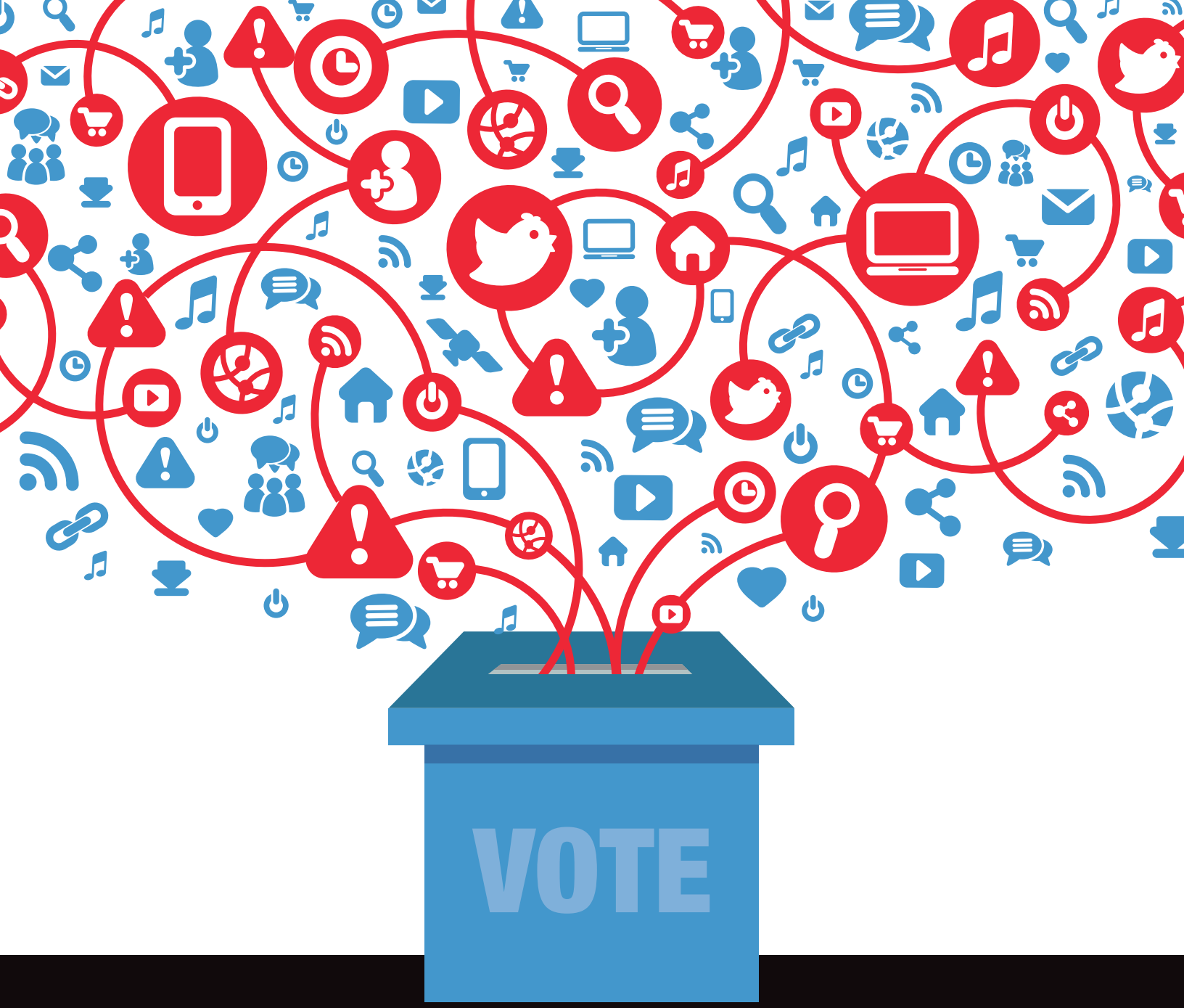

As a Matter of Fact

The Harms Caused by Election Disinformation

Common Cause
Education Fund

About Common Cause Education Fund

The Common Cause Education Fund is the research and public education affiliate of Common Cause, founded by John Gardner in 1970. We work to create open, honest, and accountable government that serves the public interest; promote equal rights, opportunity, and representation for all; and empower all people to make their voices heard in the political process.

Acknowledgments

This report was co-authored by Sylvia Albert, Yosef Getachew, Jesse Littlewood, Beth Rotman, Paul S. Ryan, Emma Steiner, and Jonathan Walter and published by Common Cause Education Fund.

We also thank Karen Hobert Flynn, Michael Copps, Marilyn Carpinteyro, Susannah Goodman, Stephen Spaulding, and Aaron Scherb for guidance and editing; Melissa Brown Levine for copyediting; Kerstin Vogdes Diehn for design; and Scott Blaine Swenson, David Vance, and Ashlee Keown for strategic communications support. Finally, special thanks to Austin Graham, legal counsel at the Campaign Legal Center, for consultation regarding exemplary state campaign finance disclosure laws.

Special thanks are due to the thousands of volunteers of Common Cause Education Fund's Stopping Cyber Suppression program who spent tens of thousands of hours monitoring social media for disinformation that could disenfranchise voters. Many of the examples in this report came from volunteers in this program.

Knowledge planted in truth grows in truth.

—Aberjhani[1]

CONTENTS

Executive Summary 5

Introduction 10

Section 1: Election Disinformation Overview 12

- What Is Election Disinformation? 12
- When Is Disinformation Spread? 16
- How Is Disinformation Spread? 17
- Who Is Spreading Election Disinformation and Why? 28
- Disinformation Case Study: Arizona Sham Ballot Review 31

Section 2: State and Federal Laws Regulating Election Disinformation 35

- Voter Intimidation and False Election Speech Laws 35
- Campaign Finance Laws 38
- Federal Communications Laws 41
- Federal Consumer Protection Laws 42
- State Media Literacy Laws 43
- State Privacy Laws 45

Section 3: Select Social Media Civic Integrity Policies 47

- Facebook 48
- Twitter 49
- YouTube 50

Section 4: Recommendations 51

- Statutory Reforms 51
  - Voter Intimidation and False Election Speech Reforms 51
  - Campaign Finance Reforms 52
  - State Media Literacy Laws 53
  - State Privacy Laws 53
  - Federal Legislative Reforms to Mitigate Platform Business Practices 54
- Executive and Regulatory Agency Reforms 55
  - Presidential and Gubernatorial Leadership 55
  - U.S. DOJ and State Law Enforcement Agencies 56
  - FTC Reforms 56
  - FEC and State Election Agency Reforms 56

Social Media Corporation Policy Reforms 57
Provide Users With Authoritative Information About Voting and Elections 57
Consistent Enforcement of Civic Integrity Policies During Both Election and Nonelection Cycles 57
Reducing the Spread and Amplification of Disinformation 58
Provide Researchers and Watchdog Journalists Greater Access to Social Media Data 58
Invest Greater Resources in Combating Disinformation Targeting Non-English-Speaking Communities 58

Conclusion **59**

Appendix I—State Voter Intimidation and False Election Speech Laws **60**

Appendix II—State Campaign Finance Disclosure Laws **63**

Appendix III—State Media Literacy Laws **65**

Endnotes **66**

EXECUTIVE SUMMARY

In America, whatever our background, color, or zip code, we value our freedom. Generation after generation has fought for the freedom to have a say in decisions that impact our lives—the freedom to participate fully in our country. But in recent years, a small faction has grown increasingly skilled at spreading lies about our elections, lies that targeted Black communities and other communities of color to suppress their votes, lies that fueled a deadly attack on our Capitol in January 2021 to disrupt the peaceful transfer of power, lies that threaten to suppress votes and undermine public confidence in future elections. This intentional use of false information to affect the participation of voters in elections is known as "election disinformation."

The United States is at a critical juncture. More than 1 in 3 U.S. residents—and nearly 80% of Republicans—wrongly believe that President Joe Biden did not legitimately win the election.[2] And a majority say they "do not have confidence that elections reflect the will of the people."[3] Donald Trump's Big Lie is working, and we have to respond. Just as we came together last year, rising up to vote safely and securely in record numbers during a global pandemic, we must now rise up to stop election disinformation efforts in future elections. This report is a game plan for success.

The United States is at a critical juncture. More than 1 in 3 U.S. residents—and nearly 80% of Republicans—wrongly believe that President Joe Biden did not legitimately win the election.

Election disinformation is not a new phenomenon. Indeed, for nearly two decades Common Cause has been monitoring and working to stop election disinformation as a part of the national Election Protection coalition.[4] As explained in our 2008 report *Deceptive Practices 2.0*,[5] co-authored with the Lawyers' Committee for Civil Rights Under Law and the Century Foundation, false or misleading information about the voting process, often targeting Black communities and intended to suppress votes, has historically been disseminated via flyers and "robocalls." But by 2008, disinformation was beginning to move to email and websites. And as explained in our 2012 report *Deceptive Election Practices and Voter Intimidation*, disinformation tactics continued to evolve: "Over time, they have become more sophisticated, nuanced, and begun to use modern technology to target certain voters more effectively."[6] The volume and sophistication of online disinformation, particularly via social media platforms, continued to rise in 2016 and 2018 preceding a veritable explosion of election disinformation throughout the 2020 election cycle.

