese Herbs Have a 'High Probability' of Preventing Coronavirus Infection" and "Why coronavirus is a punishment from God"***[1]

Individual platforms allow disinformation campaigns to leverage "dark patterns," or manipulative user interfaces, to deceive users. This opaque design makes it easy to like and share a planted story, but hard to verify a faked video.[2] Disinformation campaigns thereby overwhelm the "signal" of actual news with "noise," eroding the trust in news necessary for democracy to work. The tools of disinformation campaigners include:

- **Trojan horse outlets that deceive users about the source of disinformation** by disguising themselves as independent journalism while eschewing its practices (for example, bylines, mastheads, verification, corrections, community service principles) and leveraging platform design to boost conspiracies. Meanwhile, real news generation atrophies because platforms have absorbed the revenue of local independent journalism.

- **Spending on personalized political propaganda—which is likely to top $1 billion in 2020, three times such spending in 2016—obscures the true sponsors of online ads from the public.**[3] The platforms each have different and weak procedures for labeling and how much targeting they allow for political ads. Both Google and Facebook's ad libraries malfunctioned, failing to provide real disclosure in the days before the last U.K. election.

- **Networks of "amplifiers" flood the zone with disinformation. Fake accounts, influencers, and true believers** game algorithmic recommendations to fill trending lists and search engines with visual memes or video.

[1] Ratings were provided by NewsGuard, which employs a team of journalists and editors to review and rate news and information websites based on nine journalistic criteria assessing basic practices of credibility and transparency. In this instance, outlets failed the criterion "does not repeatedly publish false content." Public interactions were measured by media intelligence company Newswhip on Facebook and Twitter. Articles quoted ran on returntonow.net on March 12, 2020 and lifesitenews.com on March 13, 2020, respectively.

[2] "Dark pattern" design, like the boxes asking users to accept cookies with no alternative option other than "learn more," obscures information users need (that they can refuse to share data) and defaults to actions (agreeing to share data) not in the users' or the ecosystem's interest.

[3] Kate Gibson, "Spending on U.S. digital political ads to top $1 billion for first time," CBS News, February 12, 2020.

- **Digital Astro-turf** campaigns that look like organic grassroots movements use **secret groups, encrypted messaging, and fringe sites linking to the main platforms** to target vulnerable populations through disinformation and harassment.

- **Platform black box moderation that applies rules inconsistently and without transparency,** create loopholes for cross-platform disinformation operations. The self-regulatory model of negotiations with civil society appears broken; civil rights groups working on an audit have protested the platforms' lack of cooperation.

Too often, the only alternative proposed to today's laissez-faire approach would increase government control over content. This false choice—between allowing platforms or government to act as censor—has hobbled the policy debate. A new approach should empower users. Our approach is rooted in an understanding that digital information platforms are our new media gatekeepers yet have none of the obligations developed over time for our old gatekeepers: obligations to minimize user manipulation, boost public interest journalism, and promote democratic debate.

The new digital media policy roadmap we layout would steer clear of vague rules that empower governments to define "good" or "bad" content and would instead focus on updating offline protections, fostering user choice, amplifying the signal of independent news, supporting civic information, and holding platforms accountable for shared, unambiguous, and transparent rules. This policy package—tailored with input from stakeholders and sufficiently agile to account for evolving technology—would close the loopholes that allow bad actors to engage in online information warfare using the largest platforms, and it would do so without restricting free expression or stymieing innovation.

Policy Roadmap for Safeguarding the Information Ecosystem

Dampening the Noise: Update Offline Consumer, Civil Rights, Privacy, Elections, and National Security Protections

- *Design with "light patterns."* Instead of today's dark patterns manipulating users through tricky user interface, user interface defaults that favor transparency (through better labeling) and dialogue would improve the information ecosystem and protect users' freedom of mind. It should be easy to distinguish transparent and ethical journalistic practices from trolling content and to tell if video has been altered. Users should be able to customize algorithmic recommendations and easily track content complaints. Design solutions that avoid virality and instead introduce friction should make it harder to spread hate and easier to engage constructively online.

- *Restore the campaign finance bargain.* The Honest Ads Act (which would impose broadcast disclosure rules on platform ads) has bipartisan support and should set the floor on disclosure. In addition, platforms should verify who is actually funding ads rather than listing front groups, and platform fact-checking policies should be consistent and applied to politicians. As recommended by a Federal Election Commission commissioner, platforms should also limit microtargeting of political ads. A new Gallup poll funded by the Knight Foundation found that 72 percent of Americans prefer not be targeted at all, and another 20 percent are only comfortable with such ads using limited, broad information such as a person's gender, age, or ZIP code.[4]

- *Update civil and human rights law, including privacy protections.* Discrimination, harassment, and privacy laws—including public accommodation laws—should be updated for the digital age. Platforms should create and enforce rules for content removal and algorithmic prioritization that are consistent, transparent, and appealable.

- *Stipulate National Security Information Sharing.* Platforms should share information with each other and with government agencies on violent extremism as well as with the public on foreign election interference.

Boosting the Signal: Promote Local News, Public Infrastructure, and Choice of Curation

Platforms have syphoned away ad revenue that once supported public interest local journalism. A fund to support noncommercial public interest journalism, fact-checkers, and media literacy could be created by taxing platform ad revenue—raising the cost of relying on data collection and the viral spread of disinformation while also supporting more signal in the system. A commitment by platforms to highlight and boost this content would also loosen algorithmic control over information flows. Just as support for public media in the past extended to communications infrastructure, so too in the digital space must there be noncommercial information infrastructure as an alternative.

Creating Accountability: Make an Enforceable Code of Conduct

- *Data must be sharable between platforms.* Democracies traditionally prevent bottlenecks on the flow of information to ensure that neither private nor public actors have power over speech. Interoperability and portability of data (IP- and privacy-protected) can help users switch to new platforms with distinct business models and information profiles, as well as use alternative curation strategies on top of existing platforms.

- *Open the data black box.* Platforms should provide (IP- and privacy-protected) after-action disclosure of how content is algorithmically curated, what targeting policies are used, moderation decision logs, and traffic for civil society watchdogs, researchers, and government to help assess information flows.

- *Platforms should develop with civil society a technology-neutral industry/civil society code of conduct focused on practices, not content.* Monitoring would be possible with independent data sharing by neutral third parties and oversight provided by a new Digital Democracy Board or an existing agency that has been given such authority. Section 230 immunity could be conditioned on code compliance.

[4] Justin McCarthy, "In U.S., Most Oppose Microtargeting in Online Political Ads," Gallup Blog, March 2, 2020.

The Answer is Not Top-Down Government Control

Policy Roadmap for Safeguarding Digital Democracy

Dampening the Noise

Update offline consumer, elections, civil rights, privacy, and national security protections

"Light Patterns" (intuitive user design for greater transparency and helpful frictions): Provide defaults that, rather than obscuring the source of a news item, notify whether a video or audio has been altered, and if an account is verified. Allow customization of algorithmic recommendations.

Elections: In addition to the bipartisan Honest Ads Act (which imposes broadcast disclosure rules on platform ads), verify who is actually funding ads and uphold consistent fact-checking policies. Limit micro-targeting of political ads.

Civil and Human Rights and Protections: Discrimination, harassment, and privacy laws should be updated for the digital age. Platforms' rules and enforcement should be consistent, transparent, and appealable.

National Security: Platforms should share information with each other and with government agencies on violent extremism as well as with the public on foreign election interference.

Boosting the Signal

Promote independent news, public infrastructure, and choice of curation

Tax Platform Ad Revenue: Restore some of the funds diverted from journalism while raising the cost on a business model that relies on data collection and the viral spread of disinformation.

PBS of the Internet: Create an independent support mechanism for noncommercial public-interest journalism, fact-checkers, voting information, and media literacy. Create a public architecture to highlight and boost this content, loosening algorithmic control over information flows.

Independent Accountability

Create accountable codes of cunduct through data sharing/monitoring, civil and regulatory enforcement

Interoperability and Portability: Help users move to new platforms with alternative business models and information profiles, as well as use alternative curation strategies on top of existing platforms.

Open the Black Box: Provide (IP and privacy-protected) after-action disclosure of how content is algorithmically curated, what targeting policies are used, moderation decision logs, and traffic to civil society watchdogs, researchers, and government to help assess information flows.

Update the "Light Touch" Regulatory Model: Develop a technology-neutral industry/civil society code of conduct focused on practices, not content. A new Digital Democracy Board or existing agency should require monitoring and hold platforms accountable for compliance. Section 230 immunity could be conditioned on complying with the privately developed code of conduct and/or could be narrowed to exclude advertisements.

INTRODUCTION

The Internet in its early days seemed to herald a new era, with fuller participation in democratic discourse, decentralized power, and runaway innovation. Reflecting the tech utopia of the period, policies exempted Internet companies from liability. Instead of updating offline laws for the online environment, policymakers endorsed a new self-regulation model in which companies negotiated with civil society. For some years, this worked well. The Internet produced enormous societal benefits, lowering barriers to sharing content with broader audiences and accessing a vast array of information. It created new communities across geographies, enabled untold innovation, and disintermediated gatekeepers from travel agents to bank tellers to television producers.

But as the Internet's role in society grew, this model of governance became ineffective. Almost as many people now get their news from the Internet as from television. Americans now spend an average of 24 hours a week online, and 40 percent of them believe the Internet plays an integral role in U.S. politics.[5] Today's giant ad-supported digital platforms, especially Facebook, Twitter, and YouTube, now dominate the advertising market that once paid for newspapers and have displaced local papers as news providers.

Having disintermediated journalism, the digital platforms replaced editorial decisions with engagement-optimizing algorithms that prioritize enticing content—even if from a source peddling clickbait or political outrage, or promoted by bots, trolls, or sock puppets (agents using false identities). News stories delivered online lack the signals legacy newspapers provided to help a reader evaluate their reliability (for instance, separating editorial content from ads, and labeling the source of news and pictures). On digital platforms, verifiable facts and made-up nonsense walk side by side with equal stature. A story spreading the false identity of a mass shooter, for example, may start on a hyper-partisan site, be shared by organized amplifiers, eventually get tweeted by an influencer, and further ricochet around social media until becoming a trending news item picked up by mainstream media.

As a result, these platforms became hosts for third-party, politically motivated influence campaigns. Platform tools are exploited by disinformation actors to manipulate users by testing and targeting ads, hiding the source of content, and drowning out news from independent journalism. Racism, misogyny, anti-immigrant sentiment, and Islamophobia are features of many of these campaigns, which appeal to tribal loyalties and reinforce negative super-narratives about the dangers posed by certain groups.

The resulting corruption of the information ecosystem is not a victimless crime. It threatens the underpinnings of democracy in critical ways. The ability to self-govern depends on citizens having access to reliable information, as well as the ability to exchange and contest ideas without violence. In addition, democracy

[5] Jeffrey I. Cole et al., "Surveying the Digital Future: The 15th annual study on the impact of digital technology on Americans," Center for the Digital Future at USC Annenberg, 2017.

depends on the formation of changing coalitions of different groups. But when citizens are driven into fixed tribes convinced that the "other" poses an existential threat, they are unable to participate in democratic negotiations. Key institutions and processes of democracy—from the independent press to the judiciary and rule of law, from civil rights to free and fair elections—are threatened. Sovereignty and national security are also at risk when foreign states and non-state actors are able to influence and undermine elections and democratic institutions easily and cheaply.[6]

The largest digital information platforms have implemented new policies and created new internal functions to combat foreign interference, disinformation, coordination, and manipulated video since the 2016 U.S. presidential election. They are working with fact-checkers and have increased transparency for political advertisements. But the rules and procedures differ within and among platforms, creating loopholes for cross-platform disinformation campaigns. And there has been little to no government response despite the platforms' requests for a regulatory framework. The bipartisan Honest Ads Act, introduced originally in 2017 by Senators Mark Warner, Amy Klobuchar, and John McCain, has yet to receive a hearing in either house of Congress. As disinformation campaigns become increasingly homegrown and sophisticated, the platforms' policies will leave the ecosystem more vulnerable. We need mechanisms to address the societal impact of the platforms, just as we have for other socially significant industries and professions—from drugs and airlines to doctors and chemicals. These include responsibilities to disclose information, to demonstrate the safety of their products, to mitigate harm, and to comply with their own promises. Drug and airline companies disclose things like ingredients, testing results, and flight data when there is an accident; platforms do not disclose, for example, the data they collect, the testing they do, how their algorithms order newsfeeds and recommendations, political ad information, or moderation rules and actions.

