

May 2020

Getting to the Source of Infodemics: It's the Business Model

A Report from Ranking Digital Rights

Nathalie Maréchal, Rebecca MacKinnon, & Jessica Dheere

Acknowledgments

This report was written by Ranking Digital Rights (RDR) Senior Policy Analyst Nathalie Maréchal, Director Rebecca MacKinnon, and Deputy Director Jessica Dheere.

Research Director Amy Brouillette, Company Engagement Lead Jan Rydzak, Communications Manager Kate Krauss, Communications Associate Hailey Choi, and Editorial Consultant Nonna Gorilovskaya also contributed to this report.

We wish to thank all the reviewers who provided their feedback on the report. Their inclusion here does not mean that they support or agree with any of the report's statements, proposals, recommendations or conclusions:

- Dunstan Allison-Hope, Vice-President, BSR
- Sharon Bradford Franklin, Policy Director, Open Technology Institute
- Melissa Brown, Partner, Daobridge Capital Limited & Advisor, Ranking Digital Rights
- Bennett Freeman, Co-Founder, Global Network Initiative & Board Secretary, 2010-2020
- David Kaye, University of California Irvine & UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression
- Gaurav Laroia, Senior Policy Counsel, Free Press
- Eric Null, U.S. Policy Manager and Global Policy Counsel, Access Now
- Courtney Radsch, Advocacy Director, Committee to Protect Journalists
- Spandana Singh, Policy Analyst, Open Technology Institute

- Amie Stepanovich, Executive Director, Silicon Flatirons Center for Law, Technology, and Entrepreneurship at the University of Colorado Law School

Original art by Paweł Kuczyński.

We would also like to thank Craig Newmark Philanthropies for making this report possible.

For a full list of current and former project funders and partners, please see: www.rankingdigitalrights.org/who/partners.

For more about RDR's vision, impact, and strategy see: www.rankingdigitalrights.org/about/

For more about New America, please visit www.newamerica.org.

For more about the Open Technology Institute, please visit www.newamerica.org/oti.

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, please visit creativecommons.org/licenses/by/4.0.

About the Author(s)

Nathalie Maréchal is senior policy analyst at Ranking Digital Rights. She leads RDR's policy engagement with stakeholders in government, civil society, and academia; coordinates the development of RDR's policy positions; and publicly represents RDR with the media and at conferences around the world.

Rebecca MacKinnon is director of Ranking Digital Rights (RDR), a program that works to promote freedom of expression and privacy on the internet by creating global standards and incentives for companies to respect and protect users' rights.

Jessica Dheere is deputy director of Ranking Digital Rights at New America, a program that works to promote freedom of expression and privacy on the internet by creating global standards and incentives for companies to respect and protect users' rights.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Open Technology Institute

OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

About Ranking Digital Rights

Ranking Digital Rights (RDR) works to promote freedom of expression and privacy on the internet by creating global standards and incentives for companies to respect and protect users' rights.

Contents

| | |
|---|----|
| Executive Summary | 5 |
| Introduction | 8 |
| Targeted Advertising and COVID-19 Misinformation: A Toxic Combination | 13 |
| Human Rights: Our Best Toolbox for Platform Accountability | 22 |
| The Impact of Targeted Advertising and Algorithmic Systems on Human Rights | 25 |
| Making All Ads “Honest” Through Transparency, Limited Targeting, and Enforcement | 28 |
| By Protecting Data, Federal Privacy Law Can Reduce Algorithmic Targeting and the Spread of Disinformation | 31 |
| Scope and Purpose of Data Collection, Use, and Sharing | 32 |
| Inferred Information and Targeting | 34 |
| The Challenge of Effective Enforcement | 35 |
| Good Content Governance Requires Good Corporate Governance | 38 |
| Empower Shareholders to Address Environmental, Social, and Governance Issues by Phasing Out Dual-class Shares | 38 |
| Investors Need More and Better Disclosure | 40 |
| Targeted Advertising Revenue Disclosure | 43 |
| Due Diligence: Understanding the Full Scope of Platforms’ Social Impact | 45 |
| Without Civil Society, Platform Accountability is a Pipe Dream | 49 |
| Key Recommendations for Policymakers | 54 |
| Conclusion | 57 |

Executive Summary

Before the COVID-19 pandemic hit, democracies were already struggling to address disinformation, hate, extremism, and other dangerous online content while also protecting free speech and privacy. Now, Facebook, Twitter, and Google's YouTube are awash with disinformation and misinformation that can be deadly. Despite the companies' commitment to take unprecedented steps to control the problem, they are failing.

This report argues that Facebook, Twitter, and Google's targeted advertising business models, and the opaque algorithmic systems that support them, are the root cause of their failure to staunch the flow of misinformation.

The second in a two-part series aimed at U.S. policymakers and anybody concerned with the question of how internet platforms should be regulated, this report reinforces the need to adopt a human rights framework for platform accountability. We propose concrete areas where Congress needs to act to mitigate the harms of misinformation and other dangerous speech without compromising free expression and privacy: transparency and accountability for online advertising, starting with political ads; federal privacy law; and corporate governance reform.

First, we point to concerning examples from the pandemic that highlight the connection between targeted advertising and misinformation about the coronavirus and its purported remedies. We explain how international human rights standards provide a framework for holding social media platforms accountable that complements existing U.S. law and can help lawmakers determine how best to regulate these companies without curtailing users' rights.

Drawing on our five years of research for the Ranking Digital Rights (RDR) Corporate Accountability Index, we then point to concrete ways that the three social media giants have failed to respect users' human rights as they deploy targeted advertising business models and algorithmic systems. We describe how the absence of data protection rules enables the unrestricted use of algorithms to make assumptions about users that determine what content they see and what advertising is targeted to them. We note that such targeting can result in discriminatory practices as well as the amplification of misinformation and harmful speech.

Next, we explain why expanding the transparency requirements that currently apply to print and broadcast political ads to all types of online advertising is a prerequisite for oversight and accountability, and how a robust federal privacy law can help fight misinformation and dangerous speech, while acknowledging enforcement challenges.

The final section makes a case for corporate governance reform. We explain how trends in environmental, social, and governance (ESG) investing are prompting companies to adopt due diligence and impact assessment standards, and can strengthen corporate governance over the long term. In light of investors' growing interest in holding companies accountable for their social impact, we describe the role Congress can play in mandating corporate disclosure of information pertaining to the social and human rights impact of targeted advertising and algorithmic systems. We also recommend actions that could be taken by the U.S. Securities and Exchange Commission (SEC) to empower shareholders. We again highlight enforcement challenges while also noting strides made by European companies that, if ignored, may portend a loss in global market share for American companies that do not follow.

To conclude, we offer some thoughts about how civil society stakeholders, including researchers, journalists, and advocacy and grassroots organizations, are critical to addressing accountability gaps, especially in the absence of effective regulation and oversight. We also explain why companies must proactively engage with civil society as a part of their efforts to mitigate the negative social impacts of their business models.

Key Recommendations for U.S. Policymakers

Enact federal privacy law that protects people from the harmful impact of targeted advertising. Specifically, this law should:

- **Ensure effective enforcement** by designating an existing federal agency, or create a new agency, to enforce privacy and transparency requirements applicable to digital platforms.
- **Include strong data-minimization and purpose limitation provisions:** Users should not be able to opt-in to discriminatory advertising or to the collection of data that would enable it.
- **Give users very clear control** over collection and sharing of their information.
- **Restrict how companies are able to target users.** The law should prohibit the use of third-party data to target specific individuals, as well as discriminatory advertising that violates users' civil rights.

Require that platforms maintain a public ad database to ensure compliance with all privacy and civil rights laws when engaging in ad targeting: Pass the Honest Ads Act, expand the public ad database to include all advertisements, and allow regulators and researchers to audit it.

Require relevant disclosure and due diligence around the social and human rights impact of targeted advertising and algorithmic systems.

- **Mandate disclosure of targeted advertising revenue along with disclosure of environmental, social, and governance (ESG) information**, including information relevant to the social impact of targeted advertising and algorithmic systems.
- **Require due diligence:** Companies should be required to conduct assessments of their social impact and risks, including human rights risks associated with targeted advertising and algorithmic systems.

Strengthen corporate governance and oversight. The U.S. Securities and Exchange Commission (SEC) rules should empower shareholders to hold company leadership accountable for social impact.

- **Phase out dual-class shares:** Companies should not be able to maintain a dual class system of shares that effectively empowers the CEO to vote down shareholder resolutions in perpetuity.
- **Do not make it harder to file shareholder resolutions:** The SEC should scrap proposed rule changes that will make it more difficult for shareholders to file proposals.

Introduction

As the pandemic death toll continued to rise in the spring of 2020, myriad myths and conspiracy theories circulated, including some dangerous falsehoods, about COVID-19 on Twitter and other social media: mobile 5G technology helps spread the virus; zinc, celluloid silver, miracle mineral solution, and garlic can cure the virus; hydroxychloroquine has a 100 percent success rate in treating the virus—ingesting bleach may help; and vaccines are being developed with microchip tracking technology funded by Bill Gates.¹

Misinformation can be both polarizing and deadly. It is disturbing that social media companies failed to remove posts promoting the falsehoods described above, despite the companies' commitments to remove COVID-19 misinformation. With so little known about the novel coronavirus and how to stop its spread, conspiracy theorists, hucksters, political opportunists, and would-be authoritarians worldwide have adopted tactics honed for recent political campaigns to further exploit social media's algorithmic toolset, using platforms' targeted advertising systems to amplify unfounded virus transmission theories and remedies.

Policymakers have proposed holding companies liable for speech rather than for their targeted advertising business models, the real source of the problem.

Social media platforms are part of a broader information ecosystem that also includes news organizations and other influential actors, including political leaders and celebrities. The growing impact of social media platforms on our information environment is fueled by advertising in general, and targeted advertising in particular. Fifty-five percent of American adults say they get their news from social media.² That includes information about political candidates and policy issues from ads on Facebook and Google. In 2018, those two companies combined receive almost 60 percent of all digital advertising dollars in the United States.³ They are projected to earn 77 percent of the more than \$1.34 billion that is expected to be spent on U.S. digital political advertising in the 2019-2020 election cycle.⁴ Before deciding to ban political advertising last fall, Twitter earned \$3 million from political ads during the 2018 midterm elections.⁵

Social media platforms draw attention and advertising dollars away from news outlets whose journalism also includes critical facts without which citizens cannot make informed choices about how to live their lives—or to vote.

But digital platforms' increasing share of news and advertising is only the beginning of the story. Since the 2016 U.S. presidential election, companies like Facebook, Google, and Twitter have struggled to curtail the circulation of both organic and paid false information on their platforms. The content moderation and takedown systems that social media companies have put in place to enforce their content rules are failing society as well as individual users: harmful misinformation continues to flow; while content moderation rules are enforced in inconsistent and often arbitrary ways, resulting in unintended deletion of content produced by activists and journalists, thereby restricting freedom of expression.⁶ Company systems intended to block coronavirus misinformation from ad platforms have been proven ineffective.

In parallel, policymakers have begun to address the problem of dangerous online content, particularly by formulating proposals to amend the extent to which companies are legally liable for user-generated speech on their platforms.⁷ But such proposals do not address what makes these platforms different—and so potentially dangerous: their targeted advertising business models and the algorithmic systems that drive them.

Targeted advertising business models require extensive data collection and algorithmic content shaping in order to maximize targeted advertising revenue. Designed to prioritize sensational, eye-catching, and controversial content, they disproportionately amplify organic and paid speech that has great potential to corrupt the quality of information we need to promote not just healthy democracies and fair elections, but also, as we've seen in the COVID-19 pandemic, public health. At the same time, targeted advertising enables paying customers to target different types of content, including ads, at specific audiences based on people's demographics and declared interests as well as algorithmically inferred assumptions about other affinities and traits that may not even be correct.

Content moderation is necessary, but far from sufficient.

Against the backdrop of both a global pandemic and a U.S.-presidential election campaign, it is now incontrovertible that strengthening platform accountability and, thus, the integrity and resilience of our information ecosystem, is critical to the future of democracy. This report, which offers concrete U.S. policy recommendations, is the second in a two-part series examining how targeted advertising business models can drive the spread of misinformation⁸ and dangerous speech,⁹ and what U.S. lawmakers and regulators can do to hold companies accountable for these systems without infringing on human rights. We make the case for why and how policymakers and advocates should prioritize holding platforms accountable for mechanisms, policies, and practices that enable the amplification and targeting of user-generated misinformation and dangerous speech—without which the speech would have less reach and, thus, fewer negative effects—instead of holding the companies liable for the speech itself.

Some policymakers are focused on breaking up these huge companies as the key to limiting social harms they can cause or contribute to. Antitrust is not a focus of this report, though encouraging competition, ensuring interoperability, and potentially breaking up monopolies are important parts of the policy toolkit that have the potential to alleviate some of the problems that are exacerbated by the major platforms' enormous scale. But these regulatory interventions alone will not be sufficient. Checking the power of Big Tech will require a two-pronged approach outside the context of antitrust, and competition law more broadly, that aims to mitigate the harms posed by the underlying ad- and attention-driven business model that drives platform revenue. That approach involves: 1) a comprehensive and enforceable federal data privacy regulation, and 2) holding companies directly accountable by shining sunlight on the harms created by the business model and promoting policies that increase the fairness, accountability, and overall transparency of those practices.

Having outlined in part one the challenges to both human rights and civil liberties targeted advertising and algorithmic systems present, this second report focuses on what social media companies and, in particular, policymakers can do to address them. We borrow a metaphor from the oil industry to clarify our contention: We cannot clean up downstream pollutants like misinformation or dangerous speech without tackling the upstream processes—targeted advertising and algorithmic systems—that make this speech so damaging to our information environment in the first place. Focusing on the downstream effects of the infodemic,¹¹ as has been the approach thus far, does nothing to address its upstream structural causes.

We cannot clean up downstream pollutants like misinformation or dangerous speech without tackling upstream processes like targeted advertising and algorithmic systems.

In the first report, *It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge*, we examined two overarching types of algorithms: 1) content-shaping algorithms that determine what individuals users see when they use a company's online services (including those that target ads) and 2) content moderation algorithms that help human reviewers identify (and sometimes remove) content that violates the company's rules.¹⁰ We then gave examples of how these technologies are used both to propagate and prohibit different forms of online speech (including targeted ads), and showed how they can cause or catalyze social harm, particularly in the context of the 2020 U.S. election. We described how users are profiled, segmented, and targeted in ways that allow advertisers to continually reinforce a specific message to a particular type of audience. We illustrated how, when this capability is combined with mis- or disinformation, such as incorrect voting information or outright lies about a candidate, for political gain, the results can be disastrous for democracy.

We also highlighted what we don't know about these systems. We called on companies to be much more transparent about how their content-shaping algorithms and content moderation systems work, and to give users more control over how content is being prioritized and promoted to them, or targeted at them. We explained why a regulatory focus on holding companies liable for content shared by users, on its own, will not succeed in stemming the spread of problematic content, and will likely result in the violation of users' free expression rights. We agreed that content moderation is necessary, but far from sufficient, and we asserted that the first step in addressing the problem is to require much greater transparency and accountability around a business model that relies on algorithmic curation and exploitation of user data.

Identifying and removing misinformation and disinformation, and otherwise working to mitigate its impact by flagging it as false is an essential short-term measure. But as we pointed out in the previous report, it is important not to force companies to censor higher volumes of content across a broad range of topics, languages, and cultural contexts when their moderation systems lack the accuracy, consistency, and nuance to avoid violating users' right to freedom of expression and information. But infodemics will keep plaguing us—and may get

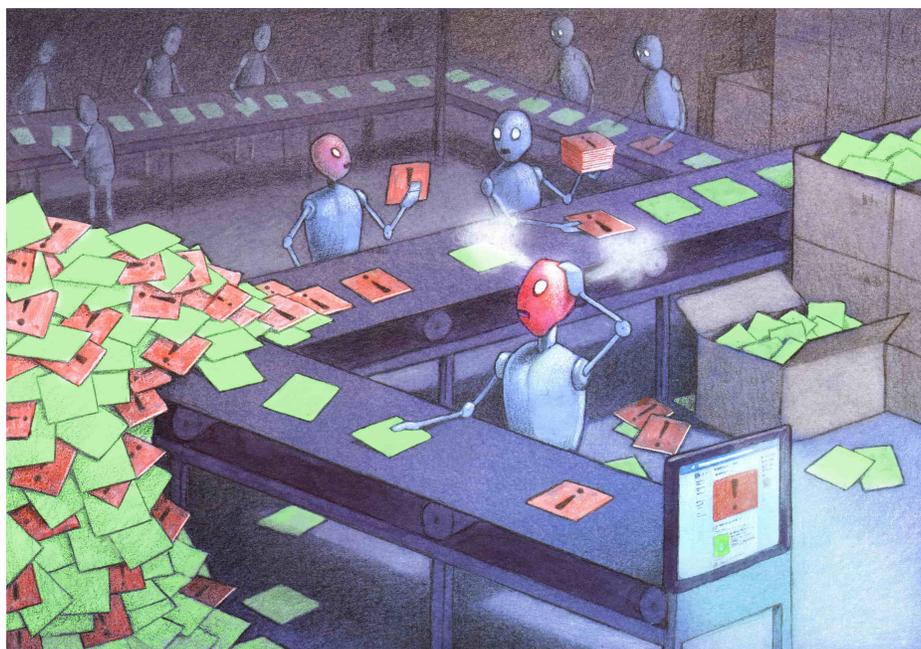
worse—unless Congress acts, and also empowers other stakeholders including institutional investors to hold companies accountable.

Building on five years of research for the Ranking Digital Rights *Corporate Accountability Index* (RDR Index), which evaluates how transparent companies are about their policies and practices that affect online freedom of expression and privacy, this report reinforces the case for adopting a human rights framework for platform accountability and proposes two concrete areas where U.S. Congress needs to act to mitigate the harms of misinformation and other dangerous speech without compromising free expression: federal privacy law and corporate governance reform.

In August 2019, the Business Roundtable published a statement signed by 181 CEOs of the major U.S. corporations, announcing their commitment to the idea that the purpose of business is no longer only to serve shareholders, but also to “create value for all our stakeholders” including employees, customers, and communities.¹² It is no longer debatable whether businesses in any sector should be held accountable for their social impact.

The proliferation of misinformation during the COVID-19 pandemic has shown just how high the human cost—and ultimately the economic cost—can be when companies prioritize shareholder returns over all else, and when the government fails to hold companies accountable to the public interest.¹³ Society is now paying the price for failing to require that companies make credible efforts to understand and track their social impact, and to take responsibility for preventing and mitigating social harms that their business may cause or contribute to. It is time to adjust course and design a resilient and equitable information environment—through increased transparency; responsive, evidence-based regulation; and persistent stakeholder engagement—that protects human rights and civil liberties especially in times of crisis and change.