As online election disinformation has increased, Common Cause Education Fund's commitment to monitoring and stopping it has likewise increased. During the 2020 election cycle, we led an Anti-Disinformation Working Group of the Election Protection coalition, hired experienced disinformation analysts, and trained dozens of partner organizations and thousands of volunteers in disinformation monitoring. We catalogued more than 3,000 disinformation posts in our election disinformation database, requested the removal of posts from social media platforms when they violated corporate policies, developed messaging to "pre-bunk" the disinformation, and dis-

seminated accurate voting and election information in partnership with the Election Protection coalition.

We continue our election disinformation work in the 2021 "off-year" elections and prepare for elections in 2022 and beyond. As part of our plan to combat election disinformation, Common Cause Education Fund has prepared this report to explain the problem of election disinformation in detail and propose commonsense public and corporate policy reforms to reduce the harmful impacts of election disinformation in future elections.

Section 1 provides an overview of election disinformation, explaining what it is, how it's being spread, and who is spreading it. Understanding the threat of election disinformation is the first step toward eliminating the threat. Common examples of election disinformation include communications providing the wrong election date, bogus election rules, voter intimidation, untrue claims about election integrity/security, and untrue claims post-election about results. Today, the most common means of disseminating disinformation include social media platforms like Facebook and Twitter, junk websites, mainstream media like Fox News, search engines like Google, email, text messages, and robocalls.

For example, in the spring of 2020, former president Donald Trump repeatedly and falsely claimed that mail-in ballots were less secure and part of a plan to rig the election against him and Republicans, generally. Supporters of Trump then repeated these claims, driving a false narrative of voter fraud. Experts analyzed social media and found a massive 3.1 million mentions of disinformation about voting by mail between January 2020 and September 2020.[7] Election disinformation is spread before, during, and after Election Day. The 2020 false voter fraud narrative fed a post-election false narrative that the election was "stolen" from Trump (i.e., Trump's "Big Lie"), giving energy to the so-called Stop the Steal movement and the deadly January 6 insurrection. These false narratives persist today, undermining public confidence in future elections and being used as justification for new voter suppression laws in states around the nation.

Section 2 details current federal and state laws regulating election disinformation—voting rights, campaign finance, communications, consumer protection, media literacy, and privacy laws—and the shortcomings of current laws. These laws are tools we must use to thwart election disinformation efforts. A primary purpose of election disinformation is to suppress and sometimes intimidate voters. Federal law and laws in nearly every state contain provisions explicitly prohibiting voter intimidation, with many of these laws being rightly interpreted as prohibiting election disinformation. A handful of states have enacted laws explicitly prohibiting knowingly disseminating materially false information about the time, place, or manner of elections with the intent to impede voting. Such laws play an important role in fighting election disinformation and should be widely enacted and enforced.

Several other bodies of law are also critically important to combating election disinformation. Strong campaign finance disclosure laws can shine the light of publicity on those seeking to undermine our elections from the shadows. Federal communications law provides digital platforms with legal protections to moderate content online without fear of liability and directly impact election disinformation. Consumer protection laws can protect us from deceptive data collection and data security breaches and have been used to punish some who have contributed to the spread of disinformation. State media literacy laws can help people build the skills necessary to discern

fact from opinion and fiction, news from infotainment, and real information from disinformation. And state privacy laws can protect personal data to prevent bad actors from precision targeting of election disinformation. All of these laws can play a part in effectively regulating and deterring election disinformation.

Section 3 describes the civic integrity policies of some of the largest social media companies, the policies Facebook, Twitter, and YouTube have put in place to address abuses of their platforms for the dissemination of election disinformation. Across all these platforms, content that is misleading about how to participate in elections is actionable and should be removed, including misleading information about the date or time or requirements to participate in an election and statements advocating for violence because of voting, voter registration, the administration, or outcome of an election.

Unfortunately, current civic integrity policies have significant loopholes that have allowed content contributing to voter suppression and election disinformation to remain on social media platforms. Part of the problem is frequent changes to civic integrity policies. For example, during the 2020 election cycle, Facebook changed its election-related misinformation policies 21 times, Twitter changed its policies 16 times, and YouTube changed its policies 12 times.[8] Most of these changes involved adding, subsequently rolling back, and then reinstating new rules concerning key issues like mail-in voting fraud or false victory claims.[9] Another problem is a lack of transparency regarding how well these policies were enforced and their impact on election misinformation. Making matters worse, Facebook and Twitter have now rolled back policies they put in place during 2020 and stopped enforcing existing policies to the degree they did during the 2020 election cycle. Our research shows that there are many pieces of content being left on the platform that would have been taken down months ago. Social media platforms must take additional steps to strengthen their policies on combating content designed to undermine our democracy.

Finally, **Section 4** identifies gaps in current laws and policies that have allowed election disinformation to flourish and recommends reforms to better enable us to fight back against election disinformation.

Federal and State Voting Rights Reforms

The **single most important tool to stop election disinformation is a statute prohibiting knowingly disseminating materially false information regarding the time, place, or manner of elections or the qualifications or restrictions on voter eligibility, with the intent to impede voting.** While the U.S. Department of Justice (DOJ) and some state law enforcement agencies have interpreted existing civil rights laws, specifically those prohibiting voter intimidation or interference, as applying to election disinformation via social media platforms, this application of the law has not yet been thoroughly tested in courts. **Congress and state legislatures should remove any doubt by enacting statutes prohibiting such false election speech**, with both criminal and private civil remedies and a mandate that the government corrects materially false election information.

Federal and State Campaign Finance Reforms

Congress and state legislatures must update campaign finance disclosure laws for the digital age. Strong campaign finance disclosure laws are key to curbing the harmful impacts of election

disinformation. Unfortunately, federal campaign finances laws and the laws of most states are out-of-date, lacking clear mandates and guidance for **"paid for by" disclaimers on digital advertising**, and effective **provisions shining a light on money transferred between groups to evade disclosure**.

Federal and State Privacy Law Reforms

Congress should pass comprehensive data privacy legislation to protect consumers from the abusive collection, use, and sharing of personal data. At a minimum, federal legislation should (1) require companies to minimize the data they collect; (2) prohibit predatory and discriminatory data practices on the basis of protected characteristics with respect to access to credit, housing, education, employment, and public accommodations; (3) provide for fairness in automated decision-making; (4) grant a private right of action to allow consumers to sue companies that violate their privacy rights; and (5) define permissible and impermissible uses for collecting, sharing, and using personal data.

State legislatures should pass comprehensive consumer privacy laws similar to the California Consumer Privacy Act (CCPA) of 2018 to provide consumers with the right to know about the personal information a business collects about them, the right to delete personal information collected from them, the right to opt out of the sale of their personal information, the right to nondiscrimination for exercising their CCPA rights, and the right for consumers to sue businesses for certain data breaches. And states should go further than the CCPA by including privacy legislation requirements that limit what data entities can collect and how that data can be used, as well as civil rights protections that ensure fairness in both automated decision-making and prohibitions on the use of personal data to discriminate on the basis of race, gender, religion, national origin, sexual orientation, gender identity, disability, familial status, biometric information, or lawful source of income, as well as a robust private right of action for consumers whose rights are violated.

State Media Literacy Law Reforms

State legislatures should experiment with best practices around media literacy and hold convenings with organizations like PEN America that are already engaged in the issue and offering media literacy training to the public to put together a set of agreed-upon principles on which to develop legislation.

Federal Media Law Reforms

Congress should enact legislation strengthening local media and protecting public access to high-quality information about government, public safety, public health, economic development, and local culture, such as the Future of Local News Act, which would create a committee to study the state of local journalism and offer recommendations to Congress.

Congress should pass legislation to protect researchers' and watchdog journalists' access to social media data, enabling researchers to study social media platform practices without fear of interference or retaliation from social media companies.

Congress should pass legislation to prohibit online platform discriminatory algorithms and to create greater transparency about how these algorithms operate.

Federal and State Executive and Regulatory Agency Reforms

The White House must play a leading role in combating election disinformation, including by issuing an executive order directing federal agencies with enforcement, rule-making, and investigatory authorities to use these capabilities in combating election disinformation. The White House should also create a federal interagency task force that would identify tools to combat election disinformation and harmful online speech. **Governors in states around the nation should likewise lead efforts to combat election disinformation on the state level.**

The DOJ and state law enforcement agencies should use all existing statutory and regulatory tools (e.g., existing anti-voter intimidation laws) to more aggressively prosecute those who use disinformation to intimidate voters and interfere with their voting rights.

The **Federal Trade Commission should expand the scope of its rule-making and enforcement practices** to more effectively regulate unfair and deceptive commercial data practices and conduct workshops and issue informal guidance on how social media platforms can provide greater transparency in their content moderation practices.

The **Federal Election Commission and state election agencies** should better use all available rule-making and enforcement authority to implement effective campaign finance disclosure requirements for online political advertising.

Social Media Corporation Policy Reforms

While self-regulation will never alone be sufficient, **social media companies must do a better job curbing the spread of disinformation by strengthening their policies** around combating content designed to undermine our democracy. We make specific recommendations in this report for how social media companies can improve their efforts to provide users with authoritative information regarding voting and elections, reduce the spread and amplification of election disinformation, and provide greater transparency concerning their content moderation policies and practices.