U.S. policymakers are right to be averse to granting the government discretion over content or in other ways limiting the expression, commerce, and creativity the Internet enables. Solutions like those documented by Freedom House in "at least 17 countries [that] approved or proposed laws that would restrict online media in the name of fighting 'fake news' and online manipulation" turn governments into arbiters of acceptable speech. The risks of government censorship are obvious. In Saudi Arabia, cracking down on fake news has become a prime justification for shutting down dissident speech.[7] That is not what we are calling for here.

As we argued back in the summer of 2019, what is needed most are structural design fixes, not discrete content moderation decisions.[8] The choice is not between a "truth police" or total abdication of a democracy's responsibility to protect the integrity of its information ecosystem. Commonsense policy actions would go a long way to secure access to reliable information and disrupt the disinformation arms race without compromising free expression. Platforms can reduce the opportunities for manipulation across the board, without wading into politics, through more transparent and consistent practices, rather than attempting to root it out on a case-by-case basis. Most importantly, platforms must have incentives to reduce the harm of disinformation noise and other dysfunctions instead of externalizing those costs onto society.

[6] Suzanne Spaulding, Devi Nair, and Arthur Nelson, "Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System," Center for Strategic and International Studies, May 1, 2019.

[7] Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism," Freedom House, 2018.

[8] Karen Kornbluh and Ellen P. Goodman, "Bringing Truth to the Internet," *Democracy: A Journal of Ideas* 53, Summer 2019.

POLITICALLY MOTIVATED DISINFORMATION CAMPAIGNS

In November 2019 the U.S. Departments of Justice, Defense, and Homeland Security, the Director of National Intelligence, the Federal Bureau of Investigation, the National Security Agency, and the Cybersecurity and Infrastructure Security Agency released a joint statement warning that "Russia, China, Iran, and other foreign malicious actors all will seek to interfere in the voting process or influence voter perceptions."[9] The cybersecurity company FireEye reported in May 2019 that a social media campaign possibly "organized in support of Iranian political interests" included Twitter accounts impersonating Republican candidates for the House of Representatives in 2018.[10]

Such threats emanate not only from states, nor only from abroad. Commercial, non-state actors have joined in, along with domestic actors. A private Ukrainian network of sites built a massive U.S. audience using ads and cross-posting to drive users to sites featuring patriotic, religious, pro-military, and cute animal memes. Its pages joined political Facebook groups and were active on Facebook-owned Instagram. Eventually the network began funneling large audiences to political stories. Shortly before they were taken down, one of the sites, "I Love America," had had more Facebook engagement—likes, shares, and comments—over 90 days than *USA Today*, one of the largest media organizations in the country with 8 million Facebook followers.[11]

As the Senate Intelligence Committee's second report on the 2016 election lays out, politically motivated disinformation campaigns work across information platforms, laundering false news stories through online hyper-partisan outlets or YouTube channels, microtargeted to vulnerable users.[12] Stories or memes are amplified to flood the news zone via networks of users, influencers, trending lists, hashtags, recommendation engines, and search manipulation. Astro-turf campaigns, or covertly sponsored messaging masked as social movements, attract adherents and—the ultimate jackpot—win coverage by mainstream journalists.[13] All along the way, platform data-collection and -targeting capacities are leveraged to gain asymmetric knowledge of user vulnerabilities. The financial rewards can also be substantial, with nearly a quarter of a billion dollars in advertising run against disinformation sites.[14]

[9] Federal Bureau of Investigation, Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, and CISA on Ensuring Security of 2020 Elections, November 5, 2019.

[10] Alice Revelli and Lee Foster, "Network of Social Media Accounts Impersonates U.S. Political Candidates, Leverages U.S. and Israeli Media in Support of Iranian Interests," FireEye, May 28, 2019.

[11] Popular Information, "Massive 'I Love America' Facebook page, pushing pro-Trump propaganda, is run by Ukrainians," September 23, 2019.

[12] U.S. Senate Select Committee on Intelligence, Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views, October 8, 2019.

[13] The Oxford Internet Institute reports that "political campaigns are likely to adopt strategies which blend both paid and organic, or non-ad, material to maximize reach while minimizing spend." Stacie Hoffmann, Emily Taylor, and Samantha Bradshaw, "The Market of Disinformation," Oxford Technology & Elections Commission, October 2019.

[14] Global Disinformation Index, "The Quarter Billion Dollar Question: How is Disinformation Gaming Ad Tech?" September, 2019, 4.

A disinformation warrior can create alternate epistemic realities, or senses of what is true, by exploiting psychological vulnerabilities. Repetition increases participants' perceptions of the truthfulness of false statements even when they know such statements are false, a phenomenon known as the illusory-truth effect.[15] In multiple experiments with thousands of participants, researchers have found that the more people are exposed to false information, the more likely they are to share it online.[16] A recent report exposed that even trained Facebook contractors hired to moderate content began, after repeated exposure, to believe conspiracies denying the Holocaust and insisting the Earth is flat.[17]

Social media is of course only a part of the information environment; for political debate in 2016, traditional media outlets were still more important.[18] However, bad actors online help corrupt the overall information ecosystem, sowing confusion and distrust, and undermining other sources of news, such as independent local journalism. Furthermore, disinformation stories that germinate online often make their way into traditional media. Thus, it is worth focusing on social media and the largest information platforms as they become primary news sources.

A few large information platforms—Facebook/Instagram, Google/YouTube, and Twitter—are the new media gatekeepers. They have exposed vulnerabilities that bad actors exploit, including:

- Trojan horse outlets, which conceal their agenda and sponsors to impersonate news outlets while applying none of the responsible practices of independent news;
- microtargeted ads that leverage dark money and user data;
- amplification, via algorithmic recommendations and search functionality manipulated by networks of bots, click farms, fake accounts, coordinated true believers, and influencers;
- secret, private groups and fringe sites with frictionless access to mainstream platforms; and
- inconsistently applied moderation rules that inevitably favor those with the most power.

[15] The phenomenon was identified by a team of psychologists led by Lynn Hasher in 1977; see Whitney Phillips, "The Toxins We Carry," *Columbia Journalism Review*, Fall 2019.

[16] James Hohmann, "New research helps explain how Trump successfully muddied the water on Ukraine and impeachment," *Washington Post,* December 4, 2019.

[17] Casey Newton, "The Trauma Floor," The Verge, February 25, 2019.

[18] As Yochai Benkler et al. have demonstrated, the importance of traditional media in the information ecosystem was more significant than social media. They also demonstrate that disinformation is so far an asymmetrical ideological game. While traditional and left-wing media still largely conform to general journalistic norms including rules of independence and facts, what Benkler et al. describe as "right wing media" conform to narratives circulated within this conservative ecosystem. Yochai Benkler, Robert Faris, and Hal Roberts, Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics, Oxford: Oxford University Press, 2018.

Trojan-Horse Outlets Thrive While Newspapers Shutter

Digital platforms have undermined the news revenue model. Advertising once padding the fat Sunday editions of newspapers has moved online, with Google and Facebook now capturing 58 percent of the market, followed by Amazon, Microsoft, and Verizon.[19] Almost as many people now get their news from the Internet as from television.[20] Platforms distribute news but do not share revenue, and news outlets have even had to pay to reach users.

McClatchy—one of the nation's leading newspaper companies with 30 newspapers—recently filed for bankruptcy, following a long line of august predecessors.[21] Since 2004 more than 1,800 local print outlets have closed, and at least 200 counties have no newspaper at all, becoming news deserts.[22] Areas with limited local news have less politically aware populations; indeed, "voting and consuming news—those things go hand in hand," noted Tom Huang, assistant managing editor of *The Dallas Morning News.*[23] One study found that the city of Denver experienced a decrease in civic engagement after the closure of *The Rocky Mountain News* and the shrinking of the *Denver Post*.[24] Just as important, newspaper layoffs and closings have hamstrung the ability to hold public and corporate officials accountable. Kevin Flynn, a former journalist turned Denver City Council member, observed a lack of awareness of local elections and a sense that "[i]t feels like we could all be getting away with murder right now."[25]

In addition, the ways in which platforms distribute news undermine news comprehension and trust. Online content is separated from the outlet that produces it, so that the reader cannot easily distinguish between evidence-based news and fabrications. Users have few signals about the integrity of an online site posing as a news source. The "user interface" of traditional media provided context to judge a newspaper's credibility, including the location of the paper in the newsstand, separate sections for news and opinion, a masthead, and bylines and datelines, all signaling industry-wide sourcing standards. To say that there is a craft of journalism is not to say that the craft was ever perfect or free from problems of exclusion, narrow framing, or corruption. When digital platforms disintermediate newspapers, however, they decontextualize stories and strip them of credibility signals. This context collapse confers undeserved credibility on trojan horse outlets, sites that appear to be news outlets but instead promote disinformation for political or financial ends.[26] In doing so, they further undermine signals of transparency and standards from traditional journalism.

Data released on Russian disinformation activity from 2014 to 2018 shows how bad actors weaponize the information space.[27] What the researchers term "narrative laundering" occurs when "a story is planted or created and then legitimized through repetition or a citation chain across other media entities." They explain

[19] Todd Spangler, "Amazon on Track to Be No. 3 In U.S. Digital Ad Revenue, but Still Way Behind Google, Facebook," *Variety*, September 9, 2018.

[20] A.W. Geiger, "Key findings about the online news landscape in America," Pew Research Center, September 11, 2019.

[21] PEN America, "Losing the News: The Decimation of Local Journalism and the Search for Solutions," November 20, 2019, 27.

[22] PEN America, "Losing the News: The Decimation of Local Journalism and the Search for Solutions," November 20, 2019, 27.

[23] PEN America, "Losing the News," 14.

[24] Ibid.

[25] Julie Bosman, "How the Collapse of Local News Is Causing a 'National Crisis,'" *New York Times*, November 20, 2019.

[26] McKay Coppins, "The Billion-Dollar Disinformation Campaign to Reelect the President," *The Atlantic*, March 2020;

[27] Renee DiResta and Shelby Grossman, "Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-19," Stanford Internet Observatory, November 12, 2019.

Weaponizing Satire Against Greta Thunberg

GMF worked with Media Ecosystems Analysis Group to track the cross-platform, global promotion of conspiracy theories about climate change activist Greta Thunberg. We found that satire websites and satire-oriented social media accounts played a role in the construction and circulation of conspiracy theory-oriented content.

- A French satire website article depicted Thunberg as the granddaughter of left-wing billionaire George Soros, including a photoshopped image of the two together. This was then shared widely on Facebook (14,503 shares) and became central to a conspiracy theory linking Thunberg and Soros.

- An article by the satire website Babylon Bee describing Thunberg as a puppet of powerful actors was shared 18,783 times, quickly leaving the satirical realm.

- Two additional social media posts, one on Facebook and one on Twitter, which seem to have been originally posted by individuals genuinely ironically (one photoshopping Thunberg with two adults wearing Antifa shirts, incorrectly identified as her parents), then shared and distributed without context, contributed to the disinformation narrative that Thunberg is a radical left-wing actor.

Platforms do not fact-check articles from outlets that claim to be satirical (for good reason), even though the article itself may not disclose that it is satirical and the satire may not be clear to the user. Increasing numbers of disinformation sites are using satire disclaimers as a shield to avoid being banned or demoted, but do not include such disclaimers on individual articles that circulate online.

** See forthcoming paper by Aashka Dave, Fernando Bermejo, and Laura Schwartz-Henderson for the German Marshall Fund of the United States and Media Cloud.*

*** Jeff Horwitz, "Facebook to Exempt Opinion and Satire From Fact-Checking," Wall Street Journal, September 30, 2019.*

how Russia's military intelligence agency (GRU) used "alternative news" sites to serve as initial content drops, from which the content was syndicated or republished on other sites.