Targeted Advertising and COVID-19 Misinformation: A Toxic Combination

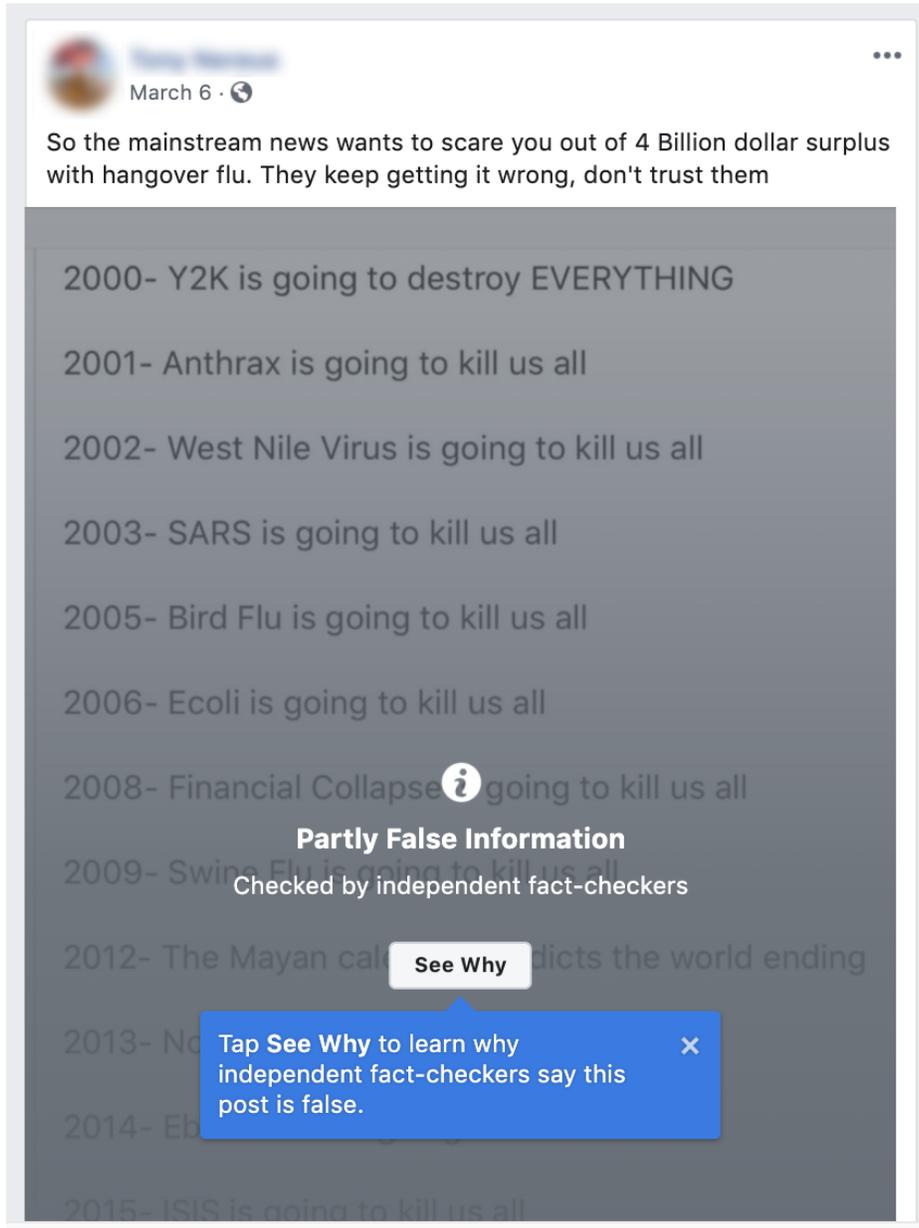


Source: Original art by Paweł Kuczyński

In March, Facebook, Twitter, Google, YouTube, and others committed to join forces and work closely with networks of fact-checkers and researchers to combat the spread of pandemic-related misinformation.¹⁴ In April, as the U.S. economy slowed to a crawl and many state and local governments ordered people to stay home, Facebook took the further step of removing some posts that openly call on people to violate government orders, and committed to display warnings to people who had interacted with misinformation about COVID-19.¹⁵

Yet the torrent of misinformation continued, despite the best efforts of a growing number of organizations dedicated to external monitoring, flagging, and fact-checking. The platforms' content moderation systems could not keep up, and also made mistakes.¹⁶ University of Oxford's Reuters Institute, examining a sample of 225 pieces of misinformation posted between January and the end of March, found that while more than half of the content was either deleted or labeled with warnings, significant amounts of such content remained in circulation.¹⁷ Fifty-nine percent of posts flagged as false by fact-checkers remained on Twitter without any warning labels. Among the tweets that did get deleted was one by Rudy Giuliani, Trump's personal attorney and former mayor of New York City, quoting a well-known conservative activist making the false

claim that “hydroxychloroquine has been shown to have a 100% effective rate treating COVID-19.”¹⁸



Facebook warning label on a fact-checked piece of misinformation related to coronavirus.

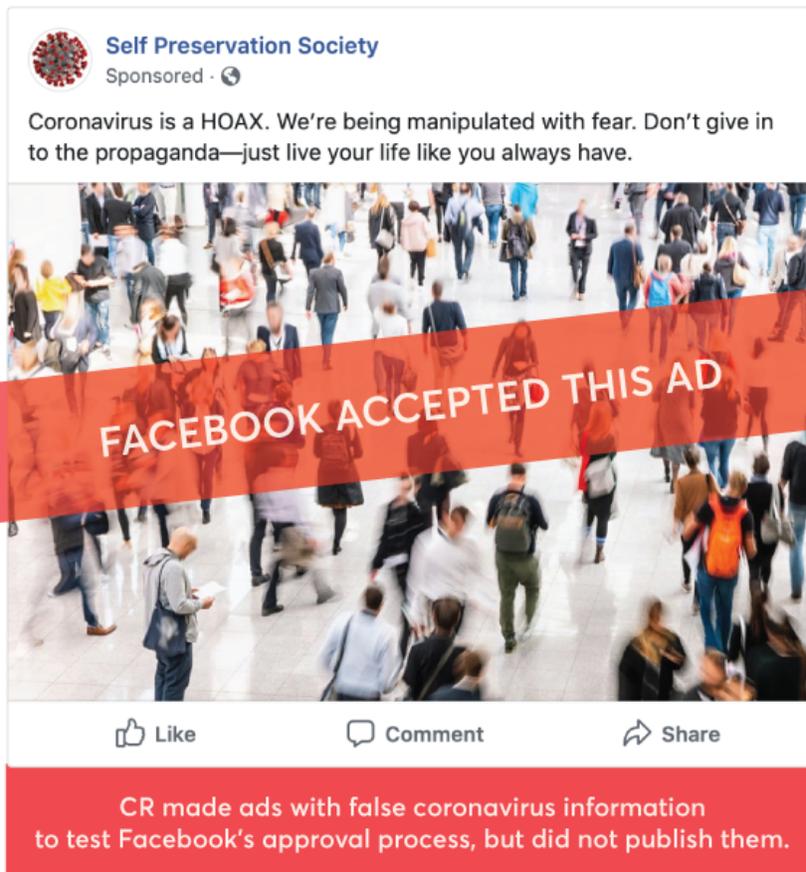
YouTube for its part kept up 27 percent of content flagged as false, while 24 percent of posts containing content that fact-checkers had identified to be false remained on Facebook without warnings of any kind.¹⁹ But what is the actual

prevalence of pandemic-related misinformation across the platforms? Facebook disclosed that in March it had displayed fact-checking labels on 40 million dangerous posts, based on 4,000 articles that its third-party reviewers had rated as false.²⁰ So given the findings from the Oxford sample, we can conclude that millions of pieces of COVID-19 misinformation remained in circulation.

Also by March, fact-checking organizations reported being overwhelmed as the volume of potential misinformation related to the pandemic exploded.²¹ And when governments around the world started issuing mandatory stay-at-home orders to mitigate contagion, the platforms announced that since their human content moderators could no longer work in the office, and most could not work remotely because they lacked home internet access (along with privacy concerns), they would need to rely more heavily on content moderation algorithms to determine what needs to be deleted. They warned that this would likely result in more mistakes being made in determining what content does or does not violate the platform rules.²²

The platforms have also failed to stem the flow of paid misinformation as well as deliberate disinformation. In mid-March, *Consumer Reports* Journalist Kaveh Waddell decided to test the effectiveness of Facebook's commitment to police its ad platform more closely. He created a page for a fake organization, then submitted several advertisements to run on the platform, calling the coronavirus a hoax and urging people to get out of the house and mingle:

“Don't give in to the propaganda—just live your life like you always have,” stated one of the ads. Another instructed people to “stay healthy with SMALL daily doses” of bleach. All were approved by Facebook for publication. Waddell responsibly removed them before they went live.²³



Source: Consumer Reports

A sample ad claiming that COVID-19 is a hoax, created as part of a Consumer Reports investigation, was approved by Facebook despite the platform's commitment to combat misinformation about the pandemic.

Facebook discloses a detailed system for reviewing all ads before they are published for compliance with its policies. Its ad policy states: "We'll check your ad's images, text, targeting, and positioning, in addition to the content on your ad's landing page."²⁴ But the company discloses no further details about what processes or technologies are used to review these ads, including if and how automation is used or if there is any human involvement. Whatever those processes might be, Waddell's experiment exposed just how ineffective Facebook's ad content policing mechanisms actually are in life-and-death crisis situations—such as a global pandemic when people are desperate to understand what is happening and face an overwhelming avalanche of often contradictory information.

Content moderation is a downstream effort by platforms to clean up the mess caused upstream by their own systems designed for automated amplification and audience targeting.

To try to mitigate the devastating effects of targeted misinformation, social media platforms are engaged in an endless circular fight, in which they now must detect and delete content whose social, political, and even medical impact is magnified by the opaque and unaccountable mechanisms of their own business models. Content moderation is a downstream effort by platforms to clean up the mess caused upstream by their own systems designed for automated amplification and audience targeting. These downstream efforts—while necessary—do not fundamentally change the upstream systems that exacerbate the problem, and do not create greater transparency with the public about exactly how targeted systems are shaping what people can share, see, and know.

Take, for example, Facebook’s mechanisms used to build profiles on users and target them with specific content. In April, just a week after Facebook CEO Mark Zuckerberg pledged to fight misinformation about COVID-19, Aaron Sankin, a journalist with *The Markup*, noticed in his Facebook news feed an advertisement for “a hat that would supposedly protect my head from cellphone radiation.”²⁵

One of the many conspiracy theories raging across social media links the spread of the coronavirus to signals emanating from 5G wireless cell towers.²⁶ After clicking the “Why am I seeing this ad?” tab on the ad, Sankin learned that the ad was targeting people interested in “pseudoscience.” We do not know how Facebook determined that Sankin was interested in pseudoscience, what types of advertisers used the audience category, or how often they did so. We do know from information provided to advertisers that the pseudoscience audience category contained 78 million users. With a few more clicks, Sankin was able to use that same category to “boost” *Markup* posts on Instagram (paying to increase how often the posts were shown to Instagram users in the target audience category). The fact that he was able to do so confirmed that Facebook had not disabled it despite its clear connection to misinformation. The audience category was only removed after Sankin brought it to the company’s attention.²⁷

This was not the first time journalists have exposed dangerous audience categories, prompting a company apology and removal. In 2017, *ProPublica* found that racist audience categories were being offered to advertisers.²⁸ Like those

disturbing categories, the pseudoscience audience category was likely generated by an algorithmic system that used a host of data points, like users' Facebook and Instagram posts, comments, and interactions with other posts as well as off-platform data about their personal characteristics and behaviors. On that basis, Facebook determined that these 78 million people were interested in pseudoscience and enabled advertisers to reach them. What's more, in many cases the automated ad targeting systems also determined which paid content was most likely to appeal to pseudoscience enthusiasts. This appears to have been the case for the anti-cell phone radiation hat: the CEO of the company behind the ad told *The Markup* that his team hadn't chosen the pseudoscience category.²⁹

Sankin's experiment suggests that in addition to classifying individual users as "interested in pseudoscience," Facebook's algorithmic systems are also able to determine that specific ads contain pseudoscience. Rather than flagging such ads for further scrutiny by a human reviewer, the company's algorithmic systems make it easier for such ads to reach users who are vulnerable to their messages. A hat that purports to block cell phone radiation may not be likely to cause much harm, but seeing an ad for one reinforces the worldview that creates demands for such products. The same ad-targeting technology also spreads dangerous hoaxes like the idea that consuming bleach protects against the novel coronavirus or that childhood immunizations cause autism, as well as posts that incite hate or violence.

The problem with targeted advertising is that you can't put the cat back in the bag.

The problem with targeted advertising is that you can't put the cat back in the bag. A clear example can be seen in how misinformation radiated from Facebook pages protesting the pandemic lockdown meant to slow the spread of the coronavirus.

In mid-April protesters in state capitols across the country wielded signs with slogans like "#endtheshutdown" and "give me liberty or give me COVID-19!" calling for governors to lift their stay-at-home orders. The protesters were driven by different motives, from economic anxiety at a time of unprecedented unemployment to long-standing fears about government overreach.

OPERATION GRIDLOCK

**SHE'S DRIVING US OUT OF BUSINESS
WE'RE DRIVING TO LANSING**

APRIL 15TH HIGH NOON

APR 15 **Operation Gridlock**
Public · Hosted by Michigan Conservative Coalition and Michigan Freedom Fund

🕒 Wednesday, April 15, 2020 at 12:00 PM EDT
about 2 weeks ago

📍 Michigan State Capitol
110 N Capitol Ave, Lansing, Michigan 48933 [Show Map](#)

4.9K Went · 18K Interested
Share this event with your friends

In April 2020, Michigan gained nationwide attention with anti-lockdown COVID-19 protests that drew hundreds. The protesters were connected and organized through Facebook pages, with the involvement of powerful backers like the National Rifle Association.

Anti-quarantine protest participants may have seen themselves as part of a spontaneous grassroots movement. But the coordinated marketing and messaging around the Facebook pages used to organize the protests was supported by organizations with long histories and deep pockets. Thanks to dogged reporting by several news organizations, it became clear that the emergence and expansion of these protests were made possible in no small part to the support of politically influential, well-funded backers including the National Rifle Association.³⁰

According to research by First Draft, an organization that tracks the spread and analyzes the causes of disinformation, 100 state-specific Facebook pages were created in April to protest state governments' stay-at-home orders. NBC reported that as of April 20, these protest pages were used to organize at least 49 different events. The groups, many with names like "Wisconsinites Against Excessive Quarantine" and "Reopen Minnesota" repeated across Facebook with different state names, had by April 20 attracted more than 900,000 members.³¹ These groups and their members were also reported to be active spreaders of coronavirus misinformation, much of it coordinated. Researchers at Carnegie Mellon University's CyLab Security and Privacy Institute tracked nearly identical claims posted across multiple platforms, from the Facebook groups to Twitter and Reddit.³²

We cannot rely on a game of whack-a-mole to protect public health—and ultimately the health of our democracy.

Frustratingly, it is impossible to document with any precision the scale at which COVID-19 misinformation circulating on social media platforms has been boosted by targeted advertising tools, as the companies keep that information to themselves. In general, the platforms do not disclose nearly enough information about whether the content users see on the platform was boosted, by whom, and whether they are being targeted by tools like Facebook's "custom audiences," which enable advertisers to target specific individuals.

But we do know that a large volume of that misinformation is being shared by followers and administrators of pages that can easily afford to pay for targeted advertising, and that many of these pages are run by people with plenty of experience in using such tools.

Disinformation, misinformation, hate speech, and scams of all sorts are powerful precisely because digital platforms' automated content optimization systems aim them at just the people who are most vulnerable to these messages, while hiding them from other users who would otherwise be in a position to flag them and provide corrective counter-speech. False information about COVID-19, and other dangerous content, would be much less effective if it was not algorithmically targeted and amplified. It is clear that even if social media companies' content rules were perfect—which they are not—enforcing them fairly and accurately at a global scale is not possible.

Banning dangerous content itself is both contrary to free expression standards and impossible to achieve at a global scale. But we can stymie its reach by denying targeting and optimization algorithms their power, through fundamental reforms grounded in human rights principles.

Human Rights: Our Best Toolbox for Platform Accountability

Viewed through the lens of human rights standards, the COVID-19 infodemic is exacerbated by social media platforms' failure to align the full range of their business operations with a commitment to human rights. Over time, their surveillance-based business models can corrode a society's information environment, poisoning the flow of information on which deliberative democracy depends as well as creating the conditions for human rights violations, or worse.

As globally dominant social media platforms, Facebook, Google and Twitter have also played a positive role in advancing global human rights, which is important to acknowledge: They enable free expression and the global free flow of information by providing opportunities for a wide range of speech, about politics, health, and practically anything else. Laudably, they have taken significant, if uneven and imperfect, steps to shield users around the world from acts of government censorship and surveillance that violate human rights.³³ Google and Facebook are both members of the Global Network Initiative (GNI), a multi-stakeholder organization that works with information and communications technology companies to protect users' rights when they receive government demands to delete content, restrict access to service, and provide access to user information that violate international human rights standards for freedom of expression and privacy.³⁴

Yet free speech clearly has a dark side: misinformation can be deadly. Given this contradiction, there is little wonder that these three companies have found themselves at the vortex of heated debates about online speech and democracy.

International human rights standards, grounded in the Universal Declaration of Human Rights (UDHR) as well as the U.S.-ratified International Covenant of Civil and Political Rights, offer a framework for companies to protect and respect the rights of users and communities in a manner that addresses key gaps in U.S. law. The U.S. Constitution is designed primarily to protect people from government abuse: The First and Fourth Amendments forbid government censorship and unlawful search and seizure. But when it comes to how companies' own business decisions affect individuals and society, U.S. law has largely left them off the hook. The law allows commercial social media platforms to moderate and take down content according to their own self-determined rules.³⁵ In essence, U.S. platforms have the right to restrict free expression and shape users' access to information on their platforms without public accountability: The companies can formulate their private rules through an opaque process, change them frequently, and present them in a way that is hard for many users to understand let alone abide by.

U.S. law has largely left companies off the hook when it comes to how their business decisions affect individuals and society.