Democracy depends on free and fair elections. Together, we must educate ourselves, demand rigorous enforcement of existing laws to stop election disinformation, and pass new laws to protect our right to vote and to stop a small faction from sabotaging our elections.

INTRODUCTION

For nearly two decades, Common Cause has been monitoring and working to stop election disinformation. As the volume and sophistication of online disinformation have risen in recent years, so too has Common Cause Education Fund's commitment to monitoring and stopping the disinformation.

Throughout the 2020 election cycle, Common Cause Education Fund trained thousands of volunteers, who contributed tens of thousands of hours searching for election disinformation in their own social media networks. We also hired experienced staff and contractor disinformation analysts who monitored the more extreme communities and social media platforms. Through this work, we created a database of election disinformation. We led an Anti-Disinformation Working Group of the Election Protection coalition and trained dozens of partner voter protection groups in how to monitor, analyze, and take action on election disinformation, which was particularly critical for language access (including Spanish, Haitian Creole, Arabic, and Asian and Pacific Islander languages). Last, we opened up a public "tip line" for disinformation reports at ReportDisinfo.org.

Throughout the 2020 election cycle, Common Cause Education Fund trained thousands of volunteers, who contributed tens of thousands of hours searching for election disinformation in their own social media networks.

Our in-house analyst reviewed disinformation reports from all these sources daily, documenting and cataloging them in our database, which was shared with our voter protection partners. Our analyst identified which posts were likely to be "actioned" by the social media companies based on their civic integrity policies and reported these posts to the companies, resulting in over 300 actions (labels, removals, and banning of accounts). Unfortunately, the posts on which the companies took action were only a fraction of the 3,000+ problematic election disinformation posts we added to our database, which either were not actioned when reported or were outside the companies' narrow rules for taking action.

Requesting removal from the social media platforms was just one of our program's interventions on election disinformation. We were in constant communication with more than 40 voter protection organizations, alerting them to disinformation threats and providing resources, including messaging and "inoculation" content to "pre-bunk" disinformation. We secured a partnership with PolitiFact to issue fact-checks on dubious social media content and worked with messaging experts and creative designers to make educational social media content for use by the Election Protection coalition. Volunteers and staff of Common Cause Education Fund and partner organizations likewise posted accurate voting and election information on social media through the Election Protection network—including answering questions raised by voters on their own social media posts (e.g., polling place hours, locations, rules, and regulations). We logged over 6,000 of these "voter assistance" posts **(see Figure 1)**.

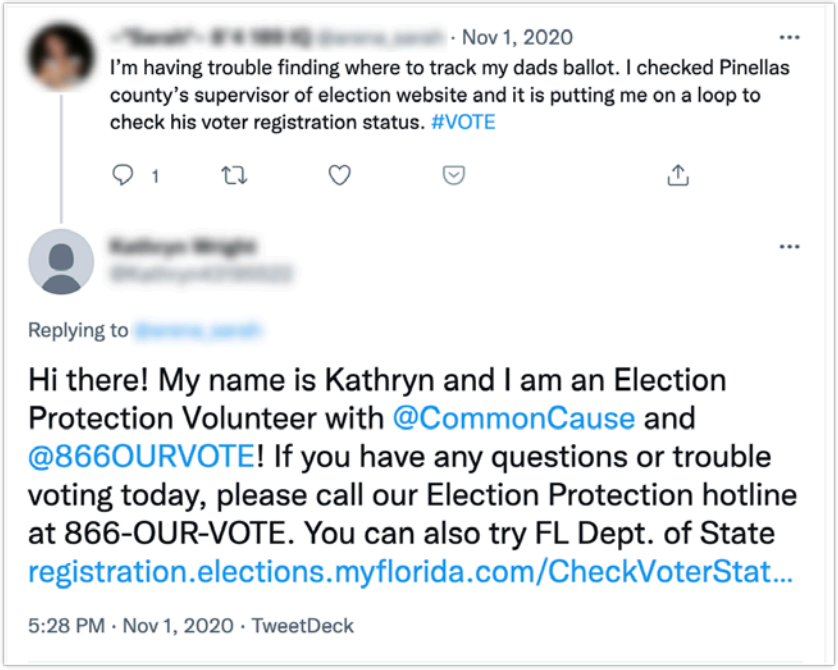

Figure 1: A "voter assistance" post by a Common Cause volunteer.

Our election disinformation monitoring and analysis program has continued during the 2021 "off-year" elections, and we are preparing for 2022. Our focus was (and remains) on **nonpartisan** election disinformation or "cyber suppression"—i.e., mis- and disinformation that could prevent voters from participating in the election and/or undermine their faith in the integrity of the electoral process. We identify and take action on disinformation from both Democrats and Republicans, left-leaning posts and right-leaning posts. However, when volunteers find disinformation about a specific candidate (e.g., disinformation about a candidate's policies, personal history, or activities), we do not catalogue or take action on the candidate-specific disinformation. Doing so would not only stretch our capacity far beyond our limits but also require us to wade into matters that are often more subjective and partisan, in tension with our strict nonpartisanship policy. Candidates and parties are better suited to handle candidate-specific disinformation and typically dedicate resources to doing so.[10]

This report is built on decades of experience monitoring and responding to election disinformation. **Section 1** provides an overview of election disinformation, explaining what it is, how it's being spread, and who is spreading it. Understanding the threat of election disinformation is the first step toward eliminating the threat. **Section 2** details current federal and state laws regulating election disinformation—voting rights, campaign finance, communications, consumer protection, media literacy, and privacy laws. These laws are tools we must use to thwart election disinformation efforts. **Section 3** describes the civic integrity policies of some of the largest social media companies, the policies Facebook, Twitter, and YouTube have put in place to address abuses of their platforms for the dissemination of election disinformation. Finally, **Section 4** identifies gaps in current laws and policies that have allowed election disinformation to flourish and recommends reforms to better enable us to fight back against election disinformation.

SECTION 1: ELECTION DISINFORMATION OVERVIEW

What Is Election Disinformation?

Broadly, election disinformation refers to intentional attempts to use false information to affect the participation of voters in elections. There is a long history of tactics used to disenfranchise voters, and our previous reports[11] detail how flyers, billboards, and other offline tactics are used to tell voters incorrect information that could prevent them from participating in an election. These reports also highlighted some of the emerging online digital tactics used to spread election disinformation, including email, the web, and Facebook, which were just gaining mainstream popularity.

Our earlier reports make clear that as communication methods and channels mature, malign actors adopt them in the service of election disinformation and voter suppression. In the present era, widely adopted social media, where anyone can be a publisher of content, often anonymously or semi-anonymously, has become the most effective communication method of election disinformation. Although purveyors of election disinformation are not limited to social media, where about half of us find our news, they have aggressively adopted the medium.[12]

For nearly two decades, Common Cause Education Fund has been monitoring and working to combat election disinformation through our Election Protection coalition. We witnessed a steady rise of disinformation online in 2016 and 2018, and then a veritable explosion of voting-related disinformation throughout the 2020 election cycle.

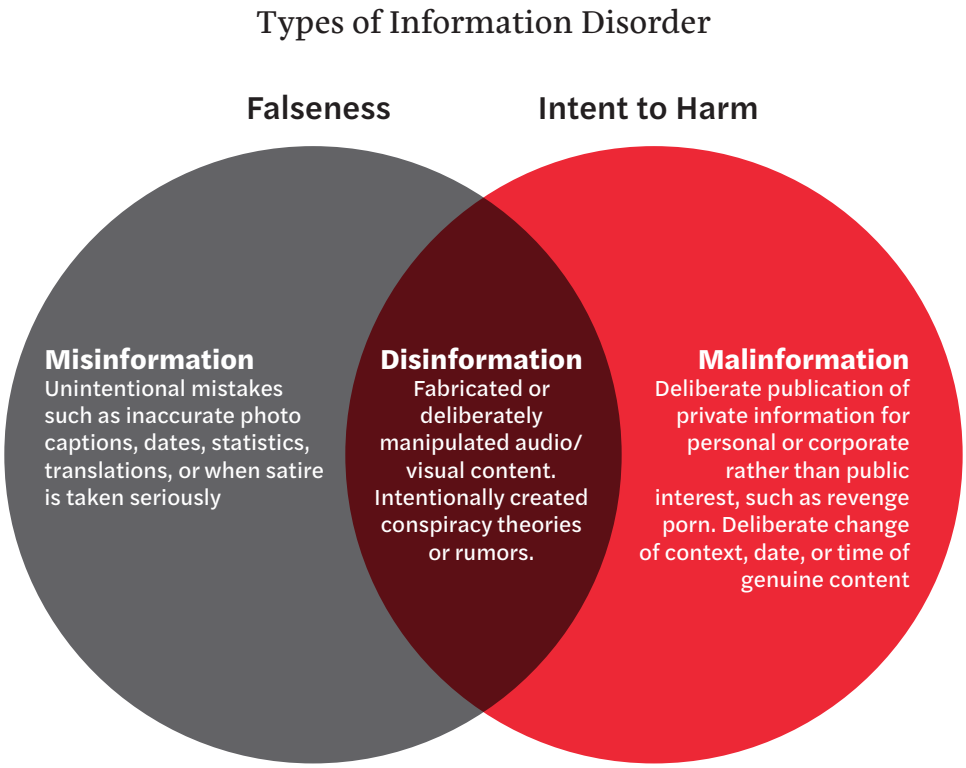

Figure 2: Three types of information disorder. Credit: Claire Wardle and Hossein Derakshan, 2017

"Information disorder" is an emerging term of art used by researchers and media experts[13] that encompasses three related terms **(see Figure 2):**

- **Disinformation** is content that is false (even if it contains some truth) and deliberately created to harm a person, social group, organization, or country.
- **Misinformation** is false information, but it is differentiated from disinformation by lacking an intent to harm any person, group, or organization.
- **Malinformation** is content that is accurate but is intentionally manipulated to cause harm, including voter suppression or voter confusion.