The largest digital platforms have taken steps to reduce the most obvious false news and clickbait content. However, journalists and researchers continue to uncover evidence of widespread engagement with their articles:

- A 2019 study found that the 100 top stories debunked by fact-checking organizations reached over 158 million estimated views.[28]

- The *Guardian* found 21 of the largest far-right pages—including one linked to a right-wing terror group—broadcast over 1,000 fake news posts a week to 1 million followers, containing headlines that when clicked

[28] Avaaz, "U.S. 2020: Another Facebook Disinformation Election?," November 5, 2019.

sent viewers to websites operated from Israel. After being notified by the newspaper, Facebook removed some of the pages and accounts.[29]

- The Beauty of Life, linked to the Epoch Media Group, operated hundreds of coordinated fake accounts that shared pro-Trump messages at high frequencies and directed users to off-Facebook sites also owned by them, until identified and removed by Facebook in violation of the platform's policy against coordinated, inauthentic behavior.[30]

Researchers found a reduction in the percentage of the most popular articles on Facebook from outlets that frequently publish unreliable information. [31] However, hyper-partisan trojan horse outlets that mix fact with opinion, straight conspiracy theory, or even satire have large audiences yet evade the new rules by claiming not to be news.[32] In addition, we analyzed outlets rated by NewsGuard as repeatedly sharing false content and found that, among the top ten of these outlets by interactions, overall interactions have continued to increase in absolute terms from 2016.[33] The composition of the top ten sites in this category has shifted thematically, however; although RT and Sputnik have remained in the top five, Infowars and Gateway Pundit have dropped in relative engagement, while a number of alternative health, religious, and anti-abortion sites have risen to the top.

Currently, disinformation warriors are especially active on the political right.[34] But this asymmetry may not continue, and it is very possible that we are heading for a race to the bottom of inflammatory garbage. Tides of disinformation are now coming in faster than researchers can document them. Here are only a few:

- The Daily Wire—a partisan site promoting stories deemed false by independent fact-checks—last year garnered more engagement for its content than any other significant publisher through the use of coordinated promotion operations.[35]

- TheSoul Publishing, run by Russian nationals and headquartered in Cyprus, distributes content to a network of YouTube accounts and was one of the largest web publishing companies, outranked only by Disney and Warner Media in views and subscribers on YouTube as of November 2019. It had over 44 million followers across its different Facebook pages.[36]

[29] Christopher Knaus et al., "Inside the hate factory: how Facebook fuels far-right profit," *Guardian*, December 5, 2019.

[30] Ben Nimmo et al., "#OperationFFS: Fake Face Swarm," Graphika and the Atlantic Council, December 20, 2019; Alex Kasparak and Jordan Liles, "If Facebook Is Dealing with Deceptive 'BL' Network, It's Not Working," Snopes, December 13, 2019.

[31] Laurel Thomas and Jessica Webster, "U-M's Iffy Quotient shows steady drop of questionable information on social media, partners with NewsGuard for better data," University of Michigan, July 23, 2019.

[32] Will Oremus, "Facebook May Face Another Fake News Crisis in 2020," OneZero, December 3, 2019.

[33] Ratings were provided by NewsGuard, which employs a team of journalists and editors to review and rate news and information websites based on nine journalistic criteria assessing basic practices of credibility and transparency. In this instance, outlets failed the criteria "does not repeatedly publish false content." Public interactions were measured by media intelligence company Newswhip on Facebook and Twitter.

[34] Zain Humayun, "Researchers have already tested YouTube's algorithms for political bias," Arstechnica, February 15, 2020.

[35] Popular Information, "Keeping it 'real'," October 30, 2019.

[36] Once exposed by Lawfare, the site removed the flagged material and pledged to stop producing historical content. See TheSoul Publishing, "A message from TheSoul Publishing," December 25, 2019; Lisa Kaplan, "The Biggest Social Media Operation You've Never Heard of Is Run Out of Cyprus by Russians," Lawfare, December 18, 2019.

- One study has found at least 450 partisan Trojan horse outlets masquerading as local news and serving up algorithmically generated partisan articles alongside a smattering of original content.[37] Facebook disabled groups and pages created by a digital marketing firm in India to direct users to non-Facebook websites imitating news outlets. They also found a Persian Gulf network, linked to two marketing firms in Egypt, that managed pages claiming to be local news organizations.[38]

Disinformation outlets masquerading as news media pose a significant threat to robust democratic debate, yet it remains difficult for both platforms and policy to distinguish them from real news. Platforms efforts, including using fact-checkers to identify disinformation and AI techniques to assess both coordination and lack of original reporting, are rather opaque and appear reactive and inconsistent.

Personalized Persuasion Fueled by Data and Dark Money

Disinformation campaigns advertise to small audiences, enticing them to share memes, take quizzes, donate money, follow "news" sites and fictitious accounts, and join groups. Such ads are targeted to audiences based on data gathered about them and people like them. For example, in one effort, women over the age of 25 who had expressed interest in pregnancy were served a targeted ad featuring anti-vaccination conspiracies.[39] In another case, ads disseminating misleading information about HIV preventive medicines, seemingly targeting men and women over the age of 30, generated millions of views; LGBT activists and organizations say that the ads resulted in many people most at risk of HIV exposure forgoing medication.[40] After the initial *Washington Post* story reporting on the issue, Facebook began removing the ads.[41]

Although Facebook now "prohibits ads that include claims debunked by third-party fact-checkers or, in certain circumstances, claims debunked by organizations with particular expertise," it decided to exempt ads from political candidates from fact-checking requirements on the grounds that it was important to allow the ads to be subject to public scrutiny.[42] However, as hundreds of Facebook employees warned in an open letter voicing their objection to the policy, "it's hard for people in the electorate to participate in the 'public scrutiny' that we're saying comes along with political speech" because these ads are only shown to small groups. [43] Google's ad policies prohibit misleading content, and the company has announced that it will only restrict misinformation in political ads that "could significantly undermine participation or trust in an electoral or democratic process," suggesting that "misleading content" will be defined narrowly to exclude misinformation about specific candidates or policies.[44] The discrepancy among platform rules provides cross-platform information operations arbitrage opportunities. We saw this when Judicial Watch made a false claim about

[37] Priyanjana Bengani, "Hundreds of 'pink slime' local news outlets are distributing algorithmic stories and conservative talking points," *Columbia Journalism Review*, December 18, 2019.

[38] Facebook, "February 2020 Coordinated Inauthentic Behavior Report," March 2, 2020.

[39] Meira Gebel, "Anti-vaccination ads on Facebook are targeting pregnant women, while a measles outbreak spreads across the country," Business Insider, February 14, 2019.

[40] Tony Romm, "Facebook ads push misinformation about HIV prevention drugs, LGBT activists say, 'harming public health,'" *Washington Post*, December 9, 2019.

[41] Tony Romm, "Facebook disables some misleading ads on HIV prevention drugs, responding to growing outcry," *Washington Post*, December 30, 2019.

[42] Facebook, Advertising Policies: Misinformation, accessed February 11, 2020.

[43] "Read the Letter Facebook Employees Sent to Mark Zuckerberg About Political Ads," *New York Times*, October 28, 2019.

[44] Scott Spencer, "An update on our political ads policy," Google, November 20, 2019.

voter fraud in Iowa during the 2020 Iowa Caucus. It was refuted by the Iowa secretary of state and debunked on Facebook, but not on Twitter.

Even if ads do not contain falsehoods, the lack of a shared information space still undermines public debate. Facebook employees warned that "these ads are often so microtargeted that the conversations on our platforms are much more siloed than on other platforms."[45] Information regulators in the United Kingdom and Spain as well as members of U.S. Congress have similarly urged that platforms pause in the distribution of campaign ads. Twitter CEO Jack Dorsey has announced that the company will no longer sell political ads that reference elections, candidates, parties, legislation and regulations, elected or appointed officials, or judicial decisions.[46] Google has restricted microtargeting in political ads. A recent survey by the Knight Foundation and Gallup found that more than 70 percent of Americans oppose the use of personal data for microtargeting purposes by political campaigns.[47]

In addition to issues with fact-checking and microtargeting, current real-time ad labelling, and public libraries after-action reports provide inconsistent and inadequate information to potential voters, depriving them of the ability to know who is sponsoring ads. In the absence of industry-wide standards, as would have been required by the Honest Ads Act, to mirror broadcast rules, platform practices differ from each other in terms of what kinds of ads they deem political. In addition, the data in the political-ad libraries or databases is not robust. One study argues that three systemic issues plague the platforms' ad databases as they are presently constituted: the inability to identify what constitutes political content; the failure to verify advertisement data, from the buyers' identity to engagement metrics; and the refusal to provide targeting information that might inform users and researchers about the specific targeting matrices used in a particular ad.[48] It is apparently easy to use a false identity when buying advertisements and Mozilla researchers found bugs and technical issues in the ad library.[49] Google's database functions better but does not include ads about topics, only candidates.[50] The *Guardian* recently reported that Google's political ad-spending transparency reports, issued weekly, underreported spending by the Labour Party in U.K. elections by a factor of a thousand, while simultaneously underreporting the amount spent by the Conservatives. Snapchat initially reported that the Conservative Party had spent money defending Johnson's Uxbridge seat when in fact it had spent money everywhere but there.[51]

Even when the information in the databases is updated and correct, it still fails to reveal the interested party behind the ads. One study found a set of ads shown in 2016 to a group of North Carolina users pretending to be travel videos enticing Muslim tourists to Paris, Berlin, and Los Angeles by boasting that Sharia Law now governed there—and that these were funded by a group called Secure America Now, which is a charity and so can keep its funders secret. It was only through a mistake by the group's accountants that OpenSe-

[45] "Read the Letter."

[46] Twitter, Political Content Policy, accessed December 18, 2019.

[47] Dannagal G. Young and Shannon C. McGregor, "Mass propaganda used to be difficult, but Facebook made it easy," *Washington Post*, February 14, 2020.

[48] Paddy Leerssen et al., "Platform ad archives: promises and pitfalls," *Internet Policy Review* 8 (4), 2019.

[49] Jonathan Albright, "Facebook and the 2018 Midterms," Medium, November 4, 2018; "Facebook's Ad Archive API is Inadequate," Mozilla Blog, April 29, 2019.

[50] Matthew Rosenberg, "Ad Tool Facebook Built to Fight Disinformation Doesn't Work as Advertised," *New York Times*, July 25, 2019; Taylor Hatmaker, "Google releases a searchable database of U.S. political ads," TechCrunch, August 15, 2018.

[51] Alex Hern and Niamh McIntyre, "Google admits major underreporting of election ad spend," *Guardian*, November 19, 2019.

crets was able to identify that influential right-wing billionaire Robert Mercer — the Cambridge Analytica investor—funded it.[52]

There are even fewer rules for when campaigns pay or coordinate with third parties to amplify their content rather than paying the platforms. When it comes to commercial actors, the Federal Trade Commission enforces guidelines that require paid influencers to reveal that they have been sponsored.[53] Broadcast payola laws also concern themselves with secret sponsorship. But these rules don't apply to political influence campaigns online. U.S. presidential candidate Michael Bloomberg paid social media influencers to spread paid-for political content for his 2020 run, taking advantage of Facebook's rules allowing politicians to connect with influencers.[54] Those posts, while labeled, will not be included in the political ad library for public scrutiny. Google prohibits campaigns from using the tool to connect with influencers but permits campaigns to connect with individual influencers on their own, and without a sponsorship label.

Manipulated and Off-the-Shelf Amplification

Ads are only one piece of disinformation campaigns. While Russia's Internet Research Agency (IRA) purchased around 3,400 advertisements on Facebook and Instagram during the 2016 election campaign, "Russian-linked accounts reached 126 million people on Facebook, at least 20 million users on Instagram, 1.4 million users on Twitter, and uploaded over 1,000 videos to YouTube."[55]

Autocratic governments have long flooded the information ecosystem to distract from inconvenient news and deceive the public about critical or independent views—making it difficult for ordinary citizens to build grassroots movements. This tactic once required considerable resources, and often ran into the roadblock of skeptical newspaper and broadcast news editors, but today such disinformation campaign tools are now available off-the-shelf from commercial vendors.