Congress has over the past century passed many laws that forbid a vast range of abusive, exploitative, or discriminatory corporate behavior. But the question of how to regulate social media has been both difficult and contentious, given the technological, political, and constitutional complexities around anything having to do with speech—or framed as such. In our first report in this two-part series, we argued that changing the law to hold companies liable for content shared by users is not the answer, and due to technical realities that content moderation ultimately clashes with freedom of expression. The problems of private content moderation are compounded by amplification and targeting systems that shape the flow of information to users based on their personal traits or political beliefs. Yet at the same time, the three social media giants have failed to fully respect and protect users' expression and information rights as articulated by international human rights standards. That failure has implications for other rights, including the rights to privacy, nondiscrimination, assembly and association, and economic, social, and cultural rights.

Buttressed by emerging accountability frameworks driven by institutional investors and civil society advocates who are pushing governments to adopt them, international human rights standards apply to companies as well as governments. They offer a corporate accountability toolbox that can be used by policymakers, institutional investors, and other affected stakeholders in any country. Yet, this toolbox has so far been largely overlooked by policymakers seeking to hold companies accountable for their social impact in the United States.

The international human rights toolbox has so far been largely overlooked by U.S. policymakers seeking to hold companies accountable for their social impact.

For social media platforms, the fundamental rights to free expression (UDHR Article 19) and privacy (UDHR Article 12) must be protected and respected so that people can use technology effectively to exercise and defend other political, religious, economic, and social rights. The pandemic further underscores how violations of free expression and information rights can cause or contribute to the violation of other rights, such as right to life, liberty, and security of person (UDHR Article 3). Similarly, violation of the right to privacy can also set off a chain reaction for the violation of other rights, including the human right to non-discrimination (UDHR Article 7, Article 23); freedom of thought (UDHR Article 18); freedom of association (UDHR Article 20); and the right to take part in the government of one's country, directly or through freely chosen representatives (UDHR Article 21).³⁶

The UN Guiding Principles on Business and Human Rights, approved in 2011 and co-sponsored by the U.S. government, has become the gold standard of “guidelines for States and companies to prevent, address and remedy human rights abuses committed in business operations.”³⁷ For the tech sector, applying the principles means respecting users' privacy and freedom of expression, and all other human rights that their business operations may have an impact on—both online and offline. Respecting users' freedom of expression does not preclude a private company establishing rules and moderation processes, or even editorial guidelines related to the purpose and scope of the service (for example, if it is meant to serve a specific community or purpose, such as a platform for members of a given profession). But to be effective, human rights standards must be “implemented transparently and consistently with meaningful user and civil society input,” and must be accompanied by industry-wide oversight and accountability mechanisms.³⁸

Ranking Digital Rights (RDR) offers a dynamic and regularly-updated instruction manual for what steps companies can take today—even in absence of clear regulation—to improve their respect for human rights. Since 2015, the RDR Index has evaluated the world's most powerful digital platforms and telecommunications companies according to their disclosed commitments to respect users' human rights.³⁹ Grounded in the UDHR and the UN Guiding Principles, the RDR Index methodology comprises more than three dozen indicators in three categories: governance, freedom of expression, and privacy. For 2020 we have upgraded the RDR Index methodology, placing greater focus on rights like non-discrimination and the right to life, liberty, and security of person.⁴⁰

The Impact of Targeted Advertising and Algorithmic Systems on Human Rights

In our previous report, we described the growing use of algorithms to moderate content even before the coronavirus outbreak, and how these algorithms make frequent errors that lead to the deletion of journalism, activism, and other speech that does not actually violate the platform rules. We also pointed to data from the past four iterations of the RDR *Corporate Accountability Index*. Only since 2018 have companies started to disclose any data about the volume and nature of content being removed for violating their rules, known variously as terms of service or community guidelines.⁴¹ But their disclosures about content moderation continue to fall very short of what free expression advocates and academic researchers believe is the minimum baseline standard for transparency and accountability as private arbiters of global online speech.⁴²

In late 2019 and early 2020, our research team examined how transparent Facebook, Twitter, and YouTube are about how their automated algorithmic systems determine what users can post and share, what gets removed or blocked for violating the rules, and what information is shown to them most prominently through news feeds and recommendations. As we described in our last report, while Facebook, Google, and Twitter do not hide the fact that they use algorithms to shape content, they disclose little about how the algorithms actually work, what factors influence them, and how users can customize their own experiences.⁴³

Pressure for change is growing with the public health crisis. Concerned that this opacity about what happens to content on platforms could be especially dangerous amidst heated public debates about how best to fight the pandemic without destroying peoples' livelihoods, 75 organizations and researchers released an open letter calling on platforms to preserve information "about what their systems are automatically blocking and taking down." Without such information, according to the nonprofit Center for Democracy and Technology which helped draft the letter, "it will be hard to assess the efficacy of efforts to share vital public health information while combating the spread of coronavirus scams and pandemic profiteering."⁴⁴

To ensure that social media platforms do not contribute to or enable the violation of users' rights, laws and regulations must strictly limit how users can be targeted.

Yet greater transparency alone will not address fundamental problems related to the targeted advertising business model. Companies have experimented with controlling, or being more transparent about, advertisements placed by or in support of political candidates in elections. Facebook now publishes a library of political ads—with a serious flaw in that its political-ad archive depends on political advertisers complying with labeling requirements, and the platforms detecting those that do not. “Currently, dishonest companies can spend an unlimited amount of undeclared money in favor of a political agenda through the Facebook ads platform,” argue the authors of one recent academic paper. Nor does the Facebook Ad Library disclose information about how these advertisers may have deployed targeted advertising tools, or what types of audience characteristics were targeted.⁴⁵

Algorithmic targeting systems only work because the companies that profit from them have access to unfathomable amounts of user data. Google (which owns YouTube), Facebook, Twitter, and other companies whose business models rely on targeted advertising have every incentive to Hoover up every crumb of data they can access, and to create more opportunities to surveil our daily behavior. Thanks to complex automated processes that frequently aren't fully understood even by their own creators, digital platforms can identify the individuals who are most likely to make a purchase, be convinced by a political message, or be susceptible to various types of misinformation. Such manipulation is a form of discrimination, in addition to being a clear violation of freedom of opinion and of information, particularly in the context of elections.⁴⁶

In our first report in this series, we outlined the dangers to democracy when targeted advertising is manipulated for political gain during elections. Election experts have raised concerns that the same technologies and tactics will also be used to spread disinformation about the voting process.⁴⁷ Both user-declared and algorithmically-deduced political leanings can be exploited to target voters with paid, deliberate disinformation about polling places and times or equally damaging but unverifiable claims about an opponent's character or the effects of their policy proposals. This practice, which relies on the processing of vast amounts of user information without explicit consent, violates the right to non-

discrimination by determining what information a user sees based on disclosed or assumed protected traits, such as race, ethnicity, age, gender identity and expression, sexual orientation, health, disability, etc.⁴⁸

But the violation of individual users' rights is not the only harm done. Company practices, incentivized by targeted advertising business models, can also contribute to the violation of the rights of entire communities or categories of people. For example, catering to advertisers' desire to reach potential job applicants who are demographically similar to their current workforce leads digital platforms to enable their advertiser clients to illegally target job ads by gender,⁴⁹ race,⁵⁰ ethnicity,⁵¹ and other protected attributes.⁵²

The human rights risks associated with targeted advertising are clear. To ensure that social media platforms do not contribute to or enable the violation of users' rights, laws and regulations must strictly limit how users can be targeted. They must also require much greater transparency about the nature and design of platforms' algorithmic systems, processes, and business models.

Making All Ads “Honest” Through Transparency, Limited Targeting, and Enforcement

The targeted advertising debate in the United States has focused on the issue of online political advertising, particularly platforms’ responsibility to police the veracity of politicians’ claims, but this narrow focus is misguided, as are the proposed solutions. Aside from the inevitable First Amendment challenges that would arise from any government attempt to force platforms to fact-check political speech, it is doubtful that they would be able to do so accurately and fairly, especially at the scale at which they operate.⁵³

Other rules that govern broadcast and print advertising by political candidates and campaigns do not currently apply online, leaving platforms in the position of setting and enforcing the norms for a growing portion of American electoral discourse. The proposed Honest Ads Act, first introduced in Congress in 2017, would require online advertising platforms to maintain a “public file” database with detailed information about the political ads they serve—similar to existing requirements for broadcast media—including who paid for each ad and how much it cost. Critically, the Honest Ads Act goes beyond platforms’ current voluntary disclosures by including targeting information.⁵⁴ The bill is unlikely to advance before the next election. For the time being, online political advertising is entirely unregulated, leaving platforms to set their own rules.

While Twitter and Google rolled out bans on targeting users by political affiliation in late 2019, Facebook in early January 2020 clarified that it would not follow suit, instead announcing changes that would make its political ad library easier to navigate and granting users somewhat more control over how many political ads they see—albeit on an opt-out basis.⁵⁵ As noted above, these voluntary ad libraries do not include targeting information, a key requirement of the proposed Honest Ads Act.⁵⁶

Thus, as of May 2020, it remains possible to target users with political advertising on Facebook (but not on Twitter or any of Google’s platforms, including YouTube) in three powerful ways. First, individuals can be targeted if advertisers upload custom lists from off-platform data, including voter registration rolls, donor lists to parties and candidates, lists of subscribers to emails from parties and candidates, etc.⁵⁷ Second, platforms can algorithmically generate new audiences that are similar to an uploaded custom list in terms of demographics, interests, and other data points. And third, advertisers can select which audience categories they want to reach, based on audience categories and profiles that Facebook has created from people’s online and offline activities, such as the content they post, the accounts and pages they follow, the content they like or otherwise engage with, their credit card purchases, and the known and/or

inferred political affiliation of the other users they are connected to on the platform.

All three tactics allow political advertisers to send different messages and even contradictory ones to different groups of users. In both 2016 and 2018, African American internet users (African Americans vote overwhelmingly Democratic)⁵⁸ in swing states were targeted with ads designed to suppress voter turnout, whether by providing false information about when, where, and how to vote or by flooding their newsfeeds with negative ads about the advertiser's opponent.⁵⁹ The platforms now prohibit ads that mislead voters about the voting process, but it's unclear how effectively this policy is enforced.

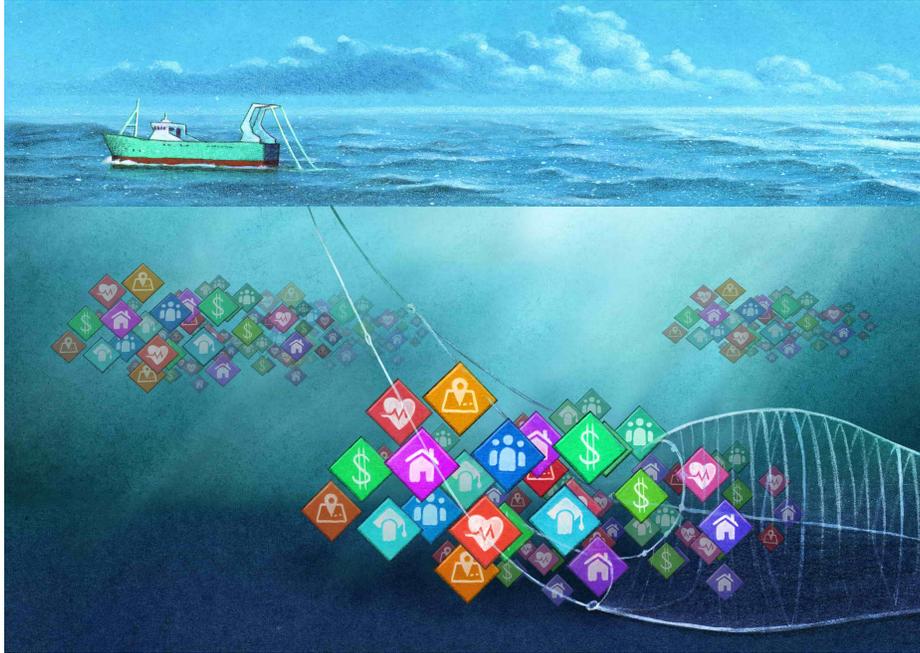
While enacting the Honest Ads Act and limiting targeting for political ads are important and urgent steps, Congress must go beyond the narrow definition of "electioneering communications" to safeguard democracy from algorithmic manipulation by both foreign and domestic actors.⁶⁰ Currently, political advertisers self-identify as such, and there is no way of knowing how many neglect to do so and consequently are not included in the existing ad libraries. Any ad database as required by the Honest Ads Act, would run into the same enforcement problem. Moreover, drawing a clear line around political and issue ads is a vexing conundrum, as the controversy surrounding Twitter's October 2019 decision to ban all political ads demonstrates. CEO Jack Dorsey's initial announcement⁶¹ indicated that issue ads, including those from public-interest organizations, would be covered by the ban, but the final policy issued a few weeks later was more narrow.⁶² No matter where the line is drawn, any database of political ads, as the Honest Ads Act would require, would miss a significant number of politically relevant paid messages, just as the current voluntary ad libraries do. This alone is reason enough to expand the advertising transparency requirement to all online ads.

In addition to these definitional and enforcement issues, the current infodemic has made it clear that ads need not be related to elections to raise serious concerns. Online advertising transparency requirements must go beyond the scope of the Honest Ads Act and include non-political ads as well. This will allow regulators as well as independent researchers to verify that platforms, and their advertisers, are complying with applicable laws and the platforms' own rules. Such transparency would further enable credible, empirical research on the state of online advertising and its impact on political life, public health, and other important issues. Moreover, it would provide crucial oversight over platforms' respect for the law (notably the Civil Rights Act, Fair Housing Act, and various public accommodation laws) and enforcement of their own rules.

As problematic as the rules themselves are, uneven enforcement—by the company of its own rules—exacerbates the extent to which people are being targeted and manipulated in ways that clearly violate users' information and non-discrimination rights. Neither Google, Facebook, nor Twitter include data about

their ad policy enforcement in their transparency reports that disclose data related to the moderation of user-generated content. Recent reporting, including the aforementioned *Consumer Reports* experiment with ads containing clear coronavirus misinformation, demonstrates the inadequacy of Facebook's ad review process. While investigative journalists have not exposed similar failures in Google's or Twitter's ad review systems, this should not be taken as evidence that these systems function well. More oversight is sorely needed, and a universal database for all online advertising would be a key step in that direction.

By Protecting Data, Federal Privacy Law Can Reduce Algorithmic Targeting and the Spread of Disinformation



Source: Original art by Paweł Kuczyński

A strong data privacy law, effectively enforced, can protect internet users from the discrimination inherent to automated content optimization and limit the viral spread of harmful messages. The way to achieve that is by strictly limiting data collection and retention to the absolute minimum that is required to deliver the service to the end-user, irrespective of the company’s business model or financial interests. As Alex Campbell wrote in *Just Security*: “Absent the detailed data on users’ political beliefs, age, location, and gender that currently guide ads and suggested content, disinformation has a higher chance of being lost in the noise.”⁶³

The United States lacks a comprehensive federal privacy law governing the collection, processing, and retention of personal information, though there are sector-specific laws that apply to education, healthcare, and other sectors.⁶⁴ A strong federal privacy law, backed up by robust enforcement mechanisms, is perhaps the strongest tool at Congress’ disposal to stem the tide of online misinformation and dangerous speech by disrupting the algorithmic systems that amplify such content. This approach would also have the benefit of side-stepping the thornier issues related to free speech and the First Amendment.

Even when these companies do disclose what they collect, the scope of what is collected is staggering.

But as things stand, targeted advertising companies are free to collect virtually any information they want to, and use it however it benefits their bottom line. Facebook, Google, and Twitter Hoover up massive amounts of data about internet users (both on their platforms and off). Indeed, not only do platforms track what users do while using their services, they also follow them around the internet and purchase data about the offline behavior from credit card companies and data brokers.⁶⁵ The data that is collected becomes the core ingredient for developing very powerful digital profiles about users that can then be used by advertisers and political operatives to target groups and individuals, like in the pseudoscience example described previously. What's worse, the tech giants do not clearly disclose exactly what they are doing with users' data. In such conditions, the notion of user consent is meaningless.

RDR's evaluation of the three American social media giants' policies and disclosed practices is useful in clarifying just what needs to change, and how the companies should be regulated. Data from the 2019 RDR Index highlights the opacity of the major U.S. digital platforms when it comes to the collection, processing, and sharing of user information. Even when these companies do disclose what they collect, the scope of what is collected is staggering.

Scope and Purpose of Data Collection, Use, and Sharing

In evaluating companies for the RDR Index, we have examined if companies clearly disclose why and how they collect user information, by which we mean any data that is connected to an identifiable person, or may be connected to such a person by combining datasets or utilizing data-mining techniques. We look for a commitment to limit collection of user information to what is directly relevant and necessary to accomplish the purpose of the service from the end user's perspective.⁶⁶ In our evaluation, we do not consider targeted advertising as the purpose of the service: While the revenue it generates enables the company to provide the service, users would get the same benefit if the company made money differently. User information should not be collected for targeted advertising by default, though people can be given a choice to opt in.

Google, Facebook, and Twitter all track users across the internet: Using "cookies" and other tracking technologies embedded in many websites, they

collect data about what web pages people visited and what they have done there (purchased items, watched videos, etc).⁶⁷ The three companies all disclose and explain what types of user information they collect but are less clear about how, and none commit to collecting only data that is necessary to provide the service.⁶⁸ Facebook, for instance, states that it collects “things you do and others do and provide,” including the “content, communications and other information” users provide when using Facebook products (for example when signing up for an account, posting text, videos or images, and using messaging functions). This can include the content of user posts, metadata, and more. Facebook also discloses that it collects device information, including location information. In short: If Facebook can capture a piece of information about you, it does.⁶⁹

All three companies disclose some information about the types of entities they share user data with, but none get more specific. Yet in the context of targeted advertising, it is especially important for companies to disclose to users specifically *who* their information is shared with for any purpose that isn't subject to legitimate law enforcement or national security limitations in accordance with human rights standards.⁷⁰

While no company discloses enough about how they handle user information, Twitter deserves credit for having disclosed more than other U.S. platforms (Google, Facebook, Microsoft, and Apple) about its data handling policies, across all the user information indicators in the 2019 RDR Index.⁷¹

Federal privacy legislation should include strong data minimization and purpose limitation provisions: Users should not be able to opt in to discriminatory advertising or to the collection of data that would enable it.⁷² Any data processing that remains should be opt in. Using the service should not be contingent on giving up more data than that which is necessary to accomplish the purpose of the service. Crucially, the delivery of targeted advertising should not be considered the purpose of the service unless the service's primary purpose is in fact clearly described as such by the company to the general public in its marketing and public communications. Companies should disclose to users and to the relevant regulatory agency what user information they collect, share, retain, and infer; for what purpose; and how long it is retained. Companies should only collect user information from third parties, or share user information with third parties, if the two companies have a vendor-contractor relationship and the sharing of this user information is directly relevant and necessary for the purpose of delivering a service to the user. Companies should allow users to obtain all of their user information (collected and inferred, broadly defined) that the company holds, in a structured data format. They should delete all user information after a user terminates their account or at the user's request. Finally, the accuracy of disclosures and compliance with the above requirements should be independently audited.