These terms can be accurately applied to individual pieces of *content (a flyer, poster, billboard, text, phone call, or social media post) but also encompass entire narratives (a sequence of pieces of content knitted together that creates a stronger and lasting impact, often referencing previous pieces of content—e.g., Donald Trump's "Big Lie"*[14]). Voting and elections are threatened by individual pieces of content and narratives that fit within each of these three categories of information disorder.

Misinformation

Misinformation is false information, but it is differentiated from disinformation by lacking an intent to harm any person, group, or organization. While it is less intentional, it can be equally harmful. Examples of misinformation include inaccuracies in dates or statistics or incorrectly identified photo captions. Anyone encountering the misinformation could believe it and draw conclusions from it, even if the content provider was not intending to misinform them.

One common misinformation narrative we encountered during the 2020 elections included a widely shared meme that has appeared in multiple election cycles that encourages voters to use "two stamps" when mailing back their absentee ballot under the (false) theory that the U.S. Postal Service (USPS) will ensure delivery or otherwise prioritize your absentee ballot **(see Figure 3). This is misinformation. The USPS stated it would deliver election mail, even if postage is required, without that postage.**[15] While unintentional, this misinformation perpetuated a negative view of the USPS and its ability to manage mail-in ballots and thereby suppress voting. While impression data is not available from social media platforms, some of the content we saw received thousands of shares, and several news organizations, including Reuters, *USA Today*, and PolitiFact responded with fact-checks. Requiring postage for returning voted ballots by mail is a known barrier to voter participation: not everyone has stamps at home, acquiring stamps required potential exposure to COVID during the early stages of the pandemic, and singular stamps are less likely to be available than entire books or packages (which cost more). A voter who believes two stamps are necessary to submit their mail-in ballot but doesn't have access to two stamps may choose not to vote at all. The now-pending Freedom to Vote Act would amend federal law to make clear that no postage is required for completed ballots.[16]

Disinformation

Disinformation content is false and deliberately created to harm a person, social group, organization, or country. Disinformation is deliberately and often covertly spread to influence public opinion

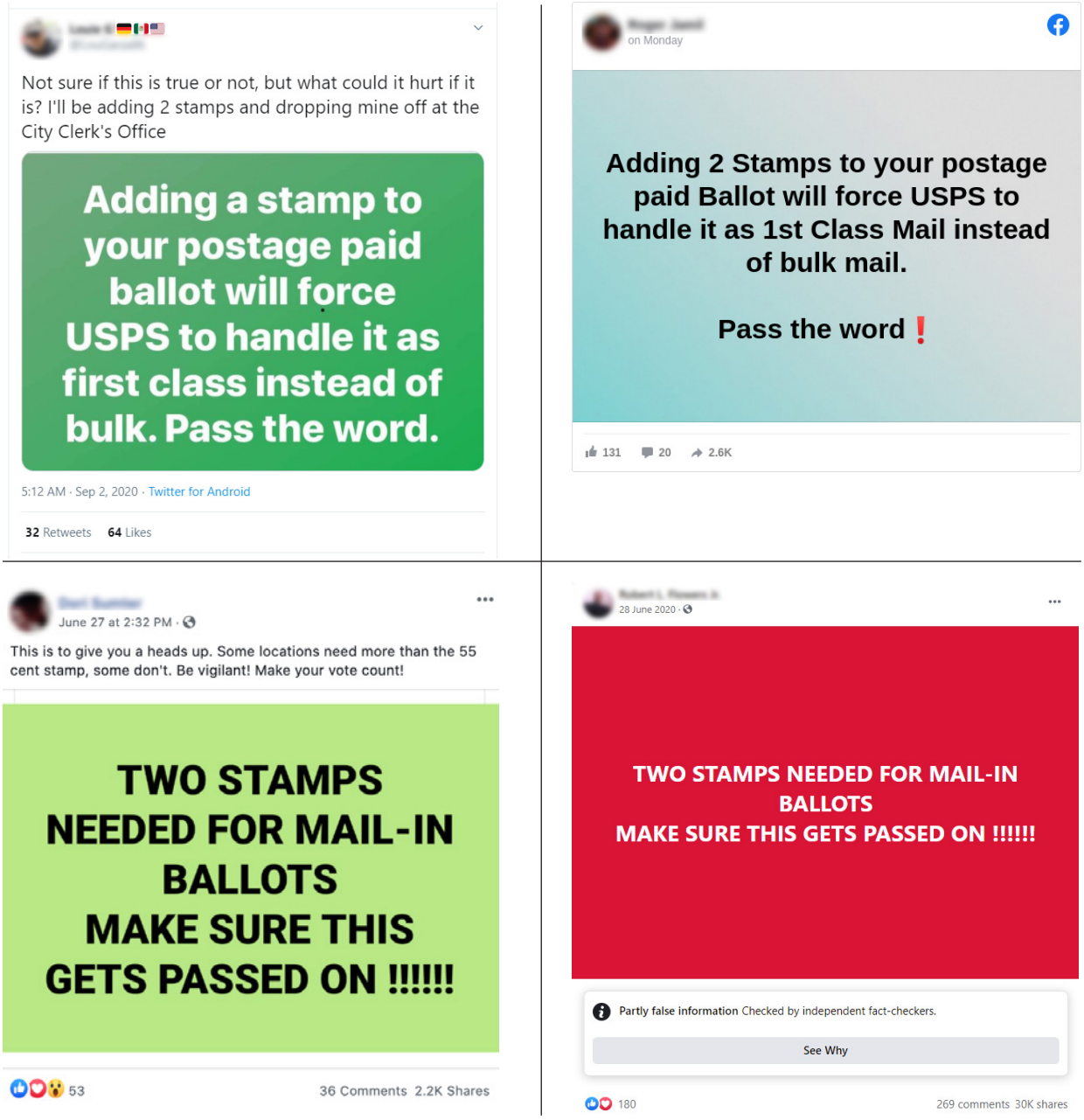

Figure 3: Information disorder posts regarding ballot postage. Credit: Claire Wardle and Hossein Derakshan, 2017

and actions, obscure or alter voting, or provide cause for outrage. Disinformation may contain some true facts, but those facts are either taken out of context or combined with falsehoods to create and support a specific intended message. An example of disinformation using true facts is when old news stories are recirculated to drive people to the wrong conclusions, such as when viral tweets claim that dumped or stolen mail contained ballots or targeted voters specifically. In one instance during the 2020 elections, the pictures that circulated—and garnered thousands of retweets—were actually from a news story two years prior.[17] **See Figure 4 where multiple users posted copycat disinformation posts with this image (successfully reaching a massive audience).**

Common examples of disinformation when it comes to voting and elections include the following:

- Wrong election date, often specific to one group (e.g., "Democrats vote on Wednesday" when the election is on a Tuesday)
- Bogus election rules, often specific to one group (e.g., during the 2016 election numerous social media posts falsely claimed that you could "text your vote" for Hillary Clinton)
- Voter intimidation (e.g., claims that by voting you may put yourself in danger because of the presence of police, Immigration and Customs Enforcement, military, or vigilantes)
- Untrue claims about election integrity/security (e.g., false claims that vote by mail is not secure, false claims that the election process was being rigged or altered)
- Untrue claims post-election about results (e.g., "The Big Lie" false claim that the 2020 election was "stolen" from Trump)

Figure 4: Two disinformation posts that used a photo from an unrelated news story two years prior to make false claims. (These posts were found by a Common Cause volunteer, and our analyst reported them to Twitter, which removed them.)

Malinformation

Malinformation is content that is accurate but is intentionally manipulated to cause harm. This includes misrepresenting the context of a true news story, doxing (releasing personal information like addresses and phone numbers of an individual online to intimidate them), or selectively leaking correspondence. There are multiple ways malinformation negatively impacts voting and elections.

One common use of malinformation is "doxing." "Doxing" is the practice of publishing an individual's personal information online in an effort to intimidate or harass them. After the 2018 midterm elections, when some Florida counties were delayed in reporting the totals of a recount in a very close election, multiple users posted the personal contact information (including home address) of two Florida elections officials while votes were still being cast.[18] The officials were both women of color, and the posts appeared on Facebook pages, including "Confederate Resistance" (which has the Confederate Flag and an image of a gun-holding soldier in its banner).