NATO's Strategic Communications Center of Excellence discovered that it is easy and cheap to purchase comments, likes, views, and followers from third parties (many in Russia) operating on major platforms.[56] Private "black PR" firms increasingly offer their online influence services using paid trolls operating fake accounts. Such firms include Smaat, whose operation in Saudi Arabia on behalf of the state was taken down by Twitter, and an advertising agency in Georgia that Facebook found to be operating hundreds of accounts, pages, and groups on behalf of the country's government. The Archimedes Group, an Israeli firm, created networks of hundreds of Facebook pages, accounts, and groups around the world which it used to influence its collective 2.8 million followers, conducting for-profit operations, for example, to sway elections in Nigeria or spread disinformation in Mali, where it managed a fake fact-checking page that claimed to be run by local students.[57] Pragmatico in Ukraine and Cat@Net in Poland manage networks of fake accounts for hire.

[52] Robert Maguire, "EXCLUSIVE: Robert Mercer backed a secretive group that worked with Facebook, Google to target anti-Muslim ads at swing voters," OpenSecrets, April 5, 2018.

[53] Federal Trade Commission, "16 CFR Part 255 Guides Concerning the Use of Endorsements and Testimonials in Advertising," accessed March 10, 2020.

[54] Barbara Ortutay and Amanda Seitz, "Facebook's influencers nod shows murky side of campaign ads," Associated Press, February 14, 2020.

[55] Robert Mueller, Report on the Investigation into Russian Interference in the 2016 Presidential Election, U.S. Department of Justice, March 2019.

[56] Davey Alba, "Fake 'Likes' Remain Just a Few Dollars Away, Researchers Say," *New York Times,* December 6, 2019.

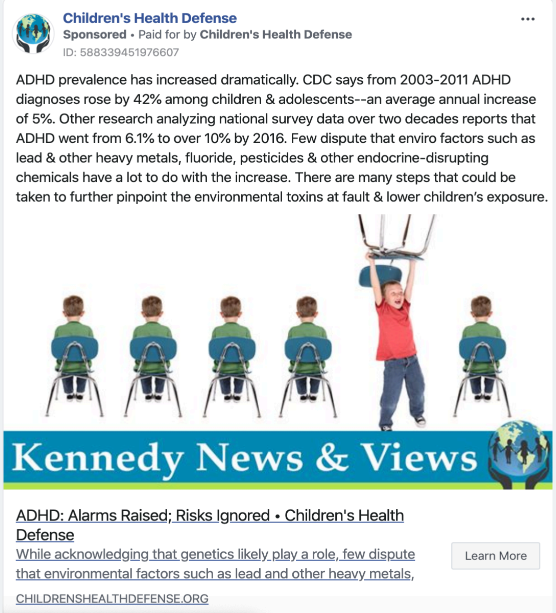
[57] Atlantic Council Digital Forensic Research Lab, "Inauthentic Israeli Facebook Assets Target the World," Medium, May 17, 2019.

Anti-Vaccine Advertisement Tactics

Recently the major platforms have implemented new policies to reduce the spread of anti-vaccine hoaxes. Reviewing Facebook's ad library for associated keywords such as "vaccine choice" or "vaccine rights" in the final quarter of 2019 reveals several ads that had either run recently or were still running that avoided using prohibited words but still took users to anti-vaccine websites. One ad—active from November 19 to November 27, 2019—promoted information on attention deficit hyperactivity disorder, but clicking on it took users to the site of Children's Health Defense, an anti-vaccine organization run by Robert F. Kennedy, Jr. Spending less than $200, Children's Health Defense was able to garner 9,000-10,000 impressions (the number of times their ad was displayed on individual screens). Of these, 60 percent were seen by women between 25 and 34 years of age, while the remaining 40 percent were viewed by women 35 to 44. Children's Health Defense is closely tied to another anti-vaccine group, the World Mercury Project, which is also headed by Kennedy and one of two organizations responsible for 54 percent of anti-vaccine advertisements placed on Facebook from December 2018 to February 2019.

Another recent anti-vaccine ad was sponsored by Michigan for Vaccine Choice. Once the user clicks on the URL in the ad or clicks on the ad sponsor, they are taken to the organization's website, which promotes articles with titles such as "$4 billion and growing DEATH AND INJURIES," featuring anti-vaccine testimonials compiled by the group and instructions on how to file vaccine injury claims. The Michigan for Vaccine Choice advertisement was still live on Facebook as of March 6, 2020, with 90,000-100,000 impressions.*

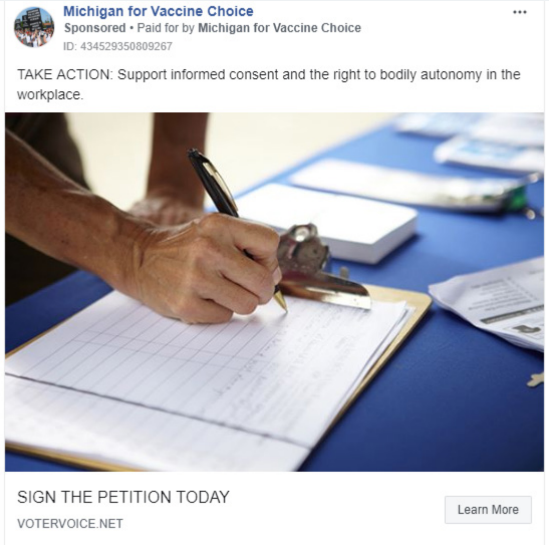
** Facebook impressions refer to the number of times a given advertisement was placed on a screen.*



Children's Health Defense
Sponsored • Paid for by Children's Health Defense
ID: 588339451976607

ADHD prevalence has increased dramatically. CDC says from 2003-2011 ADHD diagnoses rose by 42% among children & adolescents--an average annual increase of 5%. Other research analyzing national survey data over two decades reports that ADHD went from 6.1% to over 10% by 2016. Few dispute that enviro factors such as lead & other heavy metals, fluoride, pesticides & other endocrine-disrupting chemicals have a lot to do with the increase. There are many steps that could be taken to further pinpoint the environmental toxins at fault & lower children's exposure.

ADHD: Alarms Raised; Risks Ignored • Children's Health Defense
While acknowledging that genetics likely play a role, few dispute that environmental factors such as lead and other heavy metals,
CHILDRENSHEALTHDEFENSE.ORG



Michigan for Vaccine Choice
Sponsored • Paid for by Michigan for Vaccine Choice
ID: 434529350809267

TAKE ACTION: Support informed consent and the right to bodily autonomy in the workplace.

SIGN THE PETITION TODAY
VOTERVOICE.NET

According to Nathaniel Gleicher, Facebook's head of cybersecurity policy, "the professionalization of deception" is a growing threat.[58]

Disinformation is often spread through images and videos whose provenance and context are obscured and whose content is altered by editing or manufactured via AI-generated deep fakes. In this way, it slips more easily through platform rules and enforcement mechanisms. For example, Instagram has found it difficult to eliminate anti-vaccine content despite new rules and efforts.[59]

These disinformation campaigns supercharge efforts of authoritarian or Astro-turf campaigns by leveraging digital surveillance techniques to make inferences that then push people toward tailored messaging. Disinformation lies not just in the message—indeed the message may be true—but in creating an epistemic reality for people based on information the platforms have covertly gathered about them. Bots, trolls, and networks of true believers can work in coordinated fashion to increase the number of times an individual sees disinformation from different sources, crafting a sealed information environment. This repetition is persuasive. "The volume and recency of disinformation matter," according to a Hewlett Foundation review; "people are more likely to be affected by inaccurate information if they see more and more recent messages reporting facts, irrespective of whether they are true."[60]

Amplification occurs across networks. According to the Senate Intelligence Committee, "achieving the 'viral' spread of YouTube videos generally entails capitalizing on the reach and magnitude of Facebook and Twitter networks to spread links to the video hosted on YouTube."[61]

In addition, politicians, influencers, and media outlets with big platforms may contribute to amplification. The Hewlett Foundation review finds that "[i]nformation achieving mass spread usually relies on central broadcasters in a network and/or amplification by the mass media. Communities of belief, such as conspiracy theorists, are important in generating the kind of sustained attention that is needed for false information to travel."[62] Becca Lewis of the research institute Data & Society has further documented how reactionary influencers have created a fully-functioning alternative media ecosystem, one that uses YouTube as the primary medium through which to launder and amplify right-wing radicalizing content, packaging their politics as online news and entertainment and relying on the recommendation algorithm and monetization policies of YouTube itself.[63]

Bots pretending to be human and trolls assuming a false identity can deceive users about who is promoting content. Facebook reported that it shut down 5.4 billion fake accounts in the first nine months of 2019, an amount more than twice its number of actual users.[64] Search engines are manipulated using a variety of tactics identified by researchers, including

[58] Craig Silverman, Jane Lytvynenko, and William Kung, "Disinformation For Hire: How A New Breed Of PR Firms Is Selling Lies Online," Buzzfeed News, January 6, 2020.

[59] Jesselyn Cook, "Instagram's Search Results For Vaccines Are A Public Health Nightmare," *Huffington Post*, February 2, 2020.

[60] Joshua A. Tucker et al., "Social Media, Political Polarization, and Political Disinformation: A Scientific Study," William and Flora Hewlett Foundation, March 2018.

[61] U.S. Senate Select Committee on Intelligence, Report on Russian Active Measures Campaigns.

[62] Tucker et al., "Social Media."

[63] Rebecca Lewis, "Alternative Influence: Broadcasting the Reactionary Right on YouTube," Data & Society, 2018

[64] Elaine Moore, "Facebook's fake numbers problem—Lex in depth," *Financial Times*, November 18, 2019.

- keyword stuffing: adding popular keywords to unrelated websites in order to promote content in search engine rankings;

- link bombs: increasing the number of other sites (often high-traffic blogs working together) that link to the page;

- mutual admiration societies: groups of websites with links designed to appear as legitimate citations that instead point to each other;[65]

- data voids: creating news around an unused search term (for example, "crisis actor" or "caravan") and then posting content with disinformation found by users searching for the new term.[66]

One analysis of search results for senate and presidential candidates in the 2016 elections found that "up to 30 percent of these national candidates had their search results affected by potentially fake or biased content."[67]

Amplifiers and their networks cause algorithms to sense engagement and further boost the content they push, to the point where it emerges as a newsworthy or trending topic. The algorithms prioritizing content for newsfeeds, recommendations, and search results are not designed for accuracy, but rather for generating attention. They are optimized for user engagement (number of comments, shares, likes, etc.), in order to attract and keep users' attention so that they will stay online to be served more ads.[68]

Astro-turfing: Secret and Deceptive Private Groups, Pages, and Fringe Sites

In addition to microtargeting users with personalized persuasion and flooding the news zone, disinformation campaigns manipulate users by creating and infiltrating accounts, pages, and groups, pretending to represent collections of Americans with a common interest. For example, Russia's IRA created a fake "Blacktivist" page that garnered 11.2 million engagements over the course of its campaign. In general, during the 2016 elections more than 62,000 users committed to attend 129 events organized by Russian trolls, including through Russian-created Facebook pages such as Heart of Texas and United Muslims of America, which had over 300,000 followers.[69]

But as disinformation moves to Facebook's groups (the private version of pages) and encrypted messaging—which receive limited moderation and are not accessible to the public—even more users are susceptible to what researcher Jonathan Albright calls "shadow organizing" (when bad actors seed disinformation) without detection.[70] Shadow organizing can happen across multiple platforms—starting on fringe sites with more lenient rules such as Gab or 4Chan, and spreading to private Facebook groups and then beyond.

[65] Panagiotis Takis Metaxas, "Web Spam, Social Propaganda and the Evolution of Search Engine Rankings," Web Information Systems and Technologies, 2010, as quoted by Tucker et al., "Social Media."

[66] Michael Golebiewski and Danah Boyd, "Data Voids: Where Missing Data Can Easily Be Exploited," Data & Society, May 2018.

[67] Danaë Metaxa-Kakavouli and Nicolás Torres-Echeverry, "Google's Role in Spreading Fake News and Misinformation," Stanford University, October 2017.

[68] Pablo Barberá and Gonzalo Rivero, "Understanding the political representativeness of Twitter users," *Social Science Computer Review*, 2015; Daniel Preotiuc-Pietro et al., "Beyond Binary Labels: Political Ideology Prediction of Twitter Users," Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics, 2017, as quoted by Tucker et al., "Social Media."