Inferred Information and Targeting

In future versions of the RDR Index we will look for the same level of disclosure and commitment about what companies infer about users. Inference is a key way that user profiles are built. Companies perform big data analytics on their troves of collected user data in order to make predictions about the behaviors, preferences, and private lives of their users, and to then sort users into audience categories on that basis.⁷³ Take, for example, the case of Aaron Sankin at *The Markup*. He doesn't know exactly why his account was included in the pseudoscience audience category, but he speculates it was likely because he had conducted research about medical misinformation on Facebook, causing the company's algorithms to assume he had an interest in pseudoscience.⁷⁴

Targeted advertising should be allowed only if the default is that users are not targeted upon joining a service. Companies would be wise to avoid relying on targeted advertising as their sole source of revenue and consider contextual advertising and subscription models, among others. Users must be able to actively opt in to being targeted and able to fully control what information can be used to target them, if any.⁷⁵ Users might choose to be targeted based on certain types of data but not others. Companies should disclose sufficient information to users and to regulators so that people can understand exactly how, why, and by whom they have been targeted, and regulators can track broader patterns to identify abusive practices.

In the first report in this series, we called on companies to publicly explain the content-shaping algorithms that determine what user-generated content users see, and the ad-targeting systems that determine who can pay to influence them. We also called on them to disclose their rules for user content, advertising content, and ad targeting; to explain how they enforce those rules; and to publish regular transparency reports containing data about the actions they take to enforce these rules. We further call on the U.S. Congress to enact legislation to require companies to provide this information to policymakers and the public as a first step toward greater accountability.⁷⁶ These transparency measures are necessary for a more nuanced understanding of a complex and dysfunctional ecosystem but insufficient to the task of making our online ecosystem work for democracy and the public interest. For that, much more active regulatory intervention is needed, starting with the barely regulated targeted advertising industry.

Policymakers should not be convinced by tech giants' claim that targeted advertising benefits internet users by showing them ads that are most relevant to them. Targeted advertising is on by default on Facebook, Google, and Twitter. If users find targeted advertising as useful as companies say they do, many will choose to opt in. While users can customize options for the types of ads they want to see, they can't opt out of receiving tailored ads altogether. In the past year, Facebook has improved its disclosure of options users have to remove categories

of interests and pages they've visited, constituting some but not all of the information used to customize the ads they are seeing. Even when customization is an option, however, the settings can be hard to find.

A federal privacy law should also restrict the targeting options that platforms are allowed to offer to advertisers. Based on our research team's examination of company policy disclosures across Facebook, Google, and Twitter, Facebook appears to have the fewest restrictions on ad targeting and the least transparency. It disclosed that users will be targeted with ads but did not disclose the exact ad targeting parameters that are prohibited. It disclosed that advertisers can tailor ads to custom audiences—lists of individuals that advertisers can upload to the platform—but are prohibited from using these targeting options “to discriminate against, harass, provoke, or disparage users or to engage in predatory advertising practices.”⁷⁷ None of these terms are defined, and the company does not clarify how it would detect breaches of the policy or what the penalty might be for doing so.

In addition to uploading their own custom audience lists, advertisers can also select from among Facebook's algorithmically-determined audience categories, which are based on profiles that Facebook has created from people's online and offline activities. These profiles can include the content a user posts, the accounts and pages they follow, the content they like or otherwise engage with, and the known and/or inferred interests of the other users they are connected to on the platform. These targeting options, however, are only visible when logged into the platform and going through the process of placing ads. As a result, only Facebook account holders who take the time to investigate the platform's audience categories can know what they are. This is how researchers and investigative journalists have discovered the existence of racist⁷⁸ and otherwise problematic audience categories,⁷⁹ alerting public opinion to the dark side of targeted advertising and leading companies to remove the offending categories. Despite calls from civil society (including RDR) to publish the list of available categories, companies have thus far declined to do so, making any kind of systematic oversight impossible.

The Challenge of Effective Enforcement

Privacy law is key to preventing targeted advertising systems from profiling and targeting people in dangerous and harmful ways. But a law is only as good as its enforcement. In that, the EU's challenges in enforcing the General Data Protection Regulation (GDPR) offer important lessons. National-level data protection agencies are under-funded with massive case backlogs, and critics worry that fines are not high enough, nor are other penalties sufficiently punitive, to force a change in industry practices.⁸⁰ Enforcement needs a bigger stick to protect privacy rights.

For example, since the GDPR went into force in 2018, only one major tech giant has been fined for a violation: In early 2019, Google was docked 50 million euros (about \$54 million, which the *New York Times* estimated is about one-tenth of Google's daily sales) for failing to adequately disclose how data is collected across its services for use in targeted advertising.⁸¹ A complaint filed against Facebook in May 2018 by privacy advocate Max Schrems argues that in order for users to even sign onto the company's services (Facebook, Instagram, and WhatsApp), they are forced to agree to having their personal information harvested for targeted advertising. Such "forced consent" is illegal, the complaint argues, if the core purpose of the service is social networking—as the company states—and not targeted advertising.⁸² In contrast to some major multinational Asian and European internet, mobile, and telecommunications companies who disclose that they limit collection of user information to what is directly relevant and necessary to accomplish the purpose of the service, none of the U.S.-based companies evaluated in the 2019 RDR Index (including Facebook) were found to have done so.⁸³ While digital marketers once fretted that the GDPR would render targeted advertising a shadow of its former self, that will only happen if the law is strictly interpreted by courts and enforced.⁸⁴

Whether Congress opts to confer increased authority and funding on the Federal Trade Commission (FTC) to enforce a strong privacy law, or sets up a new data protection agency, the key to success will certainly be strong enforcement authority—backed by adequate funding for the enforcement process.⁸⁵ This is a non-trivial challenge, but should be considered part of the price of protecting democracy.

The Public Interest Principles for Privacy Legislation, published by 34 civil rights, consumer, and privacy organizations in late 2018, set forth baseline objectives that need to be met in order to ensure that a privacy law truly protects the public interest:

- Privacy protections must be strong, meaningful, and comprehensive.
- Data practices must protect civil rights, prevent unlawful discrimination, and advance equal opportunity.
- Governments at all levels should play a role in protecting and enforcing privacy rights.
- Legislation should provide redress for privacy violations.⁸⁶

The Public Interest Principles underscore the importance for individuals to have access to a wide range of redress mechanisms, including the right of private individuals to sue companies for privacy violations. The California Consumer Privacy Act, which grants individuals a private right of action against data

breaches, is now being tested by lawsuits against the videoconferencing platforms Zoom and Houseparty for sharing user data with third parties without consent.⁸⁷ A national privacy law that adheres to the Public Interest Principles would also contain a private right of action, and should meet all other relevant civil rights standards.

Good Content Governance Requires Good Corporate Governance

In our previous report, we called for greater transparency about the processes and technologies that digital platforms use to govern content shared by users, including advertisers. In this report, we have outlined the privacy and data protection measures necessary to lessen content-related harms that are rooted in the algorithmically curated personalization of users' online experiences. We've also pointed out ways that advertising law needs to be upgraded. There is another vector for legislative and regulatory action: To rein in the tech giants' power and hold them accountable to the public interest, lawmakers and policy advocates must prioritize corporate governance and shareholder accountability.

Good corporate governance is a prerequisite for good content governance by social media platforms. In order to identify, prevent, and mitigate social harms caused by the amplification and targeting of dangerous content, Facebook, Google, and Twitter should be subject to strong institutional oversight. Shareholders, a growing number of whom are concerned with companies' social impact and governance, need to be empowered to hold companies responsible for addressing their social and human rights impacts. Shareholder empowerment can in turn strengthen the connection between shareholders and the ecosystem of non-governmental actors—NGOs, unions, consumer advocates, academic researchers, and journalists among others—whose expertise and perspective are essential for companies to be able to fully understand and address their social impact.

Empower Shareholders to Address Environmental, Social, and Governance Issues by Phasing Out Dual-class Shares

The case for shareholder empowerment was on display at Facebook's 2019 annual shareholder meeting. Sixty-eight percent of the company's shareholders who hold normal "Class A" shares (one share, one vote) voted for CEO Mark Zuckerberg to relinquish his position as board chairman to an "independent member of the Board." The supporting statement for the resolution filed by Trillium Asset Management, and backed by a number of well-known mutual fund companies as well as several major state pension funds, called out Facebook management for "missing, or mishandling, a number of severe controversies, increasing risk exposure and costs to shareholders," which board oversight led by an independent board chair might have helped prevent.⁸⁸

Yet even with a solid majority, the shareholder resolution failed. Why? Because Zuckerberg and other members of his inner circle hold "Class B" shares weighted at 10 votes per share, giving him effective control over 60 percent of shareholder

votes at that meeting.⁸⁹ As a result, only 20 percent of the total vote supported separation of CEO and board chair, a major governance reform that would have strengthened the board of directors' power to oversee and potentially overrule the CEO's decisions.⁹⁰

The failed resolution was just one of several proposals spurred by investor concerns that Facebook's management had failed to prevent harms to users and mitigate serious social risks, including privacy breaches and Russian meddling in the 2016 U.S. presidential election.⁹¹ Ironically, one of the other failed resolutions sought to end Facebook's dual-class share structure altogether—filed to call attention to the problem itself, since it could only pass if Zuckerberg agreed to it.⁹²

In 2019, shareholders also filed unsuccessful proposals with Alphabet (Google's parent company), Facebook, and Twitter that would have required the companies to report to shareholders on various aspects of their content governance policies and enforcement. For example, the resolution filed with Alphabet sought a report “reviewing the efficacy of its enforcement of Google's terms of service related to content policies and assessing the risks posed by content management controversies related to election interference, freedom of expression, and the spread of hate speech, to the company's finances, operations, and reputation.” Google responded that its public reporting on these matters was already significant.⁹³ Like Facebook, Alphabet also has a dual-class share structure. Twitter does not.

The shareholder resolutions described above reflect that a growing number of mutual funds and institutional investors pursue environmental, social, and governance (ESG) investment strategies that favor companies that are environmentally sustainable, socially responsible, and well governed. Global sustainable investments jumped by 34 percent to nearly \$40 trillion between 2016 and 2018.⁹⁴ In 2019, nearly half of U.S. institutional investors had either included ESG factors in their investment decisions or were considering doing so.⁹⁵ According to the Sustainable Investments Institute, the percentage of shareholder resolutions addressing ESG issues grew by just 12 percent in the past 10 years, but average support of these resolutions has grown by a whopping 40 percent.⁹⁶ Most important for people concerned with platform accountability, the number of resolutions filed with companies covered by the RDR Index that focused on issues affecting internet users' rights jumped from just two in 2015 to 12 in 2019.⁹⁷

Shareholder resolutions are a tool for investors to push companies in a more sustainable, socially responsible direction and improve their governance.⁹⁸ Even when they do not pass, the attention that they bring to specific issues often prods companies to engage with investors and explain to the public how they are addressing the problems raised. But in cases like the resolution that would have removed Zuckerberg as chairman of the board, resolutions cannot ultimately

curb a CEO's unrestrained power if he is shielded by a dual-class share structure. In 2019, the Securities and Exchange Commission's (SEC) then-Commissioner Robert Jackson, warning of the consequences if CEOs cannot be fired, making them effectively monarchs of private kingdoms, called for reforms. The SEC, he proposed, should require companies to phase out dual-class shares so that shareholders can actually be in a position to hold management accountable for failing to identify and mitigate risks.⁹⁹ The SEC has not only disregarded his recommendation but has moved in the opposite direction, proposing a rule change that would make it harder for shareholders to file proposals.¹⁰⁰ Congress could compel the SEC to implement dual-class share reform and other measures that would strengthen corporate governance and oversight.

Investors Need More and Better Disclosure

Investors concerned with ESG risks are also pushing for companies to disclose more information about how they identify, track, and mitigate these risks. Such disclosures inform portfolio construction, and some investors use it to inform their engagement with companies about how to improve.¹⁰¹ In 2018, a group of investors representing \$5 trillion of assets under management petitioned the SEC to require corporate disclosure of ESG risks, to no avail.¹⁰²

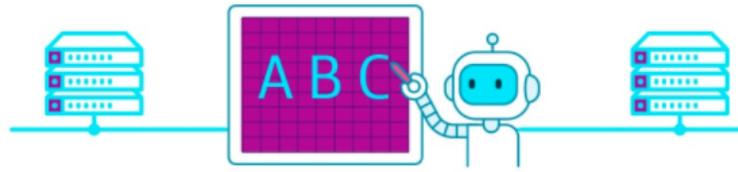
Proponents argue that ESG disclosure requirements would bring the United States into step with broader global trends.¹⁰³ Since 2018, large companies in the EU are required by law to disclose non-financial information about “the way they operate and manage social and environmental challenges,” including human rights-related policies and risks.¹⁰⁴ Meanwhile several organizations have been working to improve the quality of disclosures—whether mandatory or voluntary—by developing clear and consistent standards.¹⁰⁵ Most relevant in the U.S. investment and regulatory context is the San Francisco-based Sustainability Accounting Standards Board (SASB). Their industry-specific reporting standards include guidelines for digital platforms to disclose “data standards, advertising, and freedom of expression,” including a “description of policies and practices relating to behavioral advertising and user privacy.”¹⁰⁶ SASB is now in the early stages of developing disclosure standards related to content moderation.¹⁰⁷

While U.S. companies are not required by law to disclose ESG information, 120 U.S.-listed companies now use SASB reporting standards, including a few in the tech and communications sector, such as Adobe, Netflix, and Salesforce.¹⁰⁸ A handful of companies, including the crafting platform Etsy, are leading the way by furnishing audited SASB-based disclosures along with their official SEC filing documents, even though they are not required to do so. (They also included disclosures using standards developed by the Global Reporting Initiative, which target a broader set of stakeholders beyond investors and are widely used in Europe and internationally.)¹⁰⁹

These companies are responding to market demand: According to the data provider Morningstar, in 2019 a record \$20.6 billion flowed into U.S. sustainable investment funds, almost quadrupling net inflows from 2018.¹¹⁰ Those investment funds need better ESG data in order to make sure that the companies they invest in actually meet basic ESG standards. In January 2020, Larry Fink, the CEO of the global investment management firm Blackrock, called on all companies in which Blackrock invests to follow SASB's standards to disclose relevant ESG information or similar data in a way that is relevant to their business.¹¹¹ If Congress were to compel the SEC to require ESG disclosure, investors would be empowered to push companies to address many of their non-financial risks, including the social impact of targeted advertising and algorithmic systems.

Despite the growing investor demand, Facebook, Google, and Twitter do not systematically include ESG information in their disclosures to investors. Unlike many European telecommunications companies covered by the RDR Index, their annual reports do not cover the full range of social and human rights information that investors have signaled from shareholder resolutions and recent engagements that they consider potentially material. By contrast, Telefónica (headquartered in Spain)—the top-ranking telecommunications company in the 2019 RDR Index—publishes an annual *Consolidated Management Report* covering the full range of ways that the company is working to achieve “value for all our stakeholders.”¹¹² The company's Responsible Business portal offers a clear catalogue of information about how they track and assess impacts, including transparency reports and impact assessment data.¹¹³

TRANSPARENT AND EXPLAINABLE AI



We will be explicit about the kind of personal and/or non-personal data the AI systems uses as well as about the purpose the data is used for. When people directly interact with an AI system, we will be transparent to the users that this is the case.

The Spanish telecommunications giant Telefónica was one of only three companies in the 2019 RDR Index to disclose that it conducts human rights risk assessments on its use of automated decision-making technologies.

The three U.S.-headquartered social media giants that are the focus of this report do disclose a great deal of information related to their social and human rights impacts in a range of policy documents, transparency reports, blog posts, and other materials published online. But the material is scattered across their websites and platforms, testing the research capacity of investors seeking to understand how these companies manage their human rights risks, or how they understand and track their social impact. The RDR Index tracks such disclosures and grades companies according to the comprehensiveness and quality of their disclosures about policies and practices affecting the human rights of internet users. A high score in the RDR Index indicates strong disclosure at least in some areas. But our most recent research found very poor disclosure by these three companies related to the social and human rights impact of their targeted advertising and algorithmic systems.¹¹⁴

A growing number of investors use the RDR Index and its methodology to evaluate company disclosures, and cite RDR data in shareholder resolutions.¹¹⁵ From such resolutions and SASB's standards-development process it is clear that the investor community already has behavioral advertising on its radar and is considering the material risk associated with digital platforms' content moderation practices. The 2020 RDR Index, forthcoming in February 2021, will report on whether these companies have made any progress in their policies and disclosures by then.¹¹⁶

Targeted Advertising Revenue Disclosure

The human rights issues associated with targeted advertising have prompted a growing number of commentators to call for a ban on targeted advertising as the best way to protect privacy and stem the spread of dangerous content.¹¹⁷ At very least, the burden should be on companies that rely on targeted advertising to prove that their business model can be modified to protect human rights and still remain tenable. So far they have failed to do so.

An important step in that direction would be for companies to disclose the extent to which they rely on targeted advertising as a percentage of revenue—as well as whether that percentage is trending up or down. Doing so would help business leaders and investors quantify the driving force behind maintaining these systems as well as the extent of content-related social impact and risks that the business is taking on. Only with this cost-benefit analysis can appropriate steps be taken to identify and mitigate the negative impact of targeted advertising before the problems spiral out of control.