Malinformation—particularly doxing of elections officials—poses a significant challenge to holding free and fair elections. Election officials are receiving threats[19] and abuse[20] for helping to administer our democracy, fueled by the conspiracy theories that social media platforms allow to thrive through their inaction. Voters, elections officials, poll workers, and volunteer poll monitors have all found themselves as targets of doxing, making our elections more dangerous to participate in, particularly for women and people of color. In one example, Trump and his allies spread conspiracies about election workers in Fulton County, Georgia, claiming that election worker Shaye Moss and her mother Ruby Freeman were involved in a plot to add fraudulent ballots to the count. In Trump's phone call to the Georgia secretary of state urging him to alter the results, he brought up the women, who were the targets of months of threats and harassment.[21] This was all part of what Trump supporters referred to as "Suitcasegate"—their false belief that Fulton County election workers smuggled in fraudulent ballots in suitcases.[22] Other election workers have had to go into hiding, reporting death threats and stalking.[23] A recent survey showed that 1 in 5 election workers have reported receiving threats, and 1 in 3 have felt unsafe at work, all as a consequence of election disinformation.[24]

When elections workers and volunteers are attacked by partisans, it is more likely that only partisans themselves will take the role of administering our elections, which threatens the integrity of elections.

When Is Disinformation Spread?

Election disinformation is spread before, during, and after Election Day.

In the spring of 2020, before voting began, former president Donald Trump and his campaign promoted disinformation falsely, claiming that mail-in ballots were less secure and part of a plan to rig the election against him[25] and Republicans more generally.[26] Junk websites like the Gateway Pundit and Breitbart, as well as Fox News, promote stories of election dysfunction and isolated incidents of voter malfeasance that drive a false narrative of voter fraud, even outside of election periods. Experts analyzed social media between January 2020 and September 2020 and found a massive 3.1 million mentions of disinformation about voting by mail.[27]

With the recent growth in the use of vote-by-mail options and early voting, the active voting "election period" is longer now than in years past. Disinformation spreaders often attack during this longer voting period. During the September 2021 California gubernatorial recall election, which had universal vote by mail (where all registered voters are automatically mailed ballots), during the time that ballots were in mailboxes, Fox News host Tomi Lahren falsely claimed that "the only" thing that will defeat the recall is "voter fraud."[28] Republican candidate Larry Elder made claims of likely voter fraud in the run-up to the election, even creating a website that indicated that the election was rigged while voting was still underway.[29]

In the period after the election concludes and is called by the mainstream media, an increasing number of losers of contests have begun to use claims of a rigged election or unfounded claims of voter fraud to avoid accepting defeat. In the 2019 Kentucky gubernatorial election, after the race was called for his opponent, defeated Gov. Matt Bevin made repeated claims (without evidence) of a rigged election.[30] In the 2020 elections, after the race was called for Joe Biden, Donald Trump's claims of voter fraud and a rigged election were amplified throughout social media and mainstream media—Fox News, on its own, made nearly 800 statements that cast doubt on the results of the election in just two weeks after its own news desk called the election for Biden.[31] These lies gave energy to the so-called Stop the Steal movement that galvanized support for the deadly January 6 insurrection.[32]

Fox News, on its own, made nearly 800 statements that cast doubt on the results of the election in just two weeks after its own news desk called the election for Biden.

Unfortunately, significant damage can occur through the amplification of election disinformation year-round. disinformation efforts not only serve to undermine the legitimacy of the last election but also to lay a foundation of doubt regarding the next election and the integrity of our government, generally. With perpetual campaigns, some politicians continue disseminating election disinformation to keep their donors giving and their names in headlines. Donald Trump, for example, raised more than $100 million peddling lies in the first six months of 2021[33] and continues to tease another run for president in 2024.[34] Some individuals looking to build a following on social media use disinformation to harness the natural outrage we feel about unfairness—especially when it comes to our democracy and our voice in who is elected to lead us.

Disturbingly, from the perspective of social media companies, disinformation is good for business year-round because it drives engagement and use of the platform (which can be monetized by ads and data gathering). Facebook whistleblower Frances Haugen told *60 Minutes* that "Facebook's own research shows that it amplifies hate, misinformation, and political unrest," and that the company prioritizes profit over the public good.[35] Unfortunately, in our current political, media and regulatory frameworks, there is very little to be lost and few systems of accountability that can prevent or hold accountable bad actors or the platforms they use to spread their messages. As a result, we now have a constant, 24/7, year-round public conversation on social media and in the mainstream media anchored with the false narratives of widespread voter fraud and a rigged election. Election disinformation is always in season.

How Is Disinformation Spread?

Disinformation is spread through a variety of communications channels and changes as technology advances. Prior to the widespread adoption of the world wide web and social media, most election disinformation was spread through flyers, billboards, and phone calls.[36] The following are the most-used communications channels for the spread of disinformation today.

Websites and Media Outlets

Junk websites are frequent purveyors of disinformation. *PolitiFact*'s "Junk News Almanac" in November 2017 listed over 300 websites that frequently share mis- and disinformation.[37] But even legitimate websites and media outlets can send mis- or disinformation to voters. Even the most trusted sources of election information sometimes contain misinformation. For example, in the primary elections in New Hampshire in September 2020, at least two county websites stated incorrect information about the acceptance of absentee ballots by election workers at polling places.[38]

Search Engines

A disinformation narrative can take root or spread when users see search engine results for search queries. Google's search engine will return content from junk websites, although Google's recommendation algorithm will often surface more trustworthy sources first. However, even before users click on content that Google's results surface during their search, there are additional opportunities for election disinformation. In 2020, Common Cause researched how search engines responded to a set of voting-related queries and found multiple occasions where search results contained incorrect voting information (e.g., "online voting") or phrases that indicated a disinformation narrative surfaced by scammers or those attempting to suppress the vote.

For example, at the bottom of every page of results, Google shows a "related searches" panel **(see Figure 5).** This panel shows keywords or phrases that other users who searched for the same term also requested. For example, if many users search for "voting" followed by "register to vote," "register to vote" might show up as a related search for "voting." Google's "related searches" feature can steer users toward misinformation.

This "related searches" feature can have a significant impact on the user experience.[39] One market research firm found that 18% of searches involve the user changing the search query before they click on any results and speculated that Google promotes related searches to target such users.[40]

As one troubling example, we found that Google searches for "vote," "how to vote," and "voting" all directed users to related searches about online voting, such as "vote online," "how to vote online," and "online voting website." Encouraging people to vote online—an option that generally

Figure 5: Searches related to "voting" shown in Arizona.

doesn't exist in the United States for the voting public[41]—is a known scam and form of disinformation designed to keep people away from the real polls.[42] Disinformation asserting that voters can cast their ballots via text messages or the web plagues modern elections.[43]

Another area of concern is Google's "autocomplete" feature, which matches the characters that a user has typed into the search bar with previous searches that start with those characters.[44] Autocomplete is different from related searches in that autocomplete attempts to predict how a user will finish a query. According to Google, the search engine turns off the autocomplete feature when the query cannot be reliably matched with related content, when the predictions contain sexual or other policy-violating content, or when a user has previously reported a prediction as inappropriate.[45] Google has a special rule against autocomplete predictions that could affect election integrity.

> We don't allow predictions that could be interpreted as a position for or against any candidate or political party, nor which could be interpreted as claims about the participation in or integrity of the electoral process.[46]

On September 10, 2020, Google clarified that this ban extends to search predictions that suggest donating to a particular candidate or that discuss election processes or requirements, whether they are accurate or not.

However, we found numerous autocomplete suggestions that appear to violate Google's rules **(see Figure 6)**. For example, the third suggestion when we typed "ballot" into a clean instance of Google was "ballot harvesting," a loaded term that has been used by Trump and others to raise suspicions about the practice of ballot collection (i.e., when a person other than the voter collects a completed absentee ballot to drop off).[47]

Existing research finds that a majority of internet users trust Google to provide them with accurate information and that the way Google presents information has the potential to sway public opinion.[48] A 2015 study found that changing the order of search results had a statistically significant impact on undecided voters' candidate preferences.[49] The authors of the study noted that the "impact of such manipulations would be especially large in countries dominated by a single search engine company," like the United States, where Google's market share approaches 90%.[50]

Common Cause engaged in dialogue with Google about these examples, and the company pledged to take action where it identified that our research showed examples that were against its terms of service.

One additional way search results can harm voters is through scam advertisements. Research by the Tech Transparency Project found "search terms like 'register to vote,' 'vote by mail,' and 'where is my polling place' generated ads linking to websites that charge bogus fees for voter registration, harvest user data, or plant unwanted software on people's browsers."[51] After Google pledged to correct this issue, Common Cause collaborated with the Tech Transparency Project and found examples that the problem persisted.[52] This highlights the need for watchdogs and ongoing monitoring of different vectors where disinformation can spread.