[69] Mueller, Report on the Investigation.

[70] Jonathan Albright, "The Shadow Organizing of Facebook Groups," Medium, November 4, 2018.

New Challenge for Platforms: Dedicated Volunteers Amplifying Content

Complicating platform policies regarding inauthentic amplification, domestic volunteers now coordinate to help promote politically motivated disinformation campaigns. According to one study, online communities that "operate like fans to amplify the operation's messages and occasionally take those messages forward in unpredictable ways" interact with foreign state information operations in ways that are difficult for an observer to disentangle.* Domestic grassroots activists may share a political motivation with disinformation campaign orchestrators and work in parallel to increase outreach by targeting the same audiences, forwarding news that reinforces a message, and "also modeling a contagious emotional enthusiasm for others to follow."

Twitter's suspension of 70 accounts posting content favorable to presidential candidate Michael Bloomberg illustrates the difficulty of drawing lines when real people are involved. The accounts—part of his campaign's coordinated effort to pay people to post tweets in his favor—were suspended for violating Twitter rules on "platform manipulation and spam" that say, "you can't artificially amplify or disrupt conversations through the use of multiple accounts" including "coordinating with or compensating others" to tweet a certain message.**

Twitter similarly suspended several accounts promoting a trending phrase about U.S. Ambassador to Ukraine Marie Yovanovitch on the day of her 2019 testimony in the House of Representatives, which may have been spread through bot networks but was also promoted by authentic accounts in a coordinated fashion.***

So-called "Trumptrains," created to build up follower counts, are a way for volunteers to mass-amplify messages. Users post tweets containing lists of Twitter handles, hashtags, emojis, and usually a meme or GIF. Each "rider" is expected to follow the others in the "car," and to amplify the reach of the car by retweeting to their own followers. The result is explosive follower growth for everyone involved and a constantly expanding amplification network. As a result, many #MAGA accounts have tens of thousands of followers. Trumptrains also create and reinforce community among users, who receive notices with each retweet or like, provide organizing "work" for the participants, and build visibility for influencers.

** Kate Starbird, Ahmer Arif, and Tom Wilson, "Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations," preprint version, Human Centered Design & Engineering, University of Washington, 2019, 17.*

*** Sheera Frenkel and Davey Alba, "Digital Edits, a Paid Army: Bloomberg Is 'Destroying Norms' on Social Media," New York Times, February 22, 2020.*

**** Ryan Broderick and Lam Thuy Vo, "Twitter Has Suspended Several Accounts That Tweeted 'I Hired Donald Trump To Fire People Like Yovanovitch,'" BuzzFeed, November 15, 2019.*

Nina Jankowicz warns that private groups, along with fringe sites that link to the mainstream platforms, are "where unsavory narratives ferment and are spread, often with directions about how to achieve maximum impact."[71] These private groups and smaller platforms with looser rules provide avenues for recruiting and radicalizing extremists and for harassment, especially of women (through doxxing and revenge porn), immigrant, and minority group members. Despite Facebook policies banning content that could cause harm, in private groups users are sharing stories claiming that the coronavirus was created by the pharmaceutical industry to sell expensive drugs.[72]

The Vietnam Veterans of America, a congressionally chartered advocacy group, revealed last year that veterans are being targeted by known Russian propaganda via Facebook pages and groups. Many of these Facebook groups and pages were created and are operated by administrators from over 30 countries, including Russia, Iran, Brazil, and Vietnam.[73] The group reports that foreign individuals have created fake accounts, or in some cases stolen the accounts of real veterans, to infiltrate private groups and spread disinformation narratives. A British- and Macedonian-run Facebook page, "Vets for Trump," has garnered over 131,000 followers and disseminated not only memes and messages relevant to U.S. politics but also content promoting Russia and President Vladimir Putin.[74]

Homegrown militia movements that traffic in conspiracy theories and refuse to recognize the authority of the federal government are organizing among members of police departments through private Facebook groups. Facebook groups for militia organizations like Three Percenters and Oath Keepers (who believe that the federal government plans to take away Americans' guns, install martial law, and set up concentration camps to kill dissenters), along with neo-Confederate, Islamophobic, and white supremacist groups, count hundreds of active and former police officers among their ranks.[75]

Inconsistent Moderation Policies Do Not Meet Cross-Platform Challenge

When platforms say they do not want to police speech, they are pretending that platform moderation is not at all times a core part of their business. The Lawyers' Committee for Civil Rights Under Law wrote Mark Zuckerberg that "Facebook constantly regulates speech on its platform with curation algorithms that decide which content gets amplified and which gets buried. You have decided it is acceptable to regulate speech to increase user engagement."[76]

Disinformation disproportionately weaponizes animosity against immigrants, Muslims, Jews, women, and African Americans. Around the world, coordinated online hate speech against racial and ethnic minorities has led to violence. Rumors about Muslims circulating on WhatsApp have resulted in lynchings in India.[77]

[71] Joe Uchill, "Privacy plan could worsen Facebook's echo chamber problem," Axios, March 7, 2019.

[72] Sheera Frenkel, Davey Alba and Raymond Zhong, "Surge of Virus Misinformation Stumps Facebook and Twitter," *New York Times*, March 8, 2020.

[73] Kristofer Goldsmith, "An Investigation Into Foreign Entities Who Are Targeting Servicemembers and Veterans Online," Vietnam Veterans of America, September 17, 2019.

[74] Alex Horton, "Russian trolls are targeting American veterans, and Trump's government isn't helping, group says," *Washington Post*, January 7, 2020.

[75] Will Carless and Michael Corey, "The American militia movement, a breeding ground for hate, is pulling in cops on Facebook," Reveal News, June 24, 2019.

[76] Kristen Clarke, "Facebook, Protect Civil Rights or You Could Face Lawsuits," Lawyers' Committee for Civil Rights Under Law, November 4, 2019.

[77] Timothy McLaughlin, "How WhatsApp Fuels Fake News and Violence in India," *Wired, December* 12, 2018; Vindu Goel, Suhasini Raj, and Priyadarshini Ravichandran, "How WhatsApp Leads Mobs to Murder in India," *New York Times*, July 18, 2018.

In March 2018 the chairman of the UN Independent International Fact-Finding Mission on Myanmar said social media companies had played a "determining role" in violence in the country, having "substantively contributed to the level of acrimony and dissension and conflict." These comments were echoed a year later by the UN Special Rapporteur, who warned that "[p]ublic institutions linked to [Myanmar's] military, its supporters, extremist religious groups, and members of the government continue to proliferate hate speech and misinformation on Facebook."[78]

Albright warns that an important part of the agenda of the new online networks of amplifiers is to "silenc[e] real people who voice opposition and support for certain views." They also serve to legitimize "otherwise unsustainable rumors and ideas."[79] He found that the bulk of the harassing tweets targeting two Muslim female congressional candidates during the 2018 midterms came from a small cohort of troll-like accounts. Many of these tagged the candidates into threads and replies to "funnel hate speech, amplify rumors, and pull others into heated discussion threads."

Disinformation also targets members of more vulnerable communities. According to the Senate Intelligence Committee, during the 2016 election the IRA disproportionately targeted African Americans. Sixty-six percent of its Facebook advertisement content included terms related to race, while the vast majority of its location-based targeting was aimed at "African-Americans in key metropolitan areas with well-established black communities and flashpoints in the Black Lives Matter movement."[80] Five of the IRA's top ten Instagram accounts concentrated on African-American issues and populations. On Twitter and YouTube the picture was the same. IRA Twitter accounts frequently injected content on racial divisiveness, such as the kneeling controversy in the National Football League, and police brutality highlighted via video on its YouTube channels, 96 percent of which featured racial flashpoints.

According to Susanne Spaulding of the Center for Strategic and International Studies and formerly of the Department of Homeland Security, when bad actors use various harassment techniques to "distort or drown out disfavored speech," they disproportionately target, "journalists, women, and ethnic or racial minorities."[81] Since March 2019 at least three mass shooters announced their plans on a fringe website from which their message was spread on the larger platforms.

Platforms have adopted new rules and hired tens of thousands of staff and contractors to limit hateful content, but application and enforcement of these rules appear to be inconsistent. Leading U.S. civil rights and human rights organizations have accused Facebook of "reckless disregard for civil rights."[82] The Anti-Defamation League also points out inconsistency and lack of transparency in enforcement as major problems. Freedom House warns that social media have "provided an extremely useful and inexpensive platform for malign influence operations by foreign and domestic actors alike."[83]

[78] Mehdi Hasan, "Dear Mark Zuckerberg: Facebook Is an Engine of Anti-Muslim Hate the World Over. Don't You Care?," The Intercept, December 7, 2019; Tom Miles, "UN urges social media, investors to promote human rights in Myanmar," Reuters, March 5, 2019.

[79] Jonathan Albright, "Opinion: Trolling Is Now Mainstream Political Discourse," *Wired*, November 6, 2019.

[80] U.S. Senate Select Committee on Intelligence, Report on Russian Active Measures Campaigns.

[81] Susanne Spaulding, "Why Putin Targets Minorities," Center for Strategic and International Affairs, December 21, 2018.

[82] Clarke, "Facebook, Protect Civil Rights."

[83] Adrian Shahbaz and Allie Funk, "The Crisis of Social Media," Freedom House, 2019.

These organizations point to the fact that white nationalists continue to use event pages to harass people based on their race, religion, or other parts of their identity, and that recent changes that prevent praise of white nationalists or white supremacists are still too weak. While pages and publications associated with white nationalism—such as Red Ice TV and Richard Spencer's rebranded blog Affirmative Right have recently been taken down from YouTube and Facebook after reports by the *Guardian*—the anti-immigration page VDare and the white supremacy newsletter American Free Press are still available.[84] Spencer also remains on Twitter. Alt-right influencers and content are still widely available on YouTube, including white nationalist activist Martin Sellner, who despite documented contact with the perpetrator of the mass shooting in New Zealand in March 2019, had his YouTube channel quickly reinstated after being taken down.[85]

While the major platforms have rules against what Facebook calls "coordinated inauthentic behavior,"[86] they are not well enforced. When, for example, BuzzFeed and independent researchers identified two networks of Facebook pages that disseminated false or misleading information in a coordinated manner, the company responded that such networks did "not violate its policy against coordinated inauthentic behavior."[87] And the untruthful Daily Wire, which garners more engagement for its content than any other significant publisher on Facebook, was found to utilize a coordinated promotion operation, yet it remains online.[88]

It is difficult to hold platforms accountable for the application of their rules, since neither their enforcement actions nor platform traffic are auditable. For example, details about the Russian influence campaign in the 2016 election are only known as a result of data collected by the Senate Intelligence Committee and Special Counsel Robert Mueller. In the case of airline crashes, government officials on the National Transportation Safety Board are able to collect the black box of flight recorder data to find out what happened to help regulators at the Federal Aviation Agency update safety regulations—such ex post facto analysis cannot be conducted on social media platforms.

In April 2018 Facebook announced a plan to give researchers at a newly formed consortium, Social Science One, access to its traffic data. It was not until February 2020, however, that Facebook facilitated access to the data, after researchers complained publicly about "eternal delays and barriers from both within and beyond the company."[89] In March 2018 Twitter announced funding for research into improving civility on its platform and promised that researchers would collaborate directly with the company's team to produce "peer-reviewed, publicly available, open-access research articles and open source software whenever possible."[90] However, one of the two research teams selected was unable to reach an agreement with Twitter about how to obtain data.[91]

[84] Julia Carrie Wong, "White nationalists are openly operating on Facebook. The company won't act," *Guardian*, November 21, 2019.

[85] Mark Di Stefano, "YouTube Reinstated a Prominent European White Nationalist After He Appealed His Removal," BuzzFeed News, August 29, 2019.

[86] Alexandra Levine et al., "Why the fight against disinformation, sham accounts, and trolls won't be any easier in 2020," Politico, December 1, 2019.

[87] Craig Silverman and Jane Lytvynenko, "Facebook Says Anonymous Pages Posting Coordinated Pro-Trump Content Do Not Break Its Rules," BuzzFeed, November 20, 2019.

[88] Popular Information, "Keeping it 'real,'" October 30, 2019.