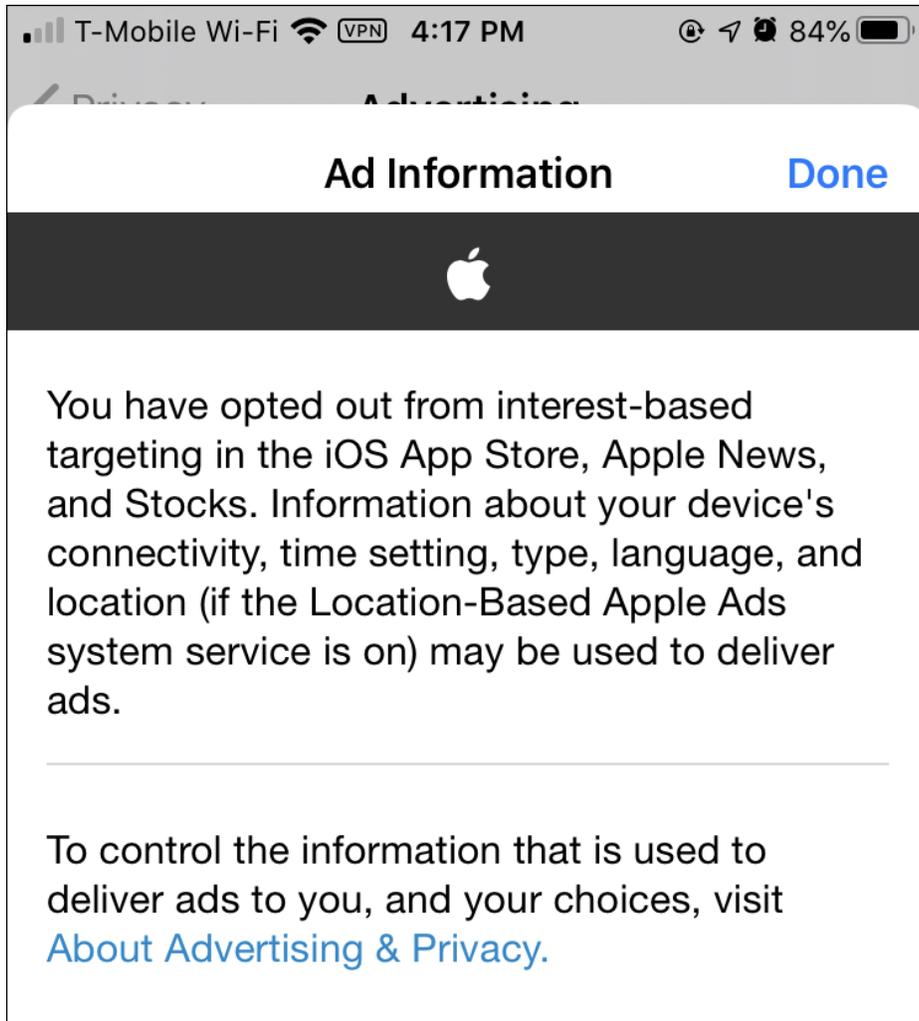
Google and YouTube's parent company, Alphabet, as well as Facebook and Twitter all disclose the percentage of their total revenue earned from advertising in general: In 2019, Facebook disclosed that it earned nearly all of its revenue from advertising (98.5 percent),¹¹⁸ while Twitter earned 86 percent from advertising,¹¹⁹ and Google's advertising revenue (including YouTube) was 83 percent of its total earnings for the year.¹²⁰ None of these companies, however, specifies how much of their revenue was earned from targeted advertising, let alone from different levels of targeting.

For example, Google's AdSense platform offers advertisers several different options, including contextual advertising and behavioral targeting. In contextual advertising, advertisements are linked to the specific keywords or keyphrases in the content alongside which the ads will be shown. For example, a cooking tutorial might be paired with ads for a grocery delivery service or gourmet cookware, regardless of the viewer's demographics or personal behavior.

In behavioral targeting, ads are targeted to specific user characteristics based on profiles that the platform has built about interests, demographics, etc., that users have either declared or that algorithms have inferred after processing user data.¹²¹ But Alphabet doesn't disclose the revenue breakdown for different types of advertising, or whether YouTube depends more heavily on behavioral advertising than other Google-operated platforms such as Search.¹²² Facebook's Advertising for Business page reflects the company's primary focus on behavioral targeting.¹²³

Microsoft and Apple, which rely heavily on other types of revenue like service fees, software license purchases, and hardware sales, do not actually disclose their advertising earnings as a distinct revenue percentage, implying that it is

quite small as a percentage of total revenue.¹²⁴ However, a small share of revenue for such massive companies amounts to serious money: In 2019, Microsoft's Bing search engine generated more than \$7.5 billion dollars in advertising revenue, more than LinkedIn or the Surface hardware line, and three times more than Twitter's total earnings.¹²⁵ As for Apple, it is the only digital platform company in the RDR Index that does not track users across the internet.¹²⁶ While the company's restrained approach to monetizing user data hampers its competitiveness against Google and Facebook, App Store ad revenue still amounted to 13 percent of total revenue for the 2017 fiscal year.¹²⁷



Apple, the only digital platform company in the RDR Index that does not track users across the internet, offers users options to limit targeted advertising.

The bottom line is that advertising, much of it behavioral, is a growing revenue stream for both Apple and Microsoft, creating pressure to collect and monetize

more and more user data.¹²⁸ That trend in turn points to growing social and human rights risks that investors, policymakers, and other civil society stakeholders need to be aware of—and why all companies with targeted advertising revenue should disclose relevant information about it.

Due Diligence: Understanding the Full Scope of Platforms' Social Impact

A key piece of information that investors expect from companies is whether they conduct meaningful and comprehensive due diligence about their ESG risks. Due diligence and impact assessment enables digital platforms to understand the full social impact of their targeted advertising business models, algorithmic systems, and all other processes and activities. Results of impact assessments inform how their policies, systems, and processes need to change in order to mitigate—and ideally prevent—harms to individuals and societies that are either caused or exacerbated by their business operations.

The UN *Guiding Principles on Business and Human Rights* set forth specific elements of due diligence that should guide companies' approach to addressing and mitigating human rights risks. Specifically, Operational Principle 16 states that companies should start by adopting formal policies publicly expressing their commitment to international human rights principles and standards.¹²⁹ A credible public commitment, published in official company documents (not just stated in ad hoc interviews or speeches by executives), confirms that the company, from the board of directors down, is aware of how its actions may affect users and their communities, and is committed to address, minimize, and ideally prevent any negative impacts. A public statement on its own may not amount to much, of course, unless there is verifiable evidence that it has been implemented. But it is the first step toward responsible practice and accountability: It provides a hook for employees, responsible investors, civil society advocates, and others to urge the company's management to implement policies and practices in line with their commitments.

Facebook, Google, and Twitter make official public commitments to users' freedom of expression and privacy, particularly in the face of efforts by governments around the world to censor content or grant access to user data and communications.¹³⁰ The charter of Facebook's new Oversight Board extends a general human rights commitment to content moderation in relation to its own private rules.¹³¹ Yet as of May 2020, Facebook and Twitter have made no explicit, formal commitment to protect human rights as they develop and use algorithmic systems.¹³² While Google does commit to avoid developing "technologies whose purpose contravenes widely accepted principles of international law and human rights," it is not clear whether the company's commitment extends to the human rights implications of algorithmic systems already developed and deployed on

YouTube and other platforms whose purpose is to moderate, amplify, shape, and target content.¹³³

Once a company makes a commitment to respect human rights across all of its business activities, its decision makers can only implement that commitment effectively if they actually understand whose human rights might be affected, and how. Due diligence processes enable the company to gain such an understanding. As the UN Guiding Principles Operating Principle 17 stipulates: “The process should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed.”¹³⁴

Responsible companies that handle user information routinely carry out due diligence and impact assessment to identify security flaws and privacy weaknesses. Security audits are commonplace across the tech sector and legally mandated in many jurisdictions. Privacy impact assessments (PIAs) are now required by law in the EU and a growing number of countries.¹³⁵ In the United States, Facebook, Google, and Twitter have been compelled by FTC consent orders to conduct PIAs in the wake of lapses that provoked complaints by privacy advocates, though as we have discussed in earlier parts of this report, such assessments are by no means adequate to address the negative social impact of the platforms’ exploitation of user information. Members of the GNI (which include Google and Facebook) carry out regular due diligence to identify and mitigate threats to users’ freedom of expression and privacy caused by censorship and surveillance demands that the platforms receive from governments all over the world.¹³⁶ But those assessments do not seek evidence that companies carry out due diligence on human rights threats caused by company actions that are unrelated to government demands or requirements.

Given companies’ lack of transparency around targeted advertisements and their significant financial incentives to deploy the technology quickly, digital platforms’ human rights commitments lack full credibility if they fail to conduct regular and systematic due diligence on their algorithmic systems and targeted advertising business models. Due diligence alone is only credible when accompanied by evidence that companies have a process to revise or implement changes based on their findings.

Responding to longstanding demands from civil rights advocates, in 2018, Facebook initiated an audit of the platform’s impact on marginalized groups and people of color in the United States. The two published updates so far detail the company’s shortcomings with respect to voting rights¹³⁷ and to hate speech, discriminatory ad targeting, the 2020 Census, and civil rights oversight within the company.¹³⁸ The process, led by respected civil rights advocate Laura Murphy, also provided updates on Facebook’s efforts and recommended additional changes. Still, civil rights groups have pointed out that the mere existence of the audit process falls short, however, of what is needed to ensure

that Facebook’s platform is not used to undermine civil rights by facilitating discriminatory targeting and the spread of harmful misinformation that disproportionately harms marginalized groups.¹³⁹

The RDR Index evaluates whether companies conduct regular, comprehensive, and credible due diligence, such as human rights impact assessments, to identify how all aspects of their business affect freedom of expression and privacy and to mitigate any risks posed by those impacts. This includes due diligence pertaining to governments and regulations, to the company’s own policy enforcement processes, and to targeted advertising and algorithmic decision-making systems.

As of May 2020, none of the three social media giants—Google, Facebook, and Twitter—that are the focus of this report series disclosed any evidence that they conduct systematic human rights due diligence or impact assessments around their use of algorithmic systems. Nor do they disclose any impact assessment process to understand how their targeted advertising policies and practices affect human rights, or the social impact of their terms of service governing content, and related enforcement mechanisms.

Only one U.S. company evaluated by the RDR Index—Microsoft—discloses that it conducts impact assessments on its development and use of algorithmic systems.¹⁴⁰ Microsoft, plus Verizon Media, are the only U.S. companies in the RDR Index that disclose impact assessments on their terms of service enforcement.¹⁴¹ As we have highlighted throughout this report, the uneven enforcement of platforms’ content policies contributes to human rights harms, both when dangerous content is left up and when protected speech is erroneously removed. Companies should consider how effectiveness and accuracy of their enforcement processes impact human rights alongside the impact of the rules themselves.

Among the companies covered by the RDR Index, the best examples of strong impact assessment around algorithmic systems and artificial intelligence come from European telecommunications companies. As investors increasingly factor ESG considerations into their decision-making, this raises concerns about U.S. companies’ competitiveness in global financial markets. Telefónica, for example, which operates in multiple European markets and across Latin America, clearly discloses that it assesses the freedom of expression, privacy, and discrimination risks associated with these systems, and that it conducts additional evaluations whenever these assessments identify concerns.¹⁴²

Comprehensive due diligence and risk assessment by European companies prepares them well for future regulatory requirements. In April 2020, a group of 105 international investors representing \$5 trillion in assets under management coordinated by the Investor Alliance for Human Rights called on governments to require companies to conduct ongoing risk assessment and human rights due diligence. They argued that such a step is not only a moral imperative but important for improving public trust in both business and government.¹⁴³

In 2017, in France, a new “duty of vigilance” law went into effect for French multinationals, making strong human rights oversight and risk assessment mandatory.¹⁴⁴ Since then, political momentum has been building across the EU—with direct support even from some multinationals seeking an even regulatory playing field.¹⁴⁵ With proposals for due diligence laws under varying stages of discussion or consideration in 13 European countries, in April 2020, EU Commissioner for Justice Didier Reynders committed to move forward with mandatory environmental and human rights due diligence legislation for EU companies in 2021.¹⁴⁶

The U.S. Congress has taken one small step: In July 2019, the House Financial Services Committee held a hearing to discuss a draft bill to create an annual requirement for public companies to assess and report on their human rights risk exposure. The bill has not been formally introduced.¹⁴⁷ Risks to the rights of users of digital platforms including privacy, information, and non-discrimination were not mentioned in the discussion, nor have they been raised in discussions of potential EU legislation. This gap must be addressed as an important tool for holding digital platforms accountable for all of their human rights impacts, including the social impact of algorithmic systems and targeted advertising business models.

Without Civil Society, Platform Accountability is a Pipe Dream

One of this report's aims has been to suggest how Congress can most constructively and effectively hold digital platforms accountable for the social impact of their targeted advertising business models and algorithmic systems. Passing laws and boosting the power of regulatory agencies are essential steps for strengthening the governance and accountability of digital platforms. But even if law could keep up with technological change, responsive regulation is not possible without the work of a robust and independent civil society.

Key civil society actors include independent social science researchers and investigative journalists, watchdog and grassroots organizations, shareholders and investor alliances, and even allies and employee activists within the companies themselves. Researchers and journalists document and investigate harms while creating an evidence base all stakeholders can access and use to push companies to respond and improve policies and practices. Neither this report series, nor RDR's work more generally, would be possible without the work of these people and organizations, many of whom are cited in our footnotes. The evidence and data that they produce helps advocacy and grassroots organizations, policymakers and investors not only identify what needs to change but also gain the credibility they need to drive the policy formulation, pressure campaigns, and responsible investing standards necessary to change it.

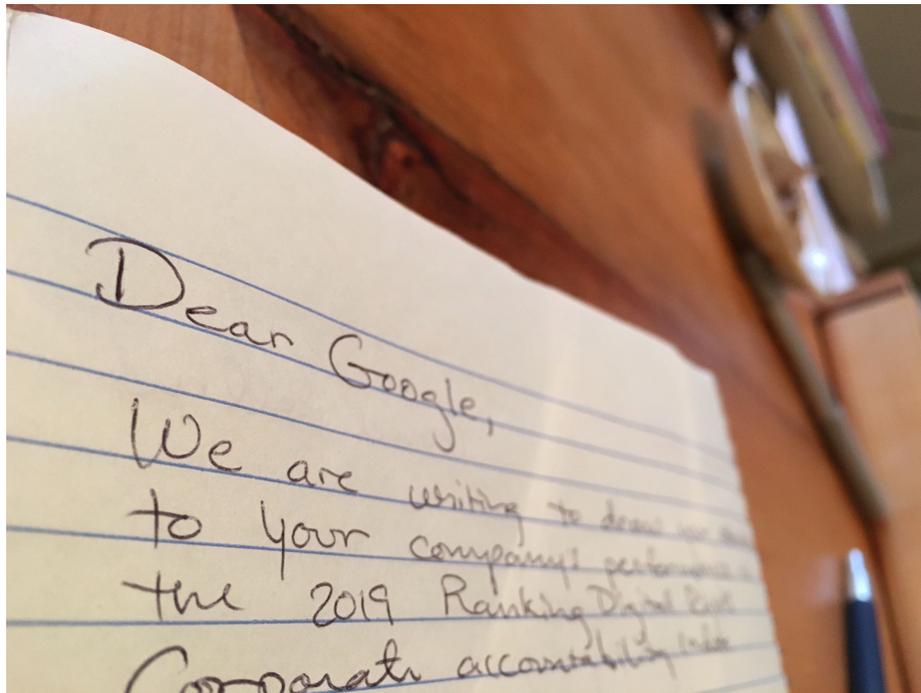
In the absence of effective regulation, independent civil society has an especially vital role to play in developing and deploying accountability mechanisms.

In the absence of effective regulation, independent civil society has an especially vital role to play in developing and deploying accountability mechanisms that fill key gaps where law and regulation have failed to hold companies responsible for their impact on society.

RDR is one of many such efforts, working closely with a network of researchers and civil society advocates and relying heavily on the work of investigative journalists, many of whom have been cited in this report. The RDR Index

methodology, used as the framework for ranking global digital platforms and telecommunications companies on their respect for users' human rights, was informed by two decades of academic research and investigative journalism, as well as by documentation from human rights advocates around the world. This work produced collectively by a broad range of civil society actors over time has clarified exactly how company policies, processes, and practices can affect users' human rights. Once companies are evaluated by the annual RDR Index, civil society advocates use it to call for specific changes by companies and governments. Shareholders use the data to inform their engagement with companies as well as formal shareholder resolutions. This report itself is an example of how the RDR Index and related research can be used by policymakers to guide legal and regulatory reforms.

For social media platforms serious about respecting users' rights and civil liberties and protecting democratic discourse, compliance with laws and engaging with policymakers is not enough. The only way to fully understand how their business operations affect society and users rights, is to consult with a wide range of stakeholders, whether through responding to open letters, participating in dialogue, or joining more formal multi stakeholder processes. For this reason, the RDR Index methodology evaluates companies on whether they engage with a range of stakeholders, particularly with those who face human rights risks in connection with their online activities. Where regulatory gaps exist or where law does not help companies understand their risk and demonstrate to stakeholders that those risks are being adequately addressed, companies should participate in processes and mechanisms through which stakeholders can hold them accountable.



A civil society letter-writing campaign to social media CEOs asked that they incorporate human rights recommendations from the 2019 RDR Index.

Source: Ellery Biddle

At a minimum, RDR researchers look for evidence that a company initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people whose freedom of expression and privacy are directly affected by the company's business. Companies that score well in the RDR Index do more than merely engage with responsible investors, civil society groups, and academic experts about their social impacts and human rights risks. The best performing companies stretch their stakeholder engagement beyond dialogue to accountability by participating in multi-stakeholder initiatives, such as the Global Network Initiative (GNI). Google and Facebook (but not Twitter) are members of GNI, which brings companies together with NGOs, investors, and academics to address the human rights risks related to government censorship and surveillance around the world.¹⁴⁸ As members, they commit to respect and protect users' freedom of expression and privacy in the face of government demands to remove content or hand over user data. As company members, they are also subject to independent assessments, overseen by a multistakeholder board, to determine whether they are satisfactorily upholding their commitments.¹⁴⁹

Because Google and Facebook disclose evidence, verified by independent GNI assessors, that they conduct due diligence on how government demands for user data and content removal affect users' human rights, they score well in the

governance category of the RDR Index compared to many other companies (including Twitter), despite a serious lack of similar due diligence or disclosures related to algorithmic systems and targeted advertising.¹⁵⁰ GNI does *not* address those aspects of the companies' business, however.¹⁵¹

Companies have yet to work with civil society to build multi-stakeholder accountability mechanisms that would address the social and human rights impact of their business operations not related to government censorship and surveillance demands. Companies do engage in multi-stakeholder fora about content moderation and algorithmic systems, but without independent assessments or related accountability mechanisms. Google and Facebook are both members of the Partnership on AI (PAI), where they work with academics and NGOs to address thorny questions related to the ethics of artificial intelligence.¹⁵² While the PAI board includes non-company members, the organization has no mechanisms for accountability; companies are not subject to assessment and they are not held to a clear set of standards, including a commitment to human rights principles, as a condition of membership.