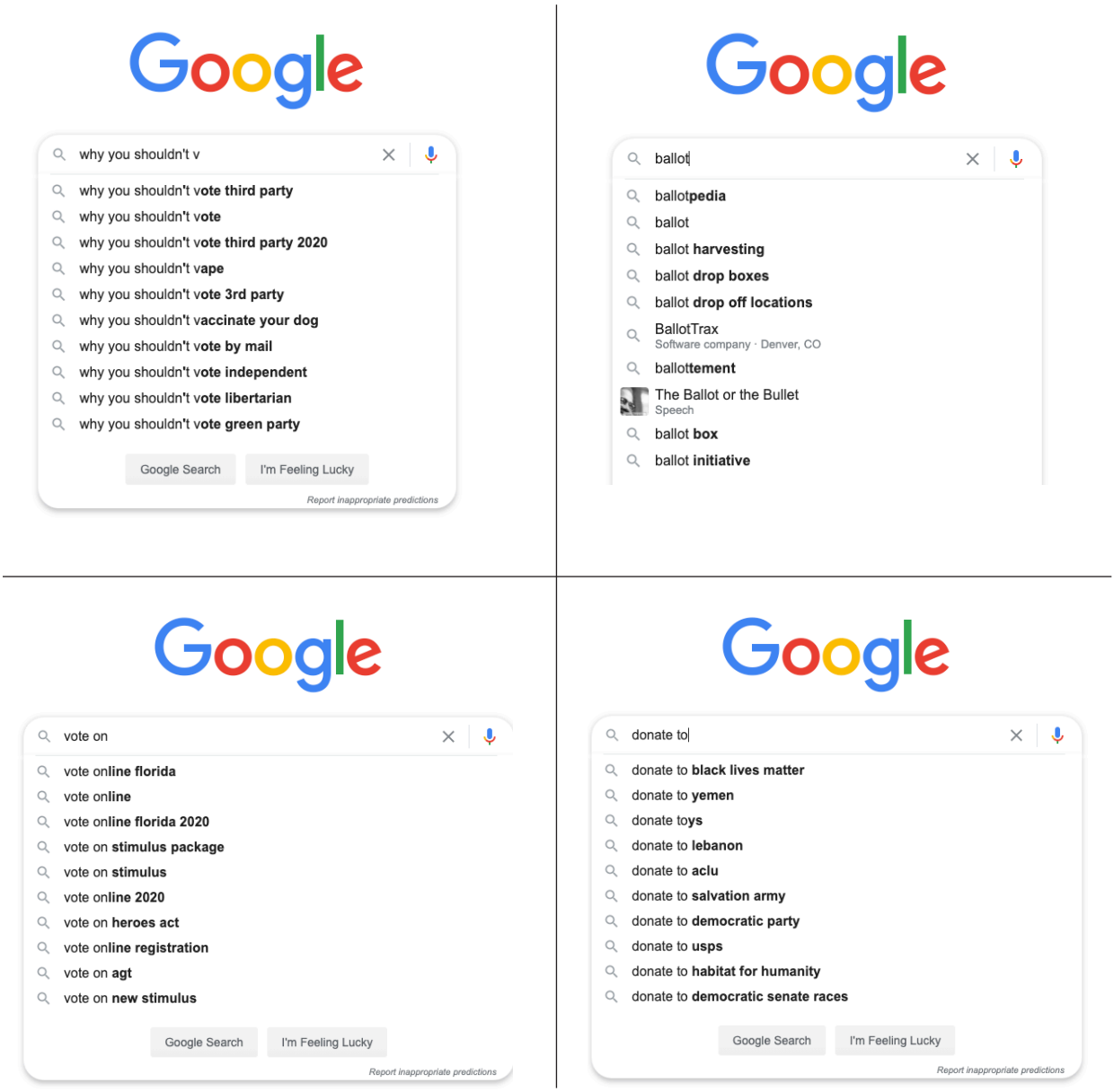

Figure 6: Google autocomplete suggestions for various election-related terms.

Email

In October 2020, the *Washington Post reported that registered Democratic Party voters in four states received threatening emails from unknown actors using the Proud Boys domain that took advantage of information from voter files to harass voters.*[53] The emails reportedly targeted Democratic voters in swing states and told them to change their votes to Trump, or "we will come after you." The emails were reported in Florida, Arizona, Pennsylvania, and Alaska. The Proud Boys denied involvement, pointing to the unsecured status of the domain as evidence that other provocateurs may have hijacked it. The FBI later reported that these emails were the work of Iranian intelligence.[54]

Robocalls

Robocalls (i.e., automated telephone calls that deliver recorded messages) are still used to spread disinformation, in part because they can target individual voters—or segments of voters. On August 27, 2020, Michigan's secretary of state tweeted a notice[55] that Detroit voters were receiving robocalls purporting to be from Jack Burkman and Jacob Wohl of "The 1599 Project" and posted a link to a YouTube audio recording of the call.[56] The robocall tells recipients that voting by mail will enter their information into a public database that "will be used by police departments to track down old warrants," be used to "collect outstanding debts," and enlist people into a mandatory vaccine program from the Centers for Disease Control and Prevention. The call then warns people not to give their information to "the Man."

Soon after these Michigan robocalls were made public,[57] reports surfaced of the same robocalls being made to voters in Philadelphia and Pittsburgh.[58] The two men cited in the call were known for their history of attempting to entrap public officials with bizarre schemes. The attorney general and secretary of state in Michigan announced an inquiry into the source of the calls.[59] On August 24, 2021, the Federal Communications Commission proposed a $5 million fine to the perpetrators.[60]

Text Messages

Similar to robocalls, text messages can be sent directly to individual voters via phone numbers and automated by computers. Text messages are also important disinformation vectors from individuals who, of their own volition, want to share disinformation with their contacts. Text messages are private communication, and most cellphone carriers, because of privacy concerns, cannot or will not actively monitor or interfere with users' text messages. This can make it more difficult to combat disinformation.

Some social media platforms, like WhatsApp, operate similarly to text messages—they are confidential and encrypted, one-to-one (or group) messages where only the receiver can view them. Similar to text messages, it is possible to send unsolicited messages on WhatsApp and similar platforms. However, most of the disinformation spread on WhatsApp in the 2020 election appears to have come from within a "group" of contacts, not from an outside interloper.[61]

Social Media

More than 70% of U.S. residents use social media,[62] and half of the adults in the United States "often" or "sometimes" get their news from social media.[63] With this increasing adoption of social media by voters, social media has become a critical vector for election disinformation. Social media is a broad category that creates multiple vectors for disinformation to spread, and the ways different social media platforms work create different challenges and opportunities to combat disinformation. Disinformation proliferates on social media. Global human rights group Avaaz found that just a small group of disinformation spreaders are responsible for a large portion of election and voting disinformation online, spawning millions

More than 70% of U.S. residents use social media, and half of the adults in the United States "often" or "sometimes" get their news from social media.

of interactions around false and misleading stories.[64] The Jacobs Technion-Cornell Institute at Cornell Tech found 7.6 million tweets and 25.6 million retweets from 2.6 million users that included key terms relating to voter fraud spanning from October 23 to December 16, 2020.[65] The spread of election disinformation via social media platforms is a huge and growing problem.

Some social media platforms, like Twitter, are "open." That is, most users can see most of the content. While some users on Twitter choose to keep their content private, and there are private "direct messages," most Twitter content is available to any user, can be searched and found, and has the potential to find its way into the "feed" of any user. YouTube and (generally) Instagram also fit into this category **(see Figure 7)**.

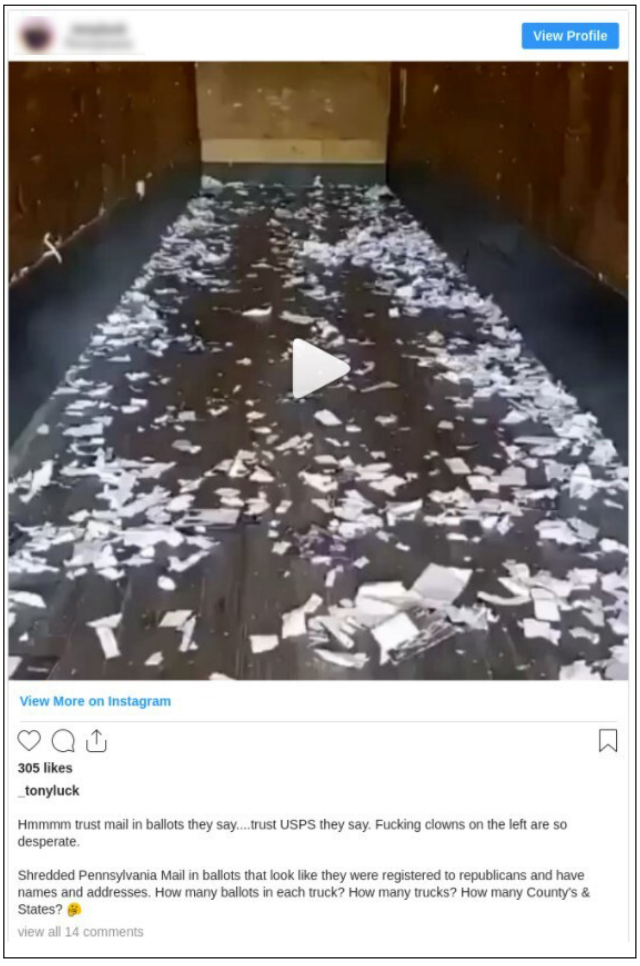

Figure 7: Instagram. The picture is from a video that went viral after people mistook residual shredding for mail-in ballots.

Some social media platforms, like WhatsApp, are "closed" and content is sent (and seen) by specific groups of users, not everyone on the platform. While WhatsApp allows group chats, you cannot search for content across the platform in the way you can with Twitter currently. NextDoor is another "closed" platform where most of the content posted there can only be seen by users in the specific neighborhood they reside in or in neighboring areas **(see Figure 8)**. Other posts on NextDoor can be public posts, but the majority are location specific.