[89] Social Science One, Public statement from the Co-Chairs and European Advisory Committee of Social Science One, December 11, 2019.

[90] Twitter, "Twitter health metrics proposal submission," March 1, 2018.

[91] Mathew Ingram, "Silicon Valley's Stonewalling," *Columbia Journalism Review*, Fall 2019.

AFTER TECH UTOPIANISM

The modern Internet is in part a function of policy choices and government design. Over the years, the U.S. federal government distributed large research grants, allowed Internet service providers to connect at a low cost with the underlying telephone network, relieved the nascent industry from taxes and legal liability, and created a legal framework to ensure the infant industry could flourish.

This framework included an amendment to the Communications Act of 1996 in which Congress granted Internet firms express authority to moderate content and shielded them from liability from third-party content posted on or moving across their networks or platforms. Section 230 of the Communications Act has been called "the law that created the Internet" because it allows content to move across the Internet without permission.[92] The United States developed the idea of limited liability for intermediaries that was subsequently adopted in various forms around the world.

A handful of multi-stakeholder organizations—including the Internet Corporation for Assigned Names and Numbers (ICANN, which manages the domain name system), the Internet Governance Forum, and the Internet Engineering Task Force (which promotes technical standards)—were tasked with global governance via negotiations among technology companies, engineers, and non-governmental organizations and institutions.

When domestic policy concerns emerged, the Internet industry worked with civil society, often under threat of government regulation, on so-called self-regulatory negotiations or "light touch regulation," including privacy and child exploitation concerns. These efforts were not always successful; when the World Wide Web Consortium sought an industry-wide agreement over Do Not Track rules, it could not reach consensus between privacy advocates and the Internet advertising industry.

As the Internet has concentrated, news has moved online, and a few large digital information platforms have come to control the flow of information and news, the negotiated self-regulatory practices of the past are unable to create accountability. Each of the platforms has set its own policies, often with minimal input from civil society intermediaries or regulators, and enforces them on its own. In part, this reflects the Internet's dramatic change since its early days as a medium of decentralized person-to-person communication. Today, a few dominant digital platforms deliver content in a manner that is algorithmically programmed to keep people online and show them advertisements. Platforms have inherited the media's role and revenue streams, but not the media's norms and rules.

[92] Jeff Kosseff, *The Twenty-Six Words That Created the Internet*, Ithaca: Cornell University Press, 2019.

Old Media Obligations in a New Media World

Traditionally, democracies have prevented bottleneck control of information or media. In the U.S., telecommunications networks were licensed to ensure they provide common carriage (or that they not discriminate among speakers) and universal public access. Congress and the FCC implemented reforms designed to encourage localized control of media and limit monopolies. Broadcasters were subject to ownership caps and, although structural ownership rules have been curtailed in recent years,[93] ownership rules limit broadcasting entities from owning TV stations that collectively reach more than 39 percent of all U.S. TV households.[94] Because there were few broadcasters in each market operating over scarce public airwaves, beginning with the 1927 Radio Act and 1936 Telecommunications Act, broadcasters were held to a public-interest standard intended in part to ensure that broadcast media would operate in a manner that enabled democracy to flourish.

Facebook CEO Mark Zuckerberg justified Facebook airing even demonstrably false ads from politicians because the Federal Communications Commission requires that broadcasters do so.[95] (In fact, broadcasters are only required to provide "reasonable access" to advertising time to legally qualified federal candidates, but they often negotiate with ad agencies when the ads are false.)[96] But broadcasters have a variety of other obligations regarding political ads. They are required to include notice of sponsorship in all ads and to maintain public files of who paid for ads, what they paid, and when the ad ran so that political opponents can buy equal time. They are also required to provide these candidates their lowest price.[97]

The Public Broadcasting Act also established the Corporation for Public Broadcasting, a private, nonprofit corporation dedicated to promoting access to media content in the public interest. Approximately 70 percent of the organization's funding was dedicated to over 1,500 local noncommercial public radio and television stations across the country.[98] Following the enactment of the Children's Television Act of 1990, the FCC required television broadcasters to air "programming that furthers the development of children."[99] In addition, the National Association of Broadcasters created an industrial code of practice to fulfil their public-interest obligations, including voluntary tape-delay systems that enable the networks to have an additional layer of editorial control.

Alongside these obligations, none of which apply to digital platforms, the news media developed voluntary obligations. After the Second World War, the Hutchins Commission on Freedom of the Press concluded that the mass media had a responsibility to society, which it could either accept or face external regulation. Although the press initially greeted the report with hostility, in time it moved toward the types of reforms the

[93] Tom Wheeler, "On Local Broadcasting, Trump Federal Communications Commission 'Can't Be Serious!'," Brookings Institution, April 12, 2018.

[94] Federal Communications Commission, FCC Broadcast Ownership Rules, accessed March 10, 2020.

[95] Mike Isaac, "Dissent Erupts at Facebook Over Hands-Off Stance on Political Ads," *New York Times*, October 28, 2019.

[96] "Ellen P. Goodman of Rutgers talks about Facebook and speech," *Columbia Journalism Review*, October 30, 2019.

[97] Ibid. Unlike broadcasters, cable companies are not required to give candidates access to airtime, equal access, or lowest unit costs—and have more liberty to refuse ads if these ads violate their standards, including accuracy.

[98] Corporation for Public Broadcasting, About CPB, accessed March 10, 2020.

[99] 47 CFR § 73.671(c)

Commission suggested.[100] These news standards not only included sourcing and editorial practices but also the provision of easy to understand information by clearly separating news from opinion, providing bylines and datelines at the top of stories, a masthead, and codes and standards.

The self-regulatory framework developed for the Internet in the 1990s to govern what was then a transparent, decentralized medium must be updated to respond to the bottleneck power of the large ad revenue-supported digital information platforms. New rules and mechanisms are needed to safeguard the information ecosystem while avoiding the false choice of doing nothing or giving more power to government to control speech through vague rules. Instead, clear, transparent rules, support for independent journalism, and enhanced competition and accountability can strengthen democratic values.

[100] Margaret A. Blanchard, "The Hutchins Commission, The Press, and the Responsibility Concept," *Journalism Monographs*, May 1977.

POLICY ROADMAP FOR SAFEGUARDING DIGITAL DEMOCRACY

Today's framework is no longer fit for purpose. The government has failed to update offline policies for the online environment. News signals are weakening with the demise of so many local news outlets, while the noise of algorithmic amplification of disinformation grows louder. And the self-regulatory approach is outmatched by the dominance of a few platforms, as was underscored again recently as civil rights groups complained about inaction on online attacks on vulnerable communities. Those who are harmed by platform action and inaction can complain but have almost no recourse as they might in dealing with another industry or profession.

Below we outline a new roadmap for eliminating mechanisms exploited by third parties to corrupt the information ecosystem. Such a framework would ensure that companies' policies are consistent and enforced in a manner that is clear and responsive to the public. By imposing similar obligations on similar companies, it would protect them from accusations of taking political sides. And the new policy package would be flexible and *content- and technology-neutral* without sacrificing regulatory protection or realistic enforcement options.

The new policy roadmap would **dampen the noise created by bad actors and disinformation** by updating offline laws that safeguard consumers and elections, as well as civil rights protections and privacy for the online information ecosystem. It would **boost the signal of good information** by creating a fund for independent journalism, creating a new public media (or PBS) service for the Internet. And it would **create accountability** by strengthening the old self-regulatory approach to Internet regulation with an industry-civil society code of conduct—*focused on practices, not content*—backed up by monitoring enabled by data sharing, with a regulatory and civil enforcement backstop.

Although there is no one silver-bullet solution to the disinformation problem, there are achievable policy options that can close the space for disinformation without demanding that governments or platforms police speech. Properly conceived accountability should remedy Internet market failures, protect individual rights and safety, and fund public goods.

Dampening the Noise: Update Offline Consumer, Civil Rights, Privacy, Elections, and National Security Protections

"Light Patterns": Intuitive User Design for Greater Transparency and Friction

Today, users are unaware when they are giving up information about their online activities or interacting with a bot, or what the source of content is. It is easy and fast to like or share a post—even a false or hateful one. However, anyone who has tried to avoid agreeing to cookies on a website has experience with dark patterns—

when websites use user interfaces to manipulate users.[101] What is needed are "light patterns"—interface designs that empower users, offering transparency, information, and options that are accessible and intuitive.

Transparency: Nutrition Labels for Digital Content

- News: To be identified as news on a feed, linked content should disclose sources of funding and editorial control and comply with journalistic standards of fact-checking and transparency. In addition, expert credibility-ranking should be integrated alongside everything user interface suggests is news. According to one study, this kind of integration had the strongest effects on changing users beliefs as they related to false content.[102] While news rating systems have challenges related to defining news quality, projects such as the Trust Project, the Credibility Coalition, and NewsGuard have made significant strides in developing robust credibility-ranking methodologies. NewsGuard's report cards, seen alongside Google search results through a Chrome extension, identify nine clear, standardized, and transparent metrics for ranking a news source's accuracy and transparency.

- Fakes: Users should receive easy to understand information about whether a video or audio has been altered.

- Algorithms: Platforms should provide far greater disclosure of the way algorithms operate on a given platform, including disclosures of how content is curated, ranked, or recommended, as well as what targeting policies are used.[103]

- Accounts: User verification should be routine on those platforms that have real-name policies or verification. Other major platforms could create verified accounts where the registration is privacy-protected and posting remains anonymous. This will make it easier to identify, label, remove, and archive bots and fake accounts.

Friction: Slow Down Content Sharing to Empower Users to Exercise Choice

In addition to users being able to see what is inside the digital content they are viewing, they should have the options to respond. Ellen Goodman has developed a concept of friction that enhances cognitive autonomy, or the ability to discern signal from noise, through communication delays, platform-initiated virality disruption, and taxes to disincentivize business models that exploit user data and contribute to the rebuilding of traditional media outlets.[104] Better user interfaces would facilitate this friction by:

- Defaulting out of data sharing and requiring an opt-in to grant third-party (data collectors other than the host platforms) permissions to monitor;

[101] Ellen P. Goodman, "Information Fidelity and Digital Flows," draft paper, January 3, 2020, 7-9.

[102] Antino Kim, Patricia L. Moravec, and Alan R. Dennis, "Combating Fake News on Social Media with Source Ratings: The Effects of User and Expert Reputation Ratings," *Journal of Management Information Systems* 36 (3), 2019: 931-68.

[103] Ranking Digital Rights, Corporate Accountability Index: Draft Indicators, October 2019.

[104] Goodman, "Information Fidelity and Digital Flows," 18-19.

- Defaulting out of being tested on and targeted (including collection and inference of political views); and
- Defaulting out of algorithmic amplification and recommendations to systems a user chooses such as chronology or interests (just as e-commerce sites often allow users to choose how to display product choices).

Research on Fakes and Frauds, Media Literacy

Public investments in technology to improve detections of fakes, authentication, and user interfaces to better signal content sources and reduce manipulation are needed. Investments should also be made in media literacy. Funding could come from the Defense Advanced Research Partnership Agency (as disinformation is a national security challenge) or from public-private partnerships. Media literacy should be offered not only in schools but also online to reach older users—creating a form of inoculation against disinformation. The program could be modeled off successes in other countries, such as Finland.[105]

New Rules for Micro-Targeted Political Ads

Political advertising has long corrupted U.S. politics. Raising money for television ads initially drove the rush for fundraising and the influence of money in politics, and has only increased since the Supreme Court's *Citizens United* ruling in 2010. But broadcast stations at least faced some restraints: they had a limited inventory of ads and were required to label them and provide a library of data on who ran ads, at what time and price. Providing users transparency about who is supporting a candidate or is behind persuasive messages is essential for democratic debate. Platform self-regulation to limit microtargeting of political ads may be part of the solution, but without any other changes could disadvantage politicians or movements with smaller budgets who need to target for fundraising. A broader package of reforms can avoid these problems while reducing the scourge of dark ads online.