Facebook, Google, and Twitter also engage with a coalition of experts and NGOs who advocate for the Santa Clara Principles on Transparency and Accountability on Content Moderation. All three have endorsed the principles.¹⁵³ But a recent evaluation by New America's Open Technology Institute found that they all fall very short in actually implementing them, disclosing inadequate information about how humans and algorithms moderate content on their platforms.¹⁵⁴ Companies also reach out to experts and NGOs for advice and input on policies, products and programs. For example, Twitter has created a Trust and Safety Council comprising a long list of experts and organizations ranging from the Anti-Defamation League to the Center for Democracy and Technology to the National Center for Missing and Exploited Children.¹⁵⁵ Such engagement is at the companies' invitation and on their terms.

To date, the most talked-about attempt at stakeholder engagement has been the launch of the Facebook Oversight Board. Funded and staffed by an independent trust, the Oversight Board brings together an international group of experts who are tasked with adjudicating Facebook's most difficult and controversial content moderation cases.¹⁵⁶ Given the extraordinary complexity and sensitivity of the issues it will consider and the platform's global reach, Facebook's willingness to open up its content moderation processes and decisions to world-class external expertise deserves praise. Still, the Oversight Board oversees only decisions related to content removal. It does not have a say in the company's business decisions, not least Facebook's targeted advertising business model.¹⁵⁷ While decisions about individual content cases will be considered binding, Zuckerberg is under no obligation to heed broader concerns its members may raise about targeted advertising and algorithmic systems. Thus the launch of the Oversight Board does nothing to change the need to hold the company accountable through

strong privacy law, anti-trust enforcement, due diligence and transparency requirements, and corporate governance reforms. Rather, it serves as another reminder that effective corporate accountability mechanisms must involve multiple actors applying pressure at various points and, most important, cannot be self-designed or self-enforced.

Holding companies accountable to the public interest is the responsibility of lawmakers, in consultation with civil society. In the next section, we outline our recommendations for concrete actions Congress should take to address the current corporate accountability gap.

Key Recommendations for Policymakers

The recommendations below call on the U.S. Congress to take legislative action to pass a federal privacy law, update advertising regulations, mandate corporate disclosure and due diligence requirements, and institute governance reform. They build on research conducted for the RDR *Corporate Accountability Index*, as well as our experience working with advocacy groups and investors seeking to hold social media platforms accountable for their social impact. They are in addition to the recommendations for corporate transparency around content shaping and moderation published at the end of the first report in this two-part series.¹⁵⁸

Enact federal privacy law that protects people from the harmful impact of targeted advertising. A comprehensive federal privacy law should encompass much more than the following recommendations, which focus on necessary rules to limit the reach of misinformation and dangerous content by limiting the power and precision of content-shaping and ad-targeting algorithms.

1. Designate an existing federal agency, or create a new agency, to enforce privacy and transparency requirements applicable to digital platforms.

The agency should be given the necessary authority and funding to accomplish its mission.

2. Enact strong data-minimization and purpose limitation provisions.

Users should not be able to opt-in to discriminatory advertising or to the collection of data that would enable it

3. Give users very clear control over collection and sharing of user information that is not otherwise prohibited, including inferred information, that is not necessary to deliver and operate the service.

- Companies should disclose to users and to the relevant regulatory agency what user information they collect, share, and infer; and for what purpose, and how long it is retained. This information should be independently audited. *“User information” is any data that is connected to an identifiable person, or may be connected to such a person by combining datasets or utilizing algorithmic data-processing techniques.*
- Companies should not collect user information from third parties, or share user information with third parties, unless the companies in question have a vendor/contractor relationship and the sharing of this user information is disclosed and directly relevant and necessary for the purpose of delivering a service to the user. *The “purpose of the service” does not include targeted advertising unless the service’s primary purpose is in fact*

clearly described as such by the company to the general public in its marketing and public communications.

- Companies should allow users to obtain all of their user information (collected and inferred) that the company holds, in a structured data format.
- Companies should delete all user information within a reasonable timeframe after users terminate their account or at the user's request. This should be independently audited.

4. Restrict how companies are able to target users.

- Companies should not enable advertisers to use their services to target specific individuals by using personally identifying information.
- Companies should not be allowed to enable advertisers to target users on the basis of any audience category or profile attribute without active user consent.
- Any ad targeting should only take place on the basis of information that is voluntarily disclosed by the user directly within the platform itself, otherwise known as first-party data. (For example, users might specify the language(s) in which they prefer to see ads, their broad geographic region, which sports teams they support, or self-select into broad audience categories including by subscribing to an advertiser's updates.)
- Companies should ensure that the combination of the advertising content and the targeting category does not amount to discrimination on the basis of one or more protected classes recognized under civil rights law.

Require that platforms maintain a public ad database to ensure compliance with all privacy and civil rights laws when engaging in ad targeting. Transparency is a prerequisite for accountability. Congress should pass the Honest Ads Act, expand its scope to include all types of online advertisements, thus mandating a universal database of advertisements, and enable regulators and researchers to audit it.

1. Pass the Honest Ads Act: Platforms should be required to maintain a “public file” database with detailed information about the political ads they serve, similar to existing requirements for broadcast media, including a digital copy of the advertisement, a description of the audience the advertisement targets, the number of views generated, the dates and times of publication, the rates charged, and the contact information of the purchaser.

2. Expand the online advertising database to include all types of ads:

Platforms should be required to expand the database that would be required by the Honest Ads Act to all online ads.

Require relevant disclosure and due diligence. Companies should be required to disclose information that demonstrates they are tracking the social impact of their targeted advertising and algorithmic systems, taking necessary steps to mitigate risk and prevent social harm.

1. Require targeted advertising revenue disclosure: All companies offering digital services and advertising should be required to disclose the percentage of revenue generated by targeted advertising.

2. Require ESG disclosures: Companies should be required to disclose non-financial information about their environmental, social, and governance (ESG) impacts, including information about the social impact of targeted advertising and algorithmic systems. Reporting should be formal, systematic, and comparable. (See Part 1 for more detailed disclosure recommendations related to algorithmic systems.)

3. Require due diligence: Companies should be required to conduct assessments of their social impact and risks, including human rights risks associated with targeted advertising and algorithmic systems.

Strengthen corporate governance and oversight. In line with the ESG and due diligence disclosures recommended above, Congress should require that Securities and Exchange Commission (SEC) rules empower shareholders to hold company leadership accountable for social impact.

1. Require companies to phase out dual-class share structures: Once a reasonable but not excessive period of time has passed after a company's IPO, dual class shares should be phased out.

2. Do not make it harder to file shareholder resolutions: The SEC should scrap proposed rule changes that will make it more difficult for shareholders to file proposals and to get them on proxy ballots.

The best way for companies to prepare for future regulation—and more important, to demonstrate maximum respect for users' human rights—is to align their policies, practices, and disclosures with the indicators outlined in the RDR *Corporate Accountability Index* methodology.¹⁵⁹

Conclusion

With a global pandemic in the run-up to a U.S. presidential election, it is now undeniable that strengthening platform accountability is critical to the future of democracy.

Despite intensifying efforts to remove potentially deadly misinformation and other dangerous speech, social media companies are still failing to effectively moderate content—paid and user-generated alike—in ways that are consistent with their human rights obligations and the protection of civil liberties. At the same time, policymakers have proposed holding these companies liable for their users' speech rather than for their targeted advertising business models, the fundamental source of the problem.

The threats have been identified. Now the question is: How are social media platforms preparing to counter them?

In the first part of this two-part series, we warned against recent proposals to revoke or dramatically revise Section 230 of the 1996 Communications Decency Act (CDA), which protects companies from liability for content posted by users on their platforms. Such a step would be counter-productive. Policymakers should instead focus on reining in social media companies' targeted advertising business model and the algorithmic systems that drive it. These upstream processes, which require the collection and sharing of vast amounts of user data to target users without their clear knowledge and consent, are the driving force in the spread and discriminatory targeting of downstream disinformation, hate speech, and other content that can endanger both public health and democratic discourse.

At the end of the first report, we made specific recommendations for corporate transparency about social media platforms' advertising content rules and ad-targeting systems, as well as their rules and processes for governing user-generated content. We called for greater corporate transparency about what happens under the hood, to enable an informed public debate about whether to regulate the algorithms themselves, and if so, how.¹⁶⁰ If the companies will not make such disclosures voluntarily, Congress should mandate them.

In this second report, we have described how companies have failed to stop the downstream torrent of COVID-19 misinformation despite throwing extra resources at the problem and strengthening cooperation with fact-checkers and independent security researchers. Infodemics will continue to plague society—and may get worse—unless and until companies make changes to the upstream systems that play a major role in driving them. If companies had made these changes voluntarily, we would have seen stricter and more responsible data use policies and practices, greater transparency, due diligence, and much stronger corporate oversight.

Strong privacy law is urgently needed to curb the negative social impact of targeted advertising business models. Regulation of political advertising must be upgraded for the era of online campaigning. Social media companies should be required to show evidence that they conduct tangible and credible due diligence around their social impacts and risks. They must disclose key categories of information necessary for external stakeholders to understand how companies are working to understand and address their risks. Corporate governance and oversight requirements must be strengthened. Shareholders must be empowered to hold companies accountable for their social impact. In turn, shareholders need to be sufficiently informed and engaged in order to understand the risks.

Time is running out for Congress to act in time to have an impact on social media's next big test: the November 2020 general election. In addition to the potential harms to democratic discourse, misinformation can also undermine the democratic process. As states shift to the widespread use of absentee ballots in an effort to protect voters during COVID-19, experts warn of disinformation about how and when to vote.¹⁶¹ They also warn us to expect that reports of any mistakes or incompetence by local election officials will be taken out of context, conflated and combined with misinformation, and used in organized attempts by bad actors to destroy the legitimacy of the presidential election result, potentially throwing the country into political uncertainty and conflict.¹⁶²

Commitments to prioritize the removal of election-related disinformation and misinformation, similar to commitments they have made to address the COVID-19 infodemic, would certainly be a start. But such steps will be insufficient—for all the reasons this report series has documented—unless more fundamental changes are made to the platforms' algorithmic systems and targeted advertising mechanisms.

What if Facebook, Google, and Twitter committed to limit targeted advertising to the same demographic categories—such as geographic area—to which print and broadcast advertisers have access?

What if they stopped allowing any advertisers to target individuals until after the November election?

What if they all agreed to stop all targeted advertising for three months prior to the election, offering contextual advertising only?

Such measures would dramatically reduce the flow and impact of election-related disinformation and misinformation on social media.

“What if Facebook, Google, and Twitter stopped allowing any advertisers to target individuals until after the November election?”

If social media companies will not commit to a full moratorium on targeted advertising for a few months, they should nonetheless commit to take strong action that prioritizes the health of democracy over their 2020 financial returns. Facebook, Google, and Twitter should commission rapid impact assessments, in collaboration with independent experts on elections and social media, to identify the greatest threats posed by disinformation and misinformation to the 2020 presidential election. The assessments should then recommend concrete changes to their targeted advertising, data collection and use policies, and algorithmic systems that can be made in time to mitigate those threats.¹⁶³ The results and recommendations should be made public, with enough time to implement a remedy.

The companies should then announce a plan for how they will change specific policies, advertising features, mechanisms, and privacy defaults in order to minimize the amplification, targeting, and overall impact of disinformation, misinformation, and other dangerous content in these final critical months leading up to the election.

While that may not solve the problem for the long term, it would be an important start to a broader national discussion about how social media platforms can best protect users' rights and how our elected representatives and regulators can set effective rules for these companies to help safeguard our democracy.

Notes

- 1 Newsguard. 2020. *Tracking Twitter's COVID-19 Misinformation "Super-Spreaders."* <https://www.newsguardtech.com/twitter-super-spreaders/> (May 15, 2020).
- 2 Khalid, Amrita. 2019. "Americans Can't Stop Relying on Social Media for Their News." *Quartz*. <https://qz.com/1720695/pew-study-shows-more-americans-rely-on-social-media-for-news/> (May 15, 2020).
- 3 Sterling, Greg. 2019. "Almost 70% of Digital Ad Spending Going to Google, Facebook, Amazon, Says Analyst Firm." *Marketing Land*. <https://marketingland.com/almost-70-of-digital-ad-spending-going-to-google-facebook-amazon-says-analyst-firm-262565> (May 17, 2020).
- 4 Gibson, Kate. 2020. "Spending on U.S. Digital Political Ads to Top \$1 Billion for First Time." *CBS News*. <https://www.cbsnews.com/news/spending-on-us-digital-political-ads-to-cross-1-billion-for-first-time/> (May 15, 2020).
- 5 Conger, Kate. 2019. "Twitter Will Ban All Political Ads, C.E.O. Jack Dorsey Says." *The New York Times*. <https://www.nytimes.com/2019/10/30/technology/twitter-political-ads-ban.html> (May 15, 2020).
- 6 Gary, Jeff, and Ashkan Soltani. 2019. "First Things First: Online Advertising Practices and Their Effects on Platform Speech." *Knight First Amendment Institute*. <https://knightcolumbia.org/content/first-things-first-online-advertising-practices-and-their-effects-on-platform-speech> (February 13, 2020).
- 7 Maréchal, Nathalie, and Ellery Roberts Biddle. 2020. *It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge - A Report from Ranking Digital Rights*. Washington, D.C.: New America. <http://newamerica.org/oti/reports/its-not-just-content-its-business-model/> (May 7, 2020).
- 8 Wardle, Claire, and Hossein Derakhshan. 2017. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg: Council of Europe. Council of Europe report. <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research-168076277c>
- 9 Dangerous Speech Project. 2016. "What Is Dangerous Speech?" *Dangerous Speech Project*. <https://dangerspeech.org/about-dangerous-speech/> (May 15, 2020).
- 10 Maréchal, Nathalie, and Ellery Roberts Biddle. 2020. *It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge - A Report from Ranking Digital Rights*. Washington, D.C.: New America. <http://newamerica.org/oti/reports/its-not-just-content-its-business-model/> (May 7, 2020).
- 11 The World Health Organization (WHO) defines an infodemic as "an over-abundance of information—some accurate and some not—that makes it hard for people to find trustworthy sources and reliable guidance when they need it." See World Health Organization. 2020. *Novel Coronavirus (2019-NCov) Situation Report - 13*. Geneva: World Health Organization. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf?sfvrsn=195f4010_6
- 12 Business Roundtable. 2019. "Business Roundtable Redefines the Purpose of a Corporation to Promote 'An Economy That Serves All Americans.'" <https://www.businessroundtable.org/business-roundtable-redefines-the-purpose-of-a-corporation-to-promote-an-economy-that-serves-all-americans> (May 15, 2020).
- 13 Goodman, Peter S. 2020. "Big Business Pledged Gentler Capitalism. It's Not Happening in a Pandemic. - The New York Times." *The New York Times*. <https://www.nytimes.com/2020/04/13/business/business-roundtable-coronavirus.html> (May 15, 2020).

- 14 Douek, Evelyn. 2020. "COVID-19 and Social Media Content Moderation." *Lawfare*. <https://www.lawfareblog.com/covid-19-and-social-media-content-moderation> (May 15, 2020).
- 15 Romm, Tony. 2020. "Facebook Will Alert People Who Have Interacted with Coronavirus 'Misinformation.'" *Washington Post*. <https://www.washingtonpost.com/technology/2020/04/16/facebook-will-alert-people-who-have-interacted-with-coronavirus-misinformation/> (May 15, 2020).
- 16 Heilweil, Rebecca. 2020. "Facebook Is Flagging Some Coronavirus News Posts as Spam." *Vox*. <https://www.vox.com/recode/2020/3/17/21183557/coronavirus-youtube-facebook-twitter-social-media> (May 15, 2020).
- 17 Brennen, J. Scott, Felix Simon, Philip N. Howard, and Rasmus Kleis Nielsen. 2020. *Types, Sources, and Claims of COVID-19 Misinformation*. Oxford: University of Oxford. <https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation> (May 15, 2020).
- 18 Wong, Queenie. 2020. "Twitter Leaves up Trump's 'liberate' Tweets about States with Lockdown Protests." *CNET*. <https://www.cnet.com/news/twitter-leaves-up-trumps-liberate-tweets-about-states-protesting-coronavirus-lockdowns/> (May 15, 2020).
- 19 Brennen, J. Scott, Felix Simon, Philip N. Howard, and Rasmus Kleis Nielsen. 2020. *Types, Sources, and Claims of COVID-19 Misinformation*. Oxford: University of Oxford. <https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation> (May 15, 2020).
- 20 Rosen, Guy. 2020. "An Update on Our Work to Keep People Informed and Limit Misinformation About COVID-19." *Facebook Newsroom*. <https://about.fb.com/news/2020/04/covid-19-misinfo-update/> (May 7, 2020). Romm, Tony. 2020. "Facebook Will Alert People Who Have Interacted with Coronavirus 'Misinformation.'" *Washington Post*. <https://www.washingtonpost.com/technology/2020/04/16/facebook-will-alert-people-who-have-interacted-with-coronavirus-misinformation/> (May 15, 2020).
- 21 Leskin, Paige. 2020. "One of the Internet's Oldest Fact-Checking Organizations Is Overwhelmed by Coronavirus Misinformation — and It Could Have Deadly Consequences." *Business Insider*. <https://www.businessinsider.com/coronavirus-snoops-misinformation-fact-checking-overwhelmed-deadly-consequences-2020-3> (May 15, 2020).
- 22 Bergen, Mark, Joshua Brustein, and Sarah Frier. 2020. "Tech's Shadow Workforce Sidelined, Leaving Social Media to the Machines." *Bloomberg*. <https://www.bloomberg.com/news/articles/2020-03-30/covid-19-impact-on-social-media-contractors-can-t-work-from-home> (May 15, 2020).
- 23 Waddell, Kaveh. 2020. "Facebook Approved Ads With Coronavirus Misinformation." *Consumer Reports*. <https://www.consumerreports.org/social-media/facebook-approved-ads-with-coronavirus-misinformation/> (May 15, 2020).
- 24 Facebook. n.d. "Advertising Policies." <https://www.facebook.com/policies/ads/#> (May 15, 2020).
- 25 Sankin, Aaron. 2020. "Want to Find a Misinformed Public? Facebook's Already Done It." *The Markup*. <https://themarkup.org/coronavirus/2020/04/23/want-to-find-a-misinformed-public-facebooks-already-done-it> (May 7, 2020).
- 26 Satariano, Adam, and Davey Alba. 2020. "Burning Cell Towers, Out of Baseless Fear They Spread the Virus." *The New York Times*. <https://www.nytimes.com/2020/04/10/technology/coronavirus-5g-uk.html> (May 15, 2020).
- 27 Sankin, Aaron. 2020. "Want to Find a Misinformed Public? Facebook's Already Done It." *The Markup*. <https://themarkup.org/coronavirus/2020/04/23/want-to-find-a-misinformed-public-facebooks-already-done-it> (May 7, 2020).