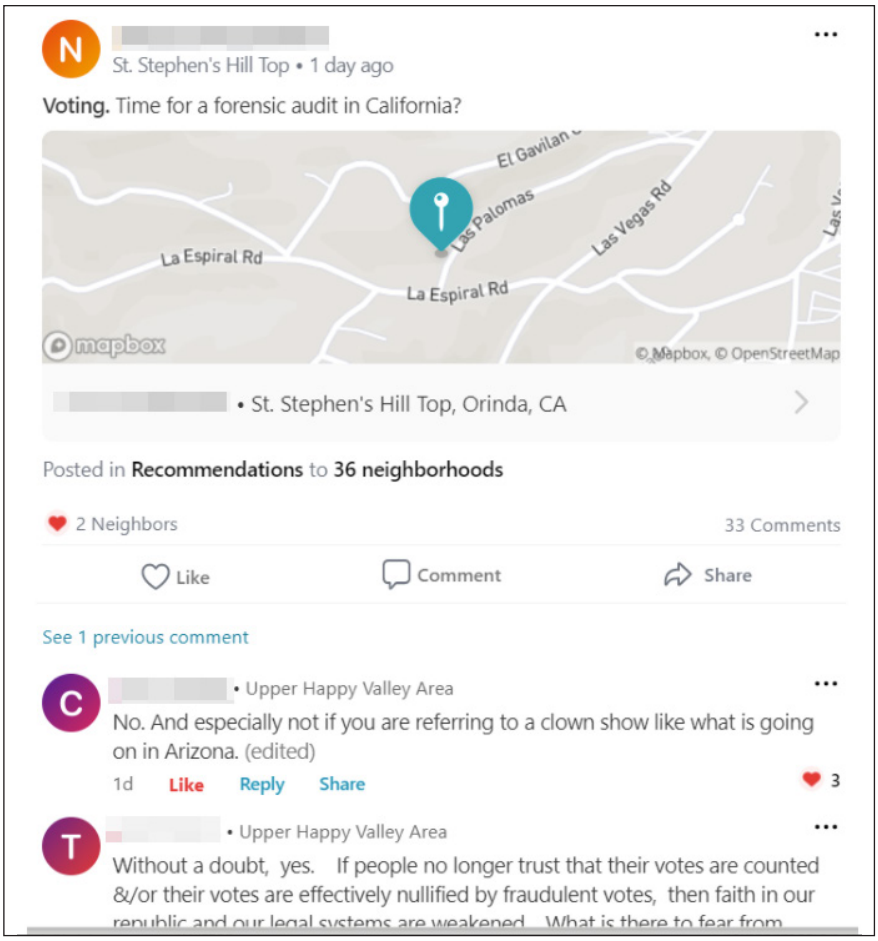

Figure 8: NextDoor. A NextDoor user calls for a "forensic audit."

Many social media platforms are a hybrid. Facebook, the platform with the largest user base in the United States, is a hybrid with both open and closed content. Open content on Facebook consists of posts by users on their own profile or page (as long as they are set to be publicly viewable). Closed content on Facebook includes not only direct messages but also groups. Groups have been growing in importance on Facebook. Between February 2017 and April 2019, active users of Facebook groups grew from 100 million people to 400 million people.[66] Groups have many different privacy settings,[67] but often their content is "private"—that is, only the users of those groups can see that content (though it appears through the main "news stream" of content when they log into Facebook). The upshot is that while some Facebook content is public (and searchable if, and only if, you have access to their CrowdTangle tool), that search will return only a portion of the content on the platform.

Telegram is another hybrid, combining encrypted one-on-one instant messaging, public posts (one-way broadcasts), and both public and private groups.[68] Telegram is most similar to WhatsApp in appearance and messaging functions but has channels where users can broadcast one-way posts, as well as capabilities for massive group chats in these channels. Posts on public groups can be forwarded to other channels and users. Because of these features and the encryption it

provides, Telegram has been a vital tool to organize against authoritarian rulers.[69] Recently, Telegram has been used by many right-wing activists and white supremacists in the United States **(see Figure 9)**.

A core tenet of social media is that users can create content that is seen, immediately, by other users. This means that any social media platform or user-generated content platform is a potential vector for election disinformation. Throughout our Stopping Cyber Suppression program, our monitoring efforts found mis- and disinformation on mainstream platforms like Facebook and Twitter, and on platforms with smaller user bases like NextDoor. We even found an example of election disinformation on the online tag function of the companion app to the Peloton exercise company **(see Figure 10)**. Peloton later banned the use of the "Stop the Steal" tags.[70]

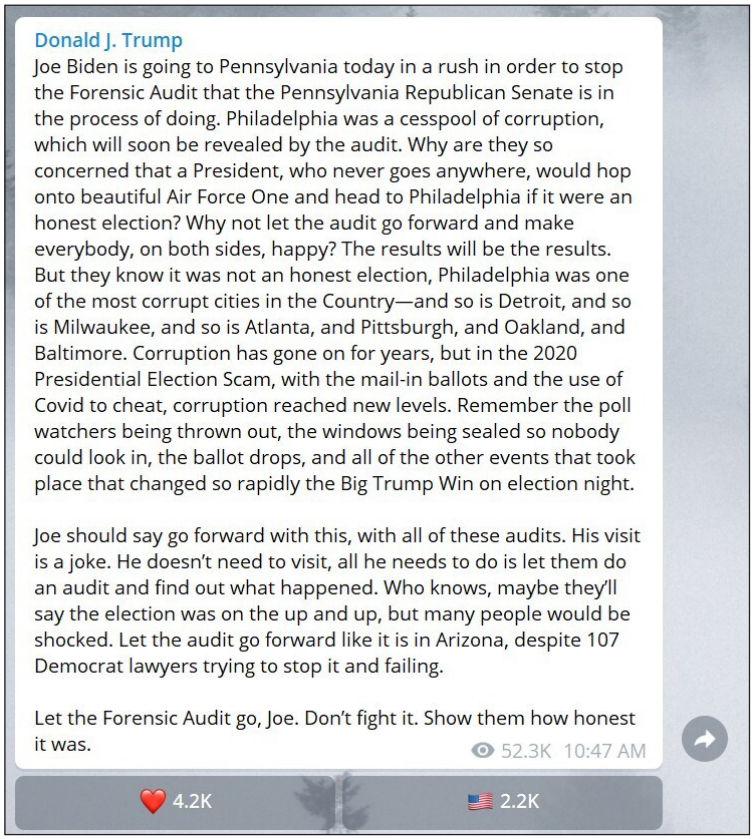

Figure 9: Telegram. This is an example of how Trump uses other social media networks to continue to spread his disinformation about 2020.

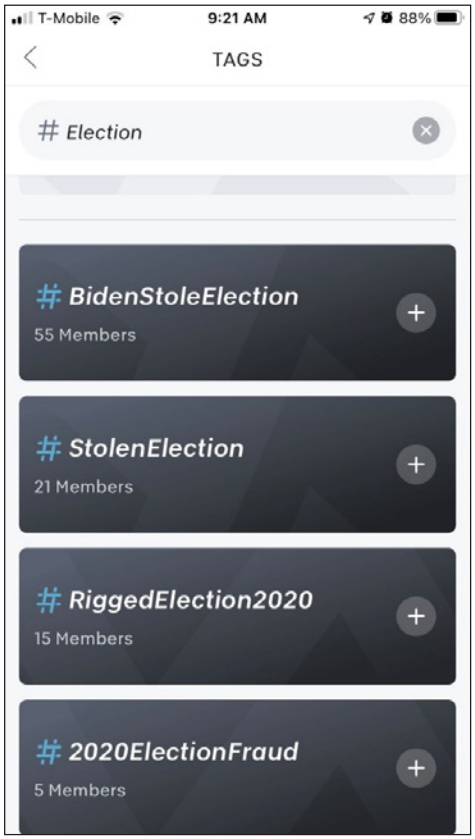

Figure 10: Peloton

Only the social media companies themselves have full access to the content and therefore are the only ones who would conclusively know how much election disinformation appeared on their platforms. A report from Stanford University found disinformation in the 2020 elections across multiple platforms.[71]

Facebook, as the social media platform with the largest user base in the United States (and worldwide), is the most important platform when it comes to preventing the spread of disinformation. According to Facebook's own reporting, between March 1 and November 2, 2020, Facebook applied some kind of label or warning to 180 million posts that shared election mis- or disinformation and removed 265,000 pieces of content for breaking the company's rules against voter interference **(see Figure 11).**[72]

Figure 11: Facebook. Here, a filing from a vote suppression group is used as proof of "voter fraud."