Limit Targeting

Federal Election Commission Chair Ellen Weintraub has proposed that platforms limit targeting of political ads to only one level below the geography of the candidate's constituency: for example, state-level targeting for presidential campaigns.[106] Others have proposed they be limited to groups of at least 50,000 users (the level for TV and radio ads to trigger election rules).[107] Senator Ron Wyden has asked platforms for a moratorium on political microtargeting, as has the U.K. information commissioner.[108] Government regulation of microtargeting might prove problematic under the First Amendment, though there is the view that it would survive constitutional scrutiny if it were applied across the board to all advertising as a way to pressure the platforms' surveillance model.[109] To mitigate the risk that any limit on microtargeting would harm smaller campaigns, it

[105] Eliza Mackintosh, "Finland is winning the war on fake news. What it's learned may be crucial to Western democracy," CNN, May 2019.

[106] Ellen L. Weintraub, "Don't abolish political ads on social media. Stop microtargeting," *Washington Post*, November 1, 2019.

[107] John Borthwick, "Ten things technology platforms can do to safeguard the 2020 U.S. election," Render-from-Betaworks on Medium, January 7, 2020.

[108] Natasha Lomas, "Facebook under fresh political pressure as U.K. watchdog calls for "ethical pause" of ad ops," TechCrunch, July 11, 2018.

[109] New Economics Foundation, "Blocking the Data Stalkers: Going Beyond GDPR to Tackle Power in the Data Economy," December 28, 2018.

would have to be accompanied by some sort of access entitlement for all qualified candidates (see lowest unit charge proposal below).

Opt-In at the Point of Data Collection

Senator Diane Feinstein has proposed that campaigns and political organizations be required to notify voters about data they gather on them and to allow people to delete that information or to prohibit the use of their data for targeted outreach.[110] A similar approach would require platforms to notify users of the collection of their political views (including inference of those views) and get permission from users before using that data to serve them targeted material.[111]

Limiting Section 230 Protection

One way to reduce false political advertising is to remove platform immunity under Section 230 for advertising. This way, platforms would have to take responsibility for the ads they run. Short of this, platforms could be nudged to apply their fact-checking rules consistently by encouraging them to create an industry code of conduct under threat of regulation, or by conditioning Section 230 protection on meeting industry best practices to prevent consumer manipulation.

Real-time Ad Transparency

The bipartisan Honest Ads Act would close the gap between rules for political advertising on broadcast media and the Internet by requiring digital platforms with at least 50 million monthly users to ensure that all political ads (including single issue ads) display information about the audience targeted, the number of views generated, the dates and times of publication, the ad rates charged, and contact information for the purchaser.

Ad Archive

The Honest Ads Act requires platforms to make available such information about ads in a public file. The major platforms have built ad libraries containing varying information. These should be expanded to include the audience reached and data used. Crucially, this public file should be user-friendly, easily searchable, and sortable through an application programming interface (API). Sponsored influencer posts for candidates should be included in the list.

"Know Your Customer" Funding Verification

Dark-money groups should be required to provide the names of their funders rather than just opaque corporate names when placing ads. Large platforms could be required to implement verification checks (as banks must to combat money laundering) to ensure that advertisers provide accurate and complete information about sponsors when purchasing ads.

[110] Office of Senator Diane Feinstein, "Feinstein Bill Would Give Voters Control Over Personal Data," press release, July 21, 2019.

[111] Karen Kornbluh, "Could Europe's New Data Protection Regulation Curb Online Disinformation?," Council on Foreign Relations, February 20, 2018.

Least Unit Cost/No Algorithmic Boost for Microtargeted Candidate Ads

As required of broadcasters, large platforms could provide political ad space to candidates at the least unit cost and provide opponents equivalent reach at equivalent price. To inhibit microtargeting, lower prices could be offered for wide distribution.

Updated Civil and Human Rights Laws and Approach to Deceptive and Hateful Content

Discrimination, harassment, and privacy laws should be updated for the online environment. Platforms should take a common approach to avoid promoting disinformation and harassment. Further, they must limit manipulation of users without their knowledge or consent.

Update Civil Rights, Terrorism, and Harassment Laws

The definition of a public accommodation can be extended for civil rights purposes (under U.S. law, this includes private facilities used by the public such as hotels and restaurants) to include businesses that offer goods or services through the Internet. As proposed by the Lawyers' Committee for Civil Rights Under Law, this would make it illegal to deny or interfere with equal access to or use of these platforms on the basis of race, religion, or national origin.[112] The Equality Act that passed the House of Representatives in May 2019 (but has not been taken up by the Senate) adopts this idea in part by expanding public accommodation provisions to apply to the Internet (in addition to expanding protected categories to include LGBTQ+ people).

Penalize Online Sextortion and Privacy Invasions

Online harassment including sextortion, doxxing, non-consensual pornography, and swatting should be penalized and resources should be provided to local and federal law enforcement to investigate and prosecute online crimes and severe online threats, as Representative Katherine Clark has proposed.[113] Law professors Danielle Keats Citron of Boston University and Mary Anne Franks of the University of Miami have argued for criminalizing non-consensual pornography.[114] Citron has also advocated combating the "constellation of sexual-privacy invasions," including "digital voyeurism, up-skirt photos, extortion, nonconsensual porn, and deep-fake videos" by expanding the coverage of privacy torts in civil claims and treating sexual privacy invasions as felonies.[115]

[112] Kristen Clarke and David Brody, "It's time for an online Civil Rights Act," The Hill, August 3, 2018.

[113] Online Safety Modernization Act of 2017, H.R. Bill 3067, 115th Cong. (2017). Sextortion is the use of coercion to obtain sexual favors. Doxxing entails releasing personal identifying information (such as street address and phone number) of a victim. Swatting is the criminal harassment of a victim by falsely reporting the need for emergency services at a victim's home.

[114] Danielle Keats Citron and Mary Anne Franks, "Criminalizing Revenge Porn," *Wake Forest Law Review*, 2014.

[115] Danielle Keats Citron, "Sexual Privacy," *Yale Law Journal*, 2018.

Make Online Voter Suppression Illegal

It should be illegal to use online fora to intimidate or deceive people into not exercising their right to vote or register to vote. Large online companies should be required to help prevent these violations on their platforms, as Free Press and the Lawyers' Committee for Civil Rights Under Law have proposed.[116] Accounts that engage in this activity should be taken down.

No Immunity for Civil Rights Violations

Policymakers could exempt violations of civil rights laws from Section 230 protection to incentivize digital platforms to be more vigilant about such violations on their platforms.

Combat Domestic Terrorism, White Supremacy

White supremacists were responsible for more homicides than any other domestic extremist movement between 2000 and 2016. Law enforcement agencies should be required to monitor, analyze, investigate, and prosecute domestic terrorist activity as laid out in the Domestic Terrorism Prevention Act, a bill introduced in 2019 by Senators Tim Kaine and Dick Durbin.[117]

Penalize Lawbreakers and Violators

Major platforms should refuse to link to fringe websites upon notice that a court has found them liable for failing to take down unlawful content, such as posts dedicated to the incitement of violence. On issues of voting and scientific or public health information (for example, vaccines), all platforms should provide banner notices with accurate information, redirect to deradicalizing sites, and refuse ads that promote voter or public health misinformation or that link to websites promoting such misinformation.

Privacy Rights

The U.S. needs a uniform privacy law to provide users with the ability to protect their privacy and ensure that platforms are not allowing such data to be used to manipulate users. California has enacted a new privacy law inspired by the European Union's General Data Protection Regulation guaranteeing Californians the right of access, deletion, portability, opt-out of sale (monetized sharing) of their data to third parties, and a "right to know" how their data is used, while also creating substantial class-action liability for some types of data breaches. Federal privacy legislation is gaining momentum that might go beyond the "notice and consent" framework to take certain practices off the table (such as collection and sale of biometric, location, or health information; information collected from microphones or cameras; or cross-device tracking), and to create new governance procedures for companies collecting personal information. Additional provisions not in the California law could also limit the collection or inference of political views for targeted advertising and could ban targeted advertising that results in prohibited discrimination.

[116] Clarke, "Facebook, Protect Civil Rights."

[117] Office of Senator Tim Kaine, "With Rise In White Supremacist Attacks, Kaine Introduces Bill To Combat Threat Of Domestic Terrorism," press release, March 27, 2019.

National Security Information Sharing

Platforms should be required to share information with one another and with government agencies on violent extremism and terrorism, including through the creation of an information-sharing network with classified details for approved platform employees, as the Alliance for Securing Democracy has proposed.[118] Other recommended information sharing measures include:

- Continue to build up and add to the Global Internet Forum to Counter Terrorism shared industry hash database for white nationalism and a list of radicalizing sites from which the platforms will not allow content or links.
- Reinstate the Cybersecurity Coordinator in the National Security Council.
- Disclose publicly when platforms or the government discover foreign interference in an election and archive the disinformation (in a way that protects the privacy of the users, not the foreign interference operators).
- Notify users who have interacted with foreign disinformation.

Boosting Signal: Promote Local News, Public Infrastructure, and Choice of Curation

Restoring the integrity of the information ecosystem will entail not only closing loopholes that allow bad actors to pollute the information environment with noise, but also strengthening productive capacities for good information: boosting the signal of independent, transparent journalism. This could be achieved by the following measures.

Superfund-Type Tax on Ad Revenue to Fund New Noncommercial Digital Infrastructure

Scholars have argued for more than a decade that the reasons for supporting non-market media and information infrastructure (like transmitters and satellite connections) persisted in the digital era and that the structure of public subsidy for these public goods needed updating.[119] Some have focused on subsidies for content, like local news.[120] Others have focused more on technology tools, such as search and discovery not beholden to corporate or advertiser interests.[121]

The problem of a marketized public sphere goes beyond platform disinformation problems and even the decimation of local journalism. Governments at all level communicate with the public through Facebook and Twitter and rely on commercial cloud services, especially Amazon's. It is also worrying that a few corporations already have power over services that nominally belong to the public. Anchor institutions such as public

[118] Jamie Fly, Laura Rosenberger, and David Salvo, "Policy Blueprint for Countering Authoritarian Interference in Democracies," The German Marshall Fund of the United States, June 2018.

[119] See, for example, Ellen P. Goodman and Ann Chen, "Modeling Policy for New Public Media Networks," *Harvard Journal of Law and Technology* 24 (1), 2010, 111.

[120] Emily Bell, "How Mark Zuckerberg could really fix journalism," *Columbia Journalism Review*, February 21, 2017; Victor Pickard, Democracy Without Journalism?: Confronting the Misinformation Society, Oxford: Oxford University Press, 2019.

[121] Ethan Zuckerman, "The Case for Digital Public Infrastructure," Knight First Amendment Institute, Columbia University, January 17, 2020.

libraries and universities, as well as public media entities, could become customers for new nonprofit digital architecture components, which would provide for public resiliency and self-reliance. These components could include social media curation and search tools, cloud infrastructure, and data repositories. These are the 21st century equivalents of broadcast towers and satellite interconnection that have been funded through appropriations to the Corporation for Public Broadcasting.

Create an Internet PBS—Funding Local Public Interest News and Civic Information Architecture

News is a public good. Internet platforms have eaten away the revenues of the providers of this good. Funds raised through a tax on advertising or other means could be directed to an independent nonprofit (like the Corporation for Public Broadcasting), or even to consumers as vouchers to support news organizations of their choice. Eligibility could be limited to outlets that follow journalistic codes of practice (for example, transparency, corrections, and separating news from opinion), possibly relying on organizations such as the Trust Project and NewsGuard. As Nicholas Lemann has argued, turning to a model of direct government subsidy may offer the best chance that high-quality, civically oriented, substantive reporting has of surviving the future.[122] New Jersey is piloting this approach, recently providing $2 million in funding for a nonprofit news incubator for local journalism, using partnerships with universities in order to provide expertise and an apolitical interface.[123] Funds could also be used to highlight and make available local news, media literacy, civic and voter information, publicly funded scientific research, and government data. These efforts could be funded in several ways, including taxing advertising revenue[124] or giving citizens a tax check-off option.[125]

Creating Accountability: Make an Enforceable Code of Conduct

It is clear from the lack of standards across platforms, shallow engagement with civil society, and contingent sharing of data that for any of the processes above to work consistently, additional accountability tools are required. But vague rules granting government power over speech are not the answer. Instead, policymakers should give users additional control through competition, bringing platforms to the table to negotiate an auditable code of conduct focused on practices rather than content.