- 28 Julia Angwin, Madeleine Varner. 2017. "Facebook Enabled Advertisers to Reach 'Jew Haters.'" *ProPublica*. <https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters> (February 12, 2020).
- 29 Sankin, Aaron. 2020. "Want to Find a Misinformed Public? Facebook's Already Done It." *The Markup*. <https://themarkup.org/coronavirus/2020/04/23/want-to-find-a-misinformed-public-facebooks-already-done-it> (May 7, 2020).
- 30 Bixby, Scott. 2020. "DeVos Has Deep Ties to Michigan Protest Group, But Is Quiet On Tactics." *The Daily Beast*. <https://www.thedailybeast.com/devos-has-deep-ties-to-michigan-protest-group-but-is-quiet-on-tactics> (May 5, 2020); Stanley-Becker, Isaac, and Rony Romm. 2020. "Pro-Gun Activists Using Facebook Groups to Push Anti-Quarantine Protests." *Washington Post*. <https://www.washingtonpost.com/technology/2020/04/19/pro-gun-activists-using-facebook-groups-push-anti-quarantine-protests/> (May 15, 2020).
- 31 Zadrozny, Brandy, and Ben Collins. 2020. "Conservative Activist Family behind 'Grassroots' Anti-Quarantine Facebook Events." *NBC News*. <https://www.nbcnews.com/tech/social-media/conservative-activist-family-behind-grassroots-anti-quarantine-facebook-events-n1188021> (May 15, 2020).
- 32 Seitz, Amanda. 2020. "Virus Misinformation Flourishes in Online Protest Groups." *Associated Press*. <https://apnews.com/5862a9201c7b1bea62069a9c5e5fbb1c> (May 15, 2020).
- 33 Crocker, Andrew et al. 2019. Who Has Your Back? Censorship Edition 2019. Electronic Frontier Foundation. <https://www.eff.org/wp/who-has-your-back-2019> (May 16, 2020).
- 34 Global Network Initiative. 2020. "Global Network Initiative." Global Network Initiative. <https://globalnetworkinitiative.org/> (May 16, 2020).
- 35 Specifically by Section 230 of the 1996 Communications Decency Act. For more, see Maréchal, Nathalie, and Ellery Roberts Biddle. 2020. It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge - A Report from Ranking Digital Rights. Washington, D.C.: New America. <http://newamerica.org/oti/reports/its-not-just-content-its-business-model/> (May 7, 2020).
- 36 Ranking Digital Rights. 2019. *Human Rights Risk Scenarios: Targeted Advertising, Consultation Draft*. Washington, D.C.: New America. <https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf>
- 37 OHCHR. 2011. *Guiding Principles on Business and Human Rights: Implementing the United Nations "Respect, Protect and Remedy" Framework*. Geneva: United Nations Office of the High Commissioner on Human Rights. http://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_en.pdf
- 38 U.N. Human Rights Council. 2018. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. A/HRC/38/35, 14*. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement> Kaye, David. 2019. *Speech Police: The Global Struggle to Govern the Internet*. New York: Columbia Global Reports.
- 39 Ranking Digital Rights. 2019. *Corporate Accountability Index*. Washington, D.C.: New America. <https://rankingdigitalrights.org/index2019/>
- 40 Ranking Digital Rights. 2020. *2020 Ranking Digital Rights Corporate Accountability Index Draft Indicators*. Washington, DC: New America. <https://rankingdigitalrights.org/2020/04/15/2020-draft-methodology/>
- 41 Frenkel, Sheera. 2018. "Facebook Says It Deleted 865 Million Posts, Mostly Spam." *The New York Times*. <https://www.nytimes.com/2018/05/15/>

technology/facebook-removal-posts-fake-accounts.html (May 16, 2020).

42 Singh, Spandana. 2019. *Assessing YouTube, Facebook and Twitter's Content Takedown Policies*. Washington, D.C.: New America. <http://newamerica.org/oti/reports/assessing-youtube-facebook-and-twitters-content-takedown-policies/> (May 16, 2020).

43 Ranking Digital Rights. 2020. *The RDR Corporate Accountability Index: Transparency and Accountability Standards for Targeted Advertising and Algorithmic Systems — Pilot Study and Lessons Learned*. Washington, D.C.: New America. www.rankingdigitalrights.org/pilot-report-2020

44 Llansó, Emma J. 2020. "Understanding Automation and the Coronavirus Infodemic: What Data Is Missing?" *Center for Democracy and Technology*. <https://cdt.org/insights/understanding-automation-and-the-coronavirus-infodemic-what-data-is-missing/> (May 16, 2020). Radsch, Courtney J. 2020. "CPJ, Partners Call on Social Media and Content Sharing Platforms to Preserve Data." <https://cpj.org/blog/2020/04/cpj-partners-call-on-social-media-and-content-shar.php> (May 16, 2020).

45 Silva, Márcio et al. 2020. "Facebook Ads Monitor: An Independent Auditing System for Political Ads on Facebook." In *Proceedings of The Web Conference 2020*, Taipei, Taiwan: ACM, 224–34. <https://dl.acm.org/doi/10.1145/3366423.3380109> (May 16, 2020).

46 Information collected for targeted advertising purposes enables companies and advertisers to segment audiences in a very granular manner, tailoring messages to very specific attributes including preferences, habits, or traits. As this data is shared across the targeted advertising ecosystem, this in turn enables discrimination against internet users on the basis of protected traits and even the targeting of specific individuals. For more on the relationship between targeted advertising business models and discrimination, see Ranking Digital

Rights. 2019. *Human Rights Risk Scenarios: Targeted Advertising, Consultation Draft*. Washington, D.C.: New America. <https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf>

47 Hasen, Richard L. 2020. "What Happens in November If One Side Doesn't Accept the Election Results?" *Slate*. <https://slate.com/news-and-politics/2020/03/2020-election-meltdown-coronavirus-delay.html> (May 16, 2020).

48 U.N. General Assembly. (1948). *Universal Declaration of Human Rights* (217 [III] A), Article 2. Paris. <https://www.un.org/en/universal-declaration-human-rights/>

49 Tobin, Ariana, and Jeremy B. Merrill. 2018. "Facebook Is Letting Job Advertisers Target Only Men." *ProPublica*. <https://www.propublica.org/article/facebook-is-letting-job-advertisers-target-only-men> (May 11, 2020).

50 Angwin, Julia, and Terry Parris Jr. 2016. "Facebook Lets Advertisers Exclude Users by Race." *ProPublica*. <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race> (May 11, 2020).

51 Tobin, Ariana. 2018. "Facebook Promises to Bar Advertisers From Targeting Ads by Race Or..." *ProPublica*. <https://www.propublica.org/article/facebook-promises-to-bar-advertisers-from-targeting-ads-by-race-or-ethnicity-again> (May 11, 2020).

52 Ranking Digital Rights. 2019. *Human Rights Risk Scenarios: Targeted Advertising, Consultation Draft*. Washington, D.C.: New America. <https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf>

53 For a discussion of this point, see Maréchal, Nathalie, and Ellery Roberts Biddle. 2020. *It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge - A Report*

from *Ranking Digital Rights*. Washington, D.C.: New America. <http://newamerica.org/oti/reports/its-not-just-content-its-business-model/> (May 7, 2020).

54 Honest Ads Act, S. 1989, 115th Congress, 2017.

55 Associated Press. 2020. “Facebook Refuses to Restrict Untruthful Political Ads and Micro-Targeting.” *The Guardian*. <https://www.theguardian.com/technology/2020/jan/09/facebook-political-ads-micro-targeting-us-election> (May 16, 2020).

56 However, Reddit’s recently introduced Political Ads Transparency Community does include targeting information. See Singh, Spandana. 2020. “Reddit’s Intriguing Approach to Political Advertising Transparency.” *Slate*. <https://slate.com/technology/2020/05/reddit-political-advertising-transparency.html> (May 18, 2020).

57 The same data is used for direct mail, get-out-the-vote door-knocking, phone canvassing, and email blasts. See National Conference of State Legislatures. 2019. “Access To and Use Of Voter Registration Lists.” <https://www.ncsl.org/research/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.aspx> (May 17, 2020).

58 Laird, Chryl, and Ismael White. 2020. “Why So Many Black Voters Are Democrats, Even When They Aren’t Liberal.” *FiveThirtyEight*. <https://fivethirtyeight.com/features/why-so-many-black-voters-are-democrats-even-when-they-arent-liberal/> (May 16, 2020).

59 Romm, Tony. 2018. “How Facebook and Twitter Are Rushing to Stop Voter Suppression Online for the Midterm Elections.” *Washington Post*. <https://www.washingtonpost.com/technology/2018/11/02/how-facebook-twitter-are-rushing-stop-voter-suppression-online-midterm-election/> (May 17, 2020).

60 The Federal Election Commission defines “electioneering communications” as “persons, groups of persons or organizations, including corporations

and labor organizations, may make electioneering communications. See Federal Election Commission. n.d. “Electioneering Communications.” *FEC.gov*. <https://www.fec.gov/help-candidates-and-committees/other-filers/electioneering-communications/> (May 16, 2020).

61 Jack Dorsey (@jack). 2019. “‘We’ve Made the Decision to Stop All Political Advertising on Twitter Globally. We Believe Political Message Reach Should Be Earned, Not Bought. Why? A Few Reasons...’ / Twitter.” <https://twitter.com/jack/status/1189634360472829952> (May 16, 2020).

62 Twitter. n.d. “Political Content.” <https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html> (May 16, 2020).

63 Campbell, Alex. 2019. “How Data Privacy Laws Can Fight Fake News.” *Just Security*. <https://www.justsecurity.org/65795/how-data-privacy-laws-can-fight-fake-news/> (May 16, 2020).

64 The California Consumer Privacy Act (CCPA), which took effect on January 1 and will be enforced starting in July, may de facto apply to much of the country, as many companies may find it more expedient to extend the rights that the CCPA confers on California residents to those in other states.

65 Madrigal, Alexis C. 2012. “I’m Being Followed: How Google—and 104 Other Companies—Are Tracking Me on the Web.” *The Atlantic*. <https://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/> (May 17, 2020).

66 Organisation for Economic Cooperation and Development. 2013. *The OECD Privacy Framework*. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (May 17, 2020).

67 Ranking Digital Rights. 2019. *Corporate Accountability Index*. Indicator P9: Collection of user

information from third parties. Washington, D.C.: New America. <https://rankingdigitalrights.org/index2019/indicators/p9/>

68 Ranking Digital Rights. 2019. *Corporate Accountability Index*. Indicator P3: Collection of user information. Washington, D.C.: New America. <https://rankingdigitalrights.org/index2019/indicators/p3/>

69 Facebook. 2018. "Data Policy." https://www.facebook.com/full_data_use_policy (May 16, 2020).

70 *Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance*. 2014. <https://necessaryandproportionate.org/principles>

71 Ranking Digital Rights. 2019. *Corporate Accountability Index*. Washington, D.C.: New America. <https://rankingdigitalrights.org/index2019/>

72 Laroia, Gaurav, and David Brody. 2019. "Privacy Rights Are Civil Rights. We Need to Protect Them." *Free Press*. <https://www.freepress.net/our-response/expert-analysis/insights-opinions/privacy-rights-are-civil-rights-we-need-protect-them> (May 18, 2020).

73 Wachter, Sandra. 2019. *Affinity Profiling and Discrimination by Association in Online Behavioural Advertising*. Rochester, NY: Social Science Research Network. SSRN Scholarly Paper. <https://papers.ssrn.com/abstract=3388639> (February 11, 2020).

74 Sankin, Aaron. 2020. "Want to Find a Misinformed Public? Facebook's Already Done It." *The Markup*. <https://themarkup.org/coronavirus/2020/04/23/want-to-find-a-misinformed-public-facebooks-already-done-it> (May 7, 2020).

75 Regulating so-called "dark patterns" would help ensure that consent is freely given. See Darlington, Alexander. "Dark Patterns." <https://www.darkpatterns.org/> (May 17, 2020).

76 Maréchal, Nathalie, and Ellery Roberts Biddle. 2020. *It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge - A Report from Ranking Digital Rights*. Washington D.C.: New America. <http://newamerica.org/oti/reports/its-not-just-content-its-business-model/> (May 7, 2020).

77 Facebook. n.d. "Advertising Policies." <https://www.facebook.com/policies/ads/#> (May 15, 2020). In contrast, see National Fair Housing Alliance. 2019. "Facebook Settlement." <https://nationalfairhousing.org/facebook-settlement/> (May 17, 2020).

78 Julia Angwin, Madeleine Varner. 2017. "Facebook Enabled Advertisers to Reach 'Jew Haters.'" *ProPublica*. <https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters> (March 16, 2020).

79 Sankin, Aaron. 2020. "Want to Find a Misinformed Public? Facebook's Already Done It." *The Markup*. <https://themarkup.org/coronavirus/2020/04/23/want-to-find-a-misinformed-public-facebooks-already-done-it> (May 7, 2020).

80 Satariano, Adam. 2020. "Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates." *The New York Times*. <https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html> (May 16, 2020).

81 Satariano, Adam. 2019. "Google Is Fined \$57 Million Under Europe's Data Privacy Law." *The New York Times*. <https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html> (May 16, 2020).

82 NOYB. n.d. "Forced Consent (DPAs in Austria, Belgium, France, Germany and Ireland)." [noyb.eu](https://noyb.eu/en/project/forced-consent-dpas-austria-belgium-france-germany-and-ireland). <https://noyb.eu/en/project/forced-consent-dpas-austria-belgium-france-germany-and-ireland> (May 16, 2020). Lomas, Natasha. 2018. "Facebook, Google Face First GDPR Complaints over 'Forced Consent.'" *TechCrunch*. <https://social.techcrunch.com/>

2018/05/25/facebook-google-face-first-gdpr-complaints-over-forced-consent/ (May 16, 2020).

83 Ranking Digital Rights. 2019. *Corporate Accountability Index*. Indicator P3: Collection of user information. Washington, D.C.: New America. <https://rankingdigitalrights.org/index2019/indicators/p3/>. Also see section 5.3, Privacy Gaps: <https://rankingdigitalrights.org/index2019/report/privacy/#section-53>.

84 Naidu, Prash. 2019. "Why Advertisers Are Staring down the Barrel of Big GDPR Fines." *Marketing Week*. <https://www.marketingweek.com/advertisers-gdpr-fines/> (May 16, 2020).

85 Rich, Jessica. 2019. "Opinion | Give the F.T.C. Some Teeth to Guard Our Privacy." *The New York Times*. <https://www.nytimes.com/2019/08/12/opinion/ftc-privacy-congress.html> (May 16, 2020).

86 U.S. PIRG. 2018. "Public Interest Privacy Principles." <https://uspig.org/resources/usp/public-interest-privacy-principles> (May 16, 2020).

87 JD Supra. 2020. "Privacy Suits Against Zoom and Houseparty Test the CCPA's Private Right of Action." *Data Security Law Blog*. <https://www.jdsupra.com/legalnews/privacy-suits-against-zoom-and-90966/> (May 16, 2020).

88 Trillium Asset Management. 2019. "Facebook, Inc. - Independent Board Chairman (2019)." <https://trilliuminvest.com/shareholder-proposal/facebook-inc-independent-board-chairman-2019/> (May 16, 2020). Key supporters listed at: <https://trilliuminvest.com/institutional-investors-renew-call-for-an-independent-board-chair-at-facebook-as-controversies-continue-unabated/>

89 Wolverton, Troy. 2018. "At Facebook's Annual Meeting, Mark Zuckerberg Stuck to His Talking Points — and Ignored Some of Shareholders' Biggest Concerns." *Business Insider*. <https://www.businessinsider.com/facebook-shareholder-meeting-mark-zuckerberg-2018-5> (May 16, 2020).

90 Fitzgerald, Meghan. 2019. "Why 68% of Facebook Investors Voted to Oust Zuckerberg as Chairman." *Yahoo! Finance*. <https://finance.yahoo.com/news/why-68-percent-of-facebook-investors-voted-to-oust-zuckerberg-as-chairman-222950866.html> (May 16, 2020).

91 Mayer, Jane. 2018. "How Russia Helped Swing the Election for Trump." *The New Yorker*. <https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump> (May 17, 2020).

92 Stewart, Emily. 2019. "Facebook Will Never Strip Away Mark Zuckerberg's Power." *Vox*. <https://www.vox.com/recode/2019/5/30/18644755/facebook-stock-shareholder-meeting-mark-zuckerberg-vote> (May 16, 2020).

93 Alphabet. 2019. *Notice of 2019 Annual Meeting of Stockholders and Proxy Statement*. "Proposal Number 16: Stockholder Proposal Regarding a Report on Content Governance." U.S. Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1652044/000130817919000205/lgoog2019_def14a.htm#lgooga075

94 Chasan, Emily. 2019. "Global Sustainable Investments Rise 34 Percent to \$30.7 Trillion." *Bloomberg.com*. <https://www.bloomberg.com/news/articles/2019-04-01/global-sustainable-investments-rise-34-percent-to-30-7-trillion> (May 16, 2020).

95 Callan Institute. 2019. *2019 ESG Survey*. <https://www.callan.com/wp-content/uploads/2019/09/2019-ESG-Survey.pdf>

96 Sustainable Investments Institute. 2020. *Proxy Preview 2020 Shows Jump in ESG Shareholder Proposals as SEC Prepares to Restrict Shareholder Rights*. Press release. <https://siinstitute.org/press-release.php?id=37> (May 16, 2020).

97 MacKinnon, Rebecca, Melissa Brown, and Jasmine Arooni. 2020. *Digital Rights 2020 Outlook: Market Realities and Regulation Are Raising the Bar*.

Washington, D.C.: New America. <https://rankingdigitalrights.org/wp-content/uploads/2020/01/Winter-2020-Investor-Update.pdf>

98 Mooney, Attracta. 2020. "Coronavirus Forces Investor Rethink on Social Issues." *Financial Times*. <https://www.ft.com/content/bc988e0e-687c-4c72-98eb-ae2595e29bee> (May 16, 2020).

99 SEC Commissioner Robert J. Jackson, Jr. 2018. "SEC.Gov | Perpetual Dual-Class Stock: The Case Against Corporate Royalty." Presented at San Francisco, CA. <https://www.sec.gov/news/speech/perpetual-dual-class-stock-case-against-corporate-royalty> (May 16, 2020).

100 Setty, Ganesh. 2019. "Shareholders Would Have Tougher Time Submitting Resolutions under SEC's Proposed Rule." *CNBC*. <https://www.cnbc.com/2019/11/05/rule-change-would-make-it-harder-to-submit-shareholder-resolutions.html> (May 16, 2020).

101 World Economic Forum. 2020. *Embracing the New Age of Materiality: Harnessing the Pace of Change in ESG*. White paper. www3.weforum.org/docs/WEF_Embracing_the_New_Age_of_Materiality_2020.pdf

102 Williams, Cynthia A. et al. 2018. Letter to the Secretary of the Securities and Exchange Commission Brent J. Fields. U.S. Securities and Exchange Commission. <https://www.sec.gov/rules/petitions/2018/petn4-730.pdf>

103 Clancy, Heather. 2019. "Investor Interest Fuels SASB Adoption, Inspires New GRI Tax Disclosure Standard | GreenBiz." *GreenBiz*. <https://www.greenbiz.com/article/investor-interest-fuels-sasb-adoption-inspires-new-gri-tax-disclosure-standard> (May 16, 2020).

104 European Commission. "Non-Financial Reporting." *European Commission - European Commission*. <https://ec.europa.eu/info/business->

[economy-euro/company-reporting-and-auditing/company-reporting/non-financial-reporting_en](https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting/non-financial-reporting_en) (May 16, 2020).

105 Rozen, Miriam. 2020. "Ethical Investors Want More Proof of Good Deeds." *Financial Times*. <https://www.ft.com/content/5c943b66-5a22-11ea-abe5-8e03987b7b20> (May 16, 2020).

106 Sustainability Accounting Standards Board. "Standards Overview." <https://www.sasb.org/standards-overview/> (May 16, 2020). Sustainability Accounting Standards Board. 2018. *Internet Media & Services Sustainability Accounting Standard*. Industry standard. https://www.sasb.org/wp-content/uploads/2018/11/Internet_Media_Services_Standard_2018.pdf

107 Waters, Greg. 2019. "SASB to Research Content Moderation on Internet Platforms." *Sustainability Accounting Standards Board*. <https://www.sasb.org/blog/sasb-to-research-content-moderation-on-internet-platforms/> (May 16, 2020).

108 Sustainability Accounting Standards Board. "Companies Reporting with SASB Standards." <https://www.sasb.org/company-use/sasb-reporters/> (May 16, 2020).

109 Ashwell, Ben. 2019. "More than 100 Companies Using SASB Standards." *IR Magazine*. <https://www.irmagazine.com/reporting/more-100-companies-using-sasb-standards> Mirchandani, Bhakti. 2019. "Finally a Way to Assure Sustainability and Impact! Vornado, Etsy, and LeapFrog Lead the Charge." *Forbes*. <https://www.forbes.com/sites/bhaktimirchandani/2019/12/09/finally-a-way-to-assure-sustainability-and-impact--vornado-etsy-and-leapfrog-lead-the-way/> (May 16, 2020).

110 Flood, Chris. 2020. "Record Sums Deployed into Sustainable Investment Funds." *Financial Times*. <https://www.ft.com/content/2a6c38f7-4e4b-411b-b5e6-96b36e597cfc> (May 16, 2020).

111 Fink, Larry. 2020. "A Fundamental Reshaping of Finance." *BlackRock*. <https://www.blackrock.com/corporate/investor-relations/larry-fink-ceo-letter> (May 16, 2020).

112 Telefónica. 2019. *Summary Consolidated Management Report 2019*. <https://www.telefonica.com/documents/153952/13347920/2019-Telefonica-Consolidated-Management-Summary-Report.pdf/e08d1803-95f4-6a36-e0f7-ff1257541d47>

113 Telefónica. "Responsible Business in Telefónica." <https://www.telefonica.com/en/web/responsible-business/the-responsible-business-in-telefonica> (May 16, 2020).

114 Ranking Digital Rights. 2020. *The RDR Corporate Accountability Index: Transparency and Accountability Standards for Targeted Advertising and Algorithmic Systems — Pilot Study and Lessons Learned*. Washington D.C.: New America. www.rankingdigitalrights.org/pilot-report-2020

115 MacKinnon, Rebecca. 2019. "Investors Urge Companies to Use the RDR Index to Improve Their Respect for Users' Digital Rights." *Ranking Digital Rights*. <https://rankingdigitalrights.org/2019/01/15/investors-urge-companies-to-use-rdr-index/> (May 16, 2020).

116 Ranking Digital Rights. 2020. *2020 Ranking Digital Rights Corporate Accountability Index Draft Indicators*. Washington, D.C.: New America. <https://rankingdigitalrights.org/2020/04/15/2020-draft-methodology/>

117 Edelman, Gilad. 2020. "Why Don't We Just Ban Targeted Advertising?" *Wired*. <https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/> (May 16, 2020). Lomas, Natasha. 2019. "Twitter's Political Ads Ban Is a Distraction from the Real Problem with Platforms | TechCrunch." *Tech Crunch*. <https://techcrunch.com/2019/11/02/twitters-political-ads-ban-is-a-distraction->

[from-the-real-problem-with-platforms/?guccounter=1](https://techcrunch.com/2019/11/02/twitters-political-ads-ban-is-a-distraction-from-the-real-problem-with-platforms/?guccounter=1) (May 16, 2020).

118 Facebook. 2020. *Facebook Reports Fourth Quarter and Full Year 2019 Results*. Press release. <https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results/default.aspx> (May 16, 2020).

119 Twitter. 2020. *Fiscal Year 2019 Annual Report*. Press release. https://s22.q4cdn.com/826641620/files/doc_financials/2019/q4/Q4-2019-Earnings-Press-Release.pdf

120 Alphabet. 2020. *Alphabet Announced Fourth Quarter and Fiscal Year 2019 Results*. Press release. https://abc.xyz/investor/static/pdf/2019Q4_alphabet_earnings_release.pdf?cache=79552b8

121 Google. n.d. "How Ads Are Targeted to Your Site." *AdSense Help*. <https://support.google.com/adsense/answer/9713?hl=en> (May 16, 2020).

122 Google. n.d. "About Targeting for Video Campaigns." *YouTube Help*. <https://support.google.com/youtube/answer/2454017?hl=en> (May 16, 2020).

123 Facebook. n.d. "Help Your Ads Find the People Who Will Love Your Business." *Facebook for Business*. <https://www.facebook.com/business/ads/ad-targeting> (May 16, 2020).

124 Apple. 2019. *Apple Reports Fourth Quarter Results*. Press release. <https://www.apple.com/newsroom/2019/10/apple-reports-fourth-quarter-results/> (May 16, 2020). Microsoft. *Earnings Release FY20 Q1*. Press release. <https://www.microsoft.com/en-us/Investor/earnings/FY-2020-Q1/press-release-webcast> (May 16, 2020).

125 Ovide, Shira. 2019. "Bing's Not the Laughingstock of Technology Anymore." *Bloomberg*. <https://www.bloomberg.com/opinion/articles/>

2019-05-30/microsoft-s-bing-is-not-the-laughingstock-of-technology-anymore (May 7, 2020).

126 Ranking Digital Rights. 2019. *Corporate Accountability Index*. Indicator P9: Collection of user information from third parties. Washington, D.C.: New America. <https://rankingdigitalrights.org/index2019/indicators/p9/>

127 Mickle, Tripp, and Georgia Wells. 2018. "Apple Looks to Expand Advertising Business with New Network for Apps." *Wall Street Journal*. <https://www.wsj.com/articles/apple-looks-to-expand-advertising-business-with-new-network-for-apps-1527869990> (May 7, 2020).

128 Slefo, George P. 2019. "Apple's Ad Business Borrows a Page from Facebook." <https://adage.com/article/digital/apple-s-ad-business-borrows-a-page-facebook/316762> (May 7, 2020). Monllos, Kristina. 2019. "'Reclaim a Seat at the Table': Microsoft Is Diversifying Its Advertising Business." *Digiday*. <https://digiday.com/marketing/reclaim-seat-table-microsoft-diversifying-advertising-business/> (May 7, 2020).

129 OHCHR. 2011. *Guiding Principles on Business and Human Rights: Implementing the United Nations "Respect, Protect and Remedy" Framework*. Geneva: United Nations Office of the High Commissioner on Human Rights. http://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_en.pdf

130 Ranking Digital Rights. 2019. *Corporate Accountability Index*. Indicator G1: Policy commitment. Washington, D.C.: New America. <https://rankingdigitalrights.org/index2019/indicators/g1/>

131 Facebook. 2019. *Oversight Board Charter*. https://about.fb.com/wp-content/uploads/2019/09/oversight_board_charter.pdf

132 Ranking Digital Rights. 2020. *The RDR Corporate Accountability Index: Transparency and Accountability Standards for Targeted Advertising*

and Algorithmic Systems — Pilot Study and Lessons Learned. Washington, D.C.: New America. www.rankingdigitalrights.org/pilot-report-2020

133 Ranking Digital Rights. 2020. *The RDR Corporate Accountability Index: Transparency and Accountability Standards for Targeted Advertising and Algorithmic Systems — Pilot Study and Lessons Learned*. Washington, D.C.: New America. www.rankingdigitalrights.org/pilot-report-2020

134 OHCHR. 2011. *Guiding Principles on Business and Human Rights: Implementing the United Nations "Respect, Protect and Remedy" Framework*. Geneva: United Nations Office of the High Commissioner on Human Rights. http://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_en.pdf

135 GDPR.EU. 2018. "Data Protection Impact Assessment (DPIA)." *GDPR.eu*. <https://gdpr.eu/data-protection-impact-assessment-template/> (May 16, 2020).

136 Global Network Initiative. 2020. *The GNI Principles at Work: Public Report on the Third Cycle of Independent Assessments of GNI Company Members 2018/2019*. <https://globalnetworkinitiative.org/wp-content/uploads/2020/04/2018-2019-PAR.pdf>

137 Sandberg, Sheryl. 2018. "An Update on Our Civil Rights Audit." *Facebook Newsroom*. <https://about.fb.com/news/2018/12/civil-rights-audit/> (May 11, 2020).

138 Sandberg, Sheryl. 2019. "A Second Update on Our Civil Rights Audit." *Facebook Newsroom*. <https://about.fb.com/news/2019/06/second-update-civil-rights-audit/> (May 11, 2020).

139 Scurato, Carmen. 2019. *Facebook vs. Hate: An Analysis of Facebook's Work to Disrupt Online Hate and the Path to Fully Protect Users*. Free Press. https://www.freepress.net/sites/default/files/2019-09/facebooks_vs_hate_free_press_report.pdf

140 Ranking Digital Rights. 2020. *The RDR Corporate Accountability Index: Transparency and Accountability Standards for Targeted Advertising and Algorithmic Systems — Pilot Study and Lessons Learned*. Washington, D.C.: New America. www.rankingdigitalrights.org/pilot-report-2020

141 See Governance section, Ranking Digital Rights. 2019. *Corporate Accountability Index*. Washington, D.C.: New America. <https://rankingdigitalrights.org/index2019/report/governance/#section-33>

142 Telefónica. 2018. *Integrated Management Report 2018*. <https://www.telefonica.com/documents/153952/13347920/Telefonica-Integrated-Management-Report-2018.pdf>

143 Investor Alliance for Human Rights. 2019. *The Investor Case for Mandatory Human Rights Due Diligence*. https://investorsforhumanrights.org/sites/default/files/attachments/2020-04/The%20Investor%20Case%20for%20mHRDD%20-%20FINAL_3.pdf

144 Altschuller, Sarah A., and Amy Lehr. 2017. “The French Duty of Vigilance Law: What You Need to Know.” *Corporate Social Responsibility and the Law*. <https://www.csrandthelaw.com/2017/08/03/the-french-duty-of-vigilance-law-what-you-need-to-know/> (May 16, 2020).

145 Business & Human Rights Resource Center. 2019. “National Movements for Mandatory Human Rights Due Diligence in European Countries.” <https://www.business-humanrights.org/en/national-movements-for-mandatory-human-rights-due-diligence-in-european-countries> (May 16, 2020). Business & Human Rights Resource Centre. 2020. “Landmark Report on 1,000 European Companies Shows the Need for Human Rights Due Diligence Laws.” <https://www.business-humanrights.org/en/landmark-report-on-1000-european-companies-shows-the-need-for-human-rights-due-diligence-laws> (May 16, 2020). Business & Human Rights Resource Centre. “MEPs & Companies Call for EU-Level Human Rights Due Diligence

Legislation.” <https://www.business-humanrights.org/en/meps-companies-call-for-eu-level-human-rights-due-diligence-legislation> (May 16, 2020).

146 “Commission Announcement of Due Diligence Legislation.” 2020. Heidi Hautala. <https://heidihautala.fi/en/commission-announcement-of-due-diligence-legislation/> (May 16, 2020). European Coalition for Corporate Justice. 2020. *Model Legislation on Corporate Responsibility to Respect Human Rights and the Environment - European Coalition for Corporate Justice*. Legal brief. <https://corporatejustice.org/eccj-publications/16804-eccj-legal-brief-eu-model-legislation-on-corporate-responsibility-to-respect-human-rights-and-the-environment> (May 16, 2020).

147 Kublin, Craig. 2019. “US House Financial Services Committee Holds Landmark Hearing on ESG Reporting.” *Environment, Land & Resources*. <https://www.globalelr.com/2019/07/us-house-financial-services-committee-holds-landmark-hearing-on-esg-reporting/> (May 16, 2020). Zaidi, Ali. 2019. “INSIGHT: Pending Federal ESG Legislation Could Yield Significant and Step-Wise Change.” Bloomberg Law. <https://news.bloomberglaw.com/banking-law/insight-pending-federal-esg-legislation-could-yield-significant-and-step-wise-change> (May 16, 2020). *Corporate Human Rights Risk Assessment, Prevent, and Mitigation Act*. 2019. (U.S. House of Representatives) <https://financialservices.house.gov/uploadedfiles/bills-116pih-corphuman.pdf>

148 Global Network Initiative. 2020. “Global Network Initiative.” *Global Network Initiative*. <https://globalnetworkinitiative.org/> (May 16, 2020).

149 Global Network Initiative. 2020. *The GNI Principles at Work: Public Report on the Third Cycle of Independent Assessments of GNI Company Members 2018/2019*. <https://globalnetworkinitiative.org/wp-content/uploads/2020/04/2018-2019-PAR.pdf>.

150 See Governance section, Ranking Digital Rights. 2019. *Corporate Accountability Index*. Washington,

DC: New America. <https://rankingdigitalrights.org/index2019/report/governance/#section-33>

151 The scope of GNI’s work does not include commercial privacy issues that are not directly related to government surveillance actions or user data demands. Nor does GNI address content moderation carried out to enforce companies’ own rules if the restrictions are not made in response to government demands or direct requirements. Any expansion of GNI’s scope would need the support of its board of directors. At present, GNI’s mandate does not cover the human rights risks caused by commercial business practices and mechanisms including content moderation, algorithmic systems for content recommendation and prioritization, commercial data collection and sharing, or human rights concerns related to targeted advertising business models.

152 “The Partnership on AI.” <https://www.partnershiponai.org/> (May 16, 2020).

153 Crocker, Andrew et al. 2019. *Who Has Your Back? Censorship Edition 2019*. Electronic Frontier Foundation. <https://www.eff.org/wp/who-has-your-back-2019> (May 16, 2020).

154 Singh, Spandana. 2019. *Assessing YouTube, Facebook and Twitter’s Content Takedown Policies*. Washington: New America. <http://newamerica.org/oti/reports/assessing-youtube-facebook-and-twitthers-content-takedown-policies/> (May 16, 2020).

155 Twitter. “Twitter Safety Partners.” https://about.twitter.com/en_us/safety/safety-partners.html (May 16, 2020).

156 Hern, Alex. 2020. “Facebook Judges, Journalists and Politicians on Free Speech Panel.” *The Guardian*. <https://www.theguardian.com/technology/2020/may/06/facebook-oversight-board-freedom-expression-helle-thorning-schmidt-alan-rusbridger> (May 16, 2020). Botero-Marino, Catalina, Jamal Greene, Michael W. McConnell, and Helle Thorning-Schmidt. 2020. “Opinion | We Are a New Board

Overseeing Facebook. Here’s What We’ll Decide.” *The New York Times*. <https://www.nytimes.com/2020/05/06/opinion/facebook-oversight-board.html> (May 16, 2020).

157 Wong, Julia Carrie. 2020. “Will Facebook’s New Oversight Board Be a Radical Shift or a Reputational Shield?” *The Guardian*. <https://www.theguardian.com/technology/2020/may/07/will-facebooks-new-oversight-board-be-a-radical-shift-or-a-reputational-shield> (May 16, 2020).

158 See the recommendations in Maréchal, Nathalie, and Ellery Roberts Biddle. 2020. *It’s Not Just the Content, It’s the Business Model: Democracy’s Online Speech Challenge - A Report from Ranking Digital Rights*. Washington D.C.: New America. <https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/key-transparency-recommendations-for-content-shaping-and-moderation>.

159 The 2020 RDR Index methodology has been revised and the version we will use to evaluate companies in 2020 will be published in June. For the consultation draft of the new indicators see: <https://rankingdigitalrights.org/2020/04/15/2020-draft-methodology/>. The indicators used for the 2019 RDR Index can be found at: <https://rankingdigitalrights.org/2019-indicators/>

160 See the conclusion in Maréchal, Nathalie, and Ellery Roberts Biddle. 2020. *It’s Not Just the Content, It’s the Business Model: Democracy’s Online Speech Challenge - A Report from Ranking Digital Rights*. Washington, D.C.: New America. <https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/conclusion>

161 Feldman, Max. 2020. *Dirty Tricks: Eight Falsehoods That Could Undermine the 2020 Election*. Brennan Center for Justice. <https://www.brennancenter.org/our-work/research-reports/dirty-tricks-eight-falsehoods-could-undermine-2020-election> (May 16, 2020).

162 Hasen, Richard L. 2020. "What Happens in November If One Side Doesn't Accept the Election Results?" *Slate*. <https://slate.com/news-and-politics/2020/03/2020-election-meltdown-coronavirus-delay.html> (May 16, 2020).

163 For an example of a rapid due diligence tool see Allison-Hope, Dunstan, and Jenny Vaughan. 2020. "COVID-19: A Rapid Human Rights Due Diligence Tool for Companies." *BSR*. <https://www.bsr.org/en/our-insights/blog-view/covid-19-a-rapid-human-rights-due-diligence-tool-for-companies> (May 16, 2020).



This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of New America content when proper attribution is provided. This means you are free to share and adapt New America’s work, or include our content in derivative works, under the following conditions:

- **Attribution.** You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit **creativecommons.org**.

If you have any questions about citing or reusing New America content, please visit **www.newamerica.org**.

All photos in this report are supplied by, and licensed to, **[shutterstock.com](https://www.shutterstock.com)** unless otherwise stated. Photos from federal government sources are used under section 105 of the Copyright Act.