Competition

Lack of competition can undermine the health of the public square by limiting or skewing speech options. Policymakers understood this when they subjected broadcasters to ownership limits and prohibited them from cross-ownership of stations and print newspapers. The Federal Trade Commission, Department of Justice, and state attorneys general are conducting antitrust investigations of large tech companies, and the House Antitrust Subcommittee is investigating whether antitrust law should be updated for digital platforms. Any antitrust suit would move slowly and be tough to win under current law, but in the meanwhile regulatory oversight could introduce greater competition.

[122] Nicholas Lemann, "Can Journalism Be Saved?" *New York Review of Books*, February 27, 2020.

[123] Marlee Baldridge, "Water in a news desert: New Jersey is spending $5 million to fund innovation in local news," NiemanLab, July 3, 2018.

[124] Paul Romer, "A Tax That Could Fix Big Tech," *New York Times*, May 6, 2019.

[125] Guy Rolnik et al., "Protecting Journalism in the Age of Digital Platforms," Stigler Center for the Study of the Economy and the State, University of Chicago Booth School of Business, July 1, 2019.

Data portability would provide tools for users to export their network to competing platforms with the appropriate privacy safeguards in place. Instagram owed much of its initial success to the open APIs that allowed Twitter and Facebook users to import their friend networks to a new, competing service.

Interoperability would facilitate competition by enabling communication across networks. Some have suggested implementation by requiring platforms to maintain APIs for third-party access under terms that are fair, reasonable, and non-discriminatory.[126]

Open the Black Box: After-Action Reports for Accountability

Details about the Russian influence campaign in the 2016 election are only known as a result of data collected by the Senate Intelligence Committee and Special Counsel Robert Mueller. Platforms should be required to *provide* access to information in a privacy-protected fashion with a common rubric across platforms to researchers, civil society, or a government agency so that policymakers and the public can know the nature of disinformation campaigns and the platforms' compliance with their stated policies. This information might include:

- platform policy changes;
- moderation decision logs, including lists of behavior or content that has been removed or downgraded, as well as action(s) taken on flagged accounts and content;
- traffic; and
- archived disinformation operation take-downs and alerts to users if they have interacted with disinformation.

Digital Democracy Agency

The administrative state of the 20th century relied on expert federal agencies to write rules specifying how industry sectors should comply with laws—sometimes shielding them from liability if they did so. As discussed above, the Internet developed under a different framework—a domestic, self-regulatory model (mirroring the multi-stakeholder model for global Internet governance) in which industry and stakeholders developed codes of conduct. In the early days, these domestic negotiations often took place under threat of regulation or enforcement of related broad laws. That model has broken down—and with it, public accountability.

A new model would reform both the self-regulatory and expert agency approach for accountability, flexibility, and free speech protection. To ensure that rules are workable and preclude arbitrage across platforms, neither industry alone (because it is naturally too focused on market imperatives), an agency alone (too slow and unable to develop operational solutions), civil society alone (lacking the funds and platform data to create accountability), nor the courts alone (ex-post without predictability or auditing for enforcement) can implement and enforce rules by themselves. However, a digitally nimble institution could provide oversight and, if necessary, act as a backstop to enforce both transparency and the creation and execution of a code of conduct.

[126] Office of Senator Mark R. Warner, "Potential Policy Proposals for Regulation of Social Media and Technology Firms," press release, 2018.

We have previously proposed a new public institution to protect the integrity of the digital information ecosystem (a Digital Democracy Agency), but an existing agency or several working together could also fill this role if holding sufficient authority and expertise.[127] This institution would not regulate content or specify methods or technology, but instead focus on enforcing clearly delineated practices, like those specified above, to limit the systemic vulnerabilities of platforms and defend against disinformation practices.

To prevent the typical slow pace of regulatory rulemaking—unworkable in this setting—and regulatory capture—or the corruption of regulation to benefit powerful interests—the Digital Democracy Agency would:

- put outcomes data online (in a privacy protected format), using naming and shaming to solve problems whenever possible;
- crowdsource the complaints process and use online tools for involving the public;
- use radical transparency in revealing with whom agency staff meets and sharing its anonymized data and (where possible) enforcements; and
- offer appropriate salaries to attract and retain top-level tech talent and implement strengthened post-employment lobbying restrictions.

A new or existing agency focused on emerging platform issues should work hand in hand with other agencies focused on similar or adjacent issues.

Accountable Code of Conduct

Today's variable, confusing company-specific rules for takedowns and demotions leave users in the dark about the extent to which an individual platform is protected against misinformation or harassment. Platforms should together develop a code of conduct to provide users consistent protection. While government has no role in determining content, it can be a backstop for compliance with industry best practices.

Platforms would agree with civil society to a harmonized, transparent code focused on *practices not content* and allow monitoring. The code itself would address how platforms would implement the new rules above and would also spell out a common approach for issues on which the First Amendment limits government's role, such as:

- *Clear definitions and rules, vigorously enforced, for political ads, candidates, and political figures*. This should include using only accredited fact-checkers and committing to a reasonable time frame for review. Consistent standards should be established for what is fact-checked and what is penalized (for example, whether altered audio, deep fakes, or voting misinformation is penalized). Penalties should be standardized for content fact-checked as false (for example, platforms could reduce amplification, take it down, or not allow it in ads) and when exceptions apply.

[127] Kornbluh and Goodman, "Bringing Truth."

- *Best practices for conducting research on users through tracking and testing*. For example, there could be notification standards for or limits on manipulation; these could emulate ethical rules on scientific research on humans.

- *Deference to expert bodies.* Civil and human rights groups should define hate groups and behavior, and scientific and public health bodies (such as the World Health Organization) should guide the definition of sound science.

- *Promoting voting information at the top of a user's feed*. This could include early and absentee voter information (as some now do for vaccine information).

- *Redirecting and promoting credible and deradicalizing information.* Users should be directed away from circulating conspiracy theories and radicalizing sites. Search results should not favor Islamic State, vaccine misinformation, white supremacists/nationalists (the threat of which the FBI has elevated to the level of Islamic State), climate disinformation, or similar content.

- *Deprioritizing engagement in designing recommendation algorithms*. More credible sources should be recommended, and users should be provided with options for tailoring their recommendation algorithms.

- *A robust, transparent appeals process.* Content moderation decisions should go through a transparent tribunal, as Public Knowledge has suggested. Users would be given the opportunity to present evidence, cross-examine witnesses, examine the opposing evidence, and have the right to receive findings of fact and rationale(s) for a given enforcement decision.[128]

- *White-listing of independent news through promotion, differentiation, and other means.* Platforms should agree to highlight independent, public-interest news outlets that follows journalism standards—these outlets should not have to buy ads to be promoted as well as looking different than trojan horse outlets.

- *Best practices for behavioral tracking and testing of content on users.* Senators Mark Warner and Deb Fischer have pointed out in proposed legislation that such activity (for example, A/B testing) is equivalent to conducting research on users.[129]

Limit the Immunity Provided by Section 230

Various experts have proposed eliminating or limiting Section 230 to allow victims to take concerns directly to court. However, because there is no underlying liability for disinformation and other toxic speech, this approach is unlikely to solve the problem and would result in overzealous takedowns by platforms out of fear of lawsuits. Some senators are now considering following the lead of other countries and conditioning Section 230 immunity on compliance with vague content-based outcomes. This is the wrong direction. Government

[128] John Bergmayer, "Even Under Kind Masters: A Proposal to Require that Dominant Platforms Accord Their Users Due Process," Public Knowledge, May 2018.

[129] Brian Fung, "Lawmakers want to ban 'dark patterns,' the Web designs tech companies use to manipulate you," *Washington Post*, April 9, 2019.

should not be in the position of deciding what is biased or neutral content. Instead, immunity might be limited in specific ways to enable accountability:

- *Code of Conduct Safe Harbor*: Section 230 application to Good Samaritans could be made available only to platforms that enforce a multi-stakeholder code of conduct—focused on practices (as above), rather than content.

- *Illegal Content:* Boston University's Citron and Brookings's Benjamin Wittes also propose that Section 230 immunity not apply when platforms have encouraged or failed to take reasonable steps to prevent or address illegal content.[130]

- *Remove Immunity for Monetized Content*: John Bergmayer of Public Knowledge has proposed removing Section 230 immunity for monetized content. This is likely to be a tricky category of content to define. It is relatively clear when, for example, YouTube has commercial relationships with a channel. It is less clear when content on Facebook is targeted to lookalike audiences and then shared organically. A narrower category of Section 230 immunity exemption would be just advertisements themselves. These approaches would expose platforms to liability, for example, for defamatory ads or content that directly generates revenue for the platforms.[131]

Today, citizens themselves have few tools to evaluate a platform's security, privacy, lack of transparency, or algorithms. As the United States has abdicated its traditional leadership role on Internet policy, Europe is stepping into the void, and the Russian and Chinese governments are leveraging the lack of international consensus to use the Internet for political repression and control, in their own countries and abroad. Meanwhile, smaller countries are left with few options, forced to operate in a geopolitical arena with little international consensus or guidance. It is time to take active steps to ensure that the Internet is a tool to strengthen, not undermine, democratic values. In order to do so, we must agree on a common framework for understanding these challenges and embrace practical solutions that protect privacy and free expression while strengthening the information ecosystem.

[130] Danielle Keats Citron and Benjamin Wittes, "The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity," *Fordham Law Review*, 2017.

[131] John Bergmayer, "How to Go Beyond Section 230 Without Crashing the Internet," Public Knowledge, May 21, 2019.

Policy Roadmap for Safeguarding Digital Democracy

	Independent Data Access for Monitoring	Agency Oversight	Code of Conduct	Civil Enforcement	Public Funding/Tax	Competition, Interoperability, Portability
Dampen the Noise: Update Legal Rights and Responsibilities						
Require or Incentivize "Light Patterns" (intuitive user design for greater transparency and helpful frictions)						
Clear nutrition labels for accounts, news, fakes, algorithms, ads	•	•	•	•		
Label and downrank fakes and frauds	•	•	•	•		
Default out of data sharing	•	•	•	•		
Default out of being tested and targeted	•	•	•	•		
Default out of algorithmic amplification and recommendation	•	•	•	•		
Research on fakes and frauds; media literacy					•	
Update Election Rules for Disclosure and Micro-Targeted Political Ads						
Limit targeting	•	•	•	•		
Opt-in at the point-of-data collection	•	•	•	•		
Real-time ad transparency	•	•	•	•		
Ad archive	•	•	•	•		
"Know your customer" funding verification	•	•	•	•		
Least-unit-cost regime for campaign advertising	•	•	•	•		
No-algorithmic boost for micro-targeted candidate ads	•	•	•	•		
Update Civil and Human Rights and Protections						
Update civil rights, terrorism, and harassment laws				•		
Penalize online sextortion and privacy invasions				•		
Prohibit online voter suppression				•		
Limit Section 230 immunity for civil rights violations				•		
Increase enforcement penalties				•		
New privacy rights	•	•	•	•		
Increase National Security Information Sharing						
Add to the Global Internet Forum to Counter Terrorism hash database for white nationalism and list of radicalizing sites						•
Reinstate the National Security Council cybersecurity coordinator						•
Better public disclosure of foreign interference						•
Boost the Signal: Promote Independent Local News and Public Infrastructure, and Choice of Curation						
Tax ad revenue to provide new funding for public digital infrastructure					•	
Create a PBS of the Internet—funding local public-interest news and access to news, media literacy, and civic architecture					•	
Ensure interoperability so users can use alternative curation/recommendation engines on platforms	•	•	•	•		
Accountable Code of Conduct	•	•	•	•		•

The views expressed in GMF publications and commentary are the views of the author(s) alone.

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF does this by supporting individuals and institutions working in the transatlantic sphere, by convening leaders and members of the policy and business communities, by contributing research and analysis on transatlantic topics, and by providing exchange opportunities to foster renewed commitment to the transatlantic relationship. In addition, GMF supports a number of initiatives to strengthen democracies. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

This report was made possible with the generous support of:

KNIGHT FOUNDATION

democracy fund

WILLIAM + FLORA Hewlett Foundation

G | M | F

Ankara • Belgrade • Berlin • Brussels • Bucharest
Paris • Warsaw • Washington, DC

www.gmfus.org