YouTube is owned by Google and is one of the most popular online platforms in the United States, used by seven-in-ten Americans including 26% of U.S. adults who get news there.[73] YouTube hosted videos that promoted election disinformation that had significant views: one study showed that YouTube was a key vector for disinformation used on other platforms, where Twitter users would tweet out disinformation-filled YouTube videos.[74] An independent analysis of YouTube videos revealed that during the week of November 3, 2020, videos supporting the false claim of widespread election fraud were viewed more than 138 million times.[75] YouTube's ability to grow a large audience quickly has helped spread election disinformation narratives. A group of pro-Trump channels connected to the far-right newspaper *Epoch Times* that launched on November 10, 2020, grew to 200,000 subscribers and 11 million views in less than two months with videos that contained election disinformation.[76]

From September to December 9, 2020, YouTube claimed to have removed "8000 channels and thousands of harmful and misleading elections-related videos for violating our existing policies."[77] While YouTube also pledged to disallow any "content alleging widespread fraud or errors changed the outcome of a historical U.S. Presidential election,"[78] research found that many election disinformation videos remained on the platform **(see Figure 12).**[79]

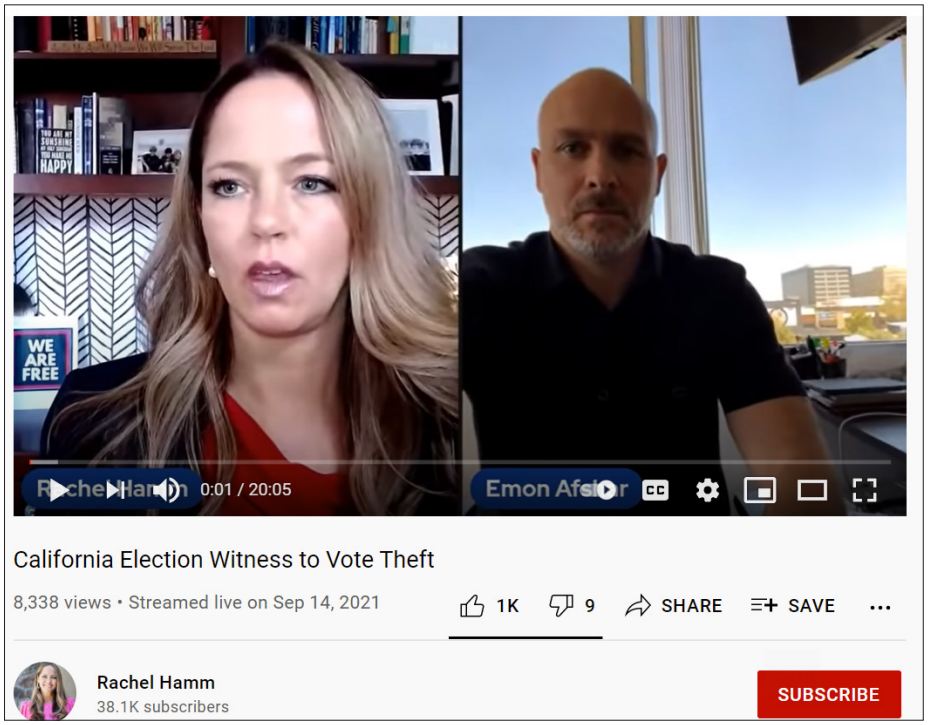

Figure 12: YouTube. In this video, a woman running for secretary of state claims votes were stolen in the California recall based on the experiences of the man interviewed.

Twitter has fewer users than Facebook and YouTube but maintains an important place in the rapid sharing and spreading of election disinformation. Most tweets are public and can be easily searched. And Twitter's application programming interface, which opens Twitter's data and functionality to external third parties, is accessible to social media monitoring tools and researchers, making it much easier for independent researchers (and Common Cause's Social Media Monitoring volunteers) to find and report disinformation. Twitter released a report that claimed it labeled 300,000 tweets containing "disputed and potentially misleading" information about the election between October 27 and November 11, 2020.[80] Twitter has not released any additional reports **(see Figure 13)**.

TikTok, a popular video app, also took measures against election disinformation. Despite reporting in February 2021 the removal of over 300,000 videos for election disinformation, it continues to surface videos to users that contain false claims **(see Figure 14).**[81] TikTok boasts up to one billion monthly users, and videos posted by users and surfaced to audiences via the algorithmic For You Page can receive thousands of views and shares before they are removed, even with a robust enforcement policy that acts to take them down within hours.[82]

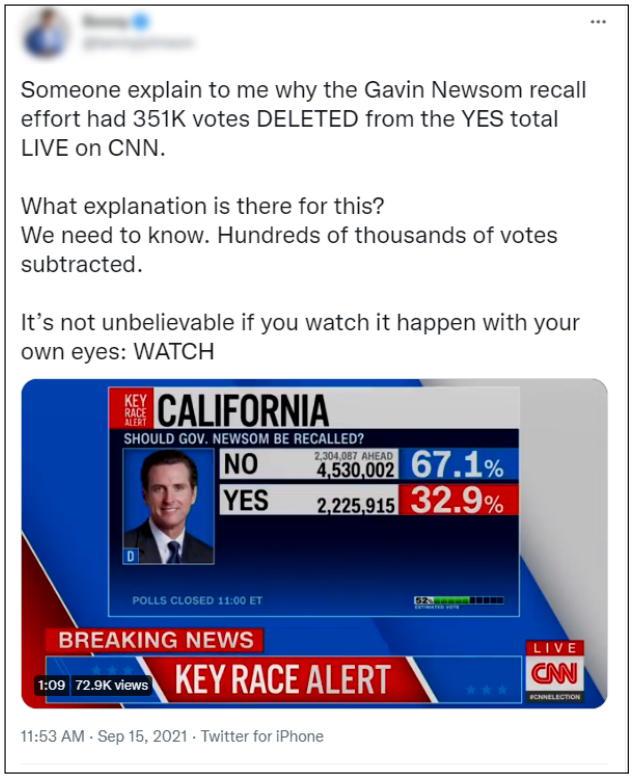

Figure 13: Twitter. Here, a popular conservative influencer claims that votes were deleted live on CNN.

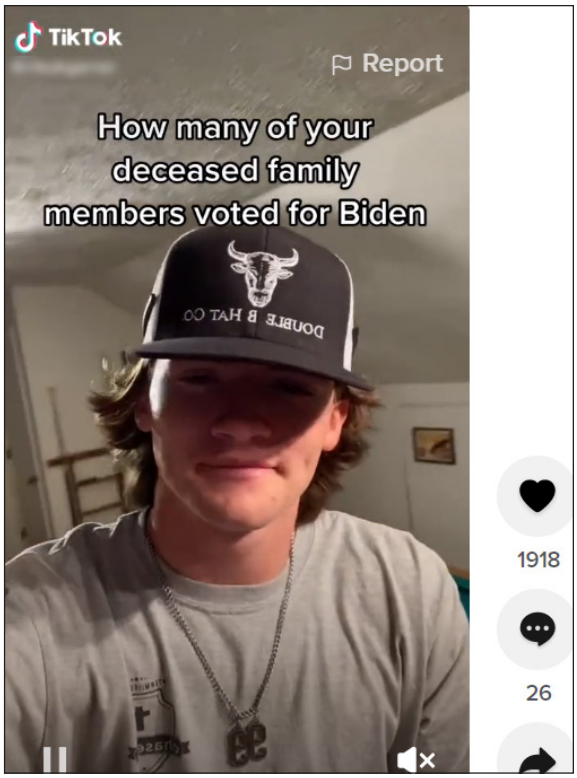

Figure 14: TikTok. A TikTok user posts a commonly used trope about "dead voters."

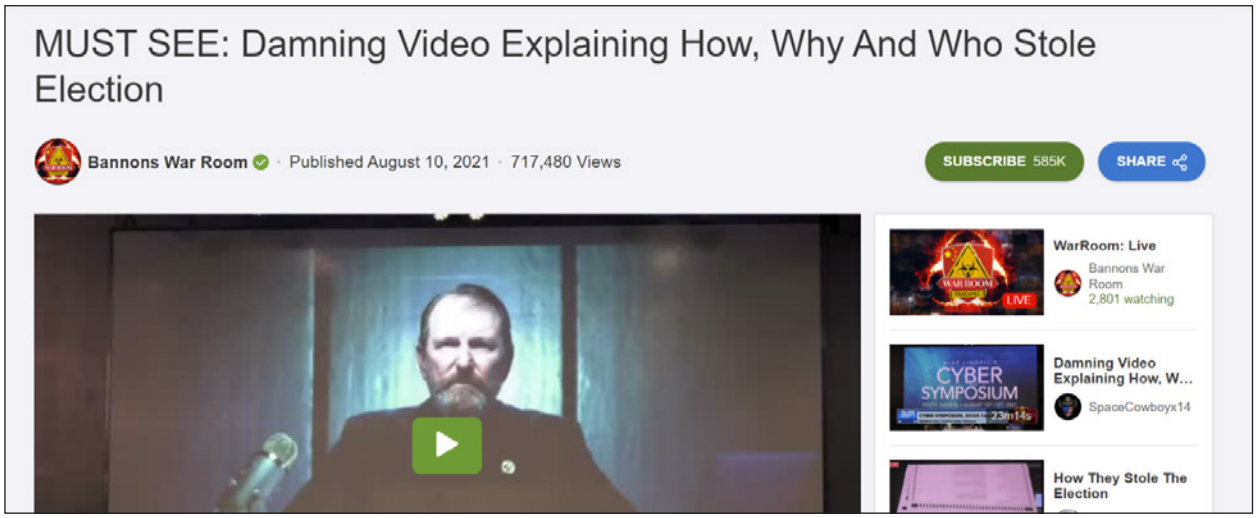

Figure 15: Rumble. Steve Bannon's show earned almost a million views with this video on "how, why, and who stole election."

Rumble is a video platform where users upload videos that can be monetized and licensed. Rumble is now the home of many viral right-wing disinformation videos, such as Steve Bannon's Pandemic War Room show, which has almost 600,000 subscribers and frequently posts clips making false claims about the 2020 presidential election **(see Figure 15)**. Analyses of Rumble show that it surfaces QAnon and conspiracy content to users at rates higher than accurate and

factual information, exposing its millions of monthly users to disinformation on a variety of subjects. According to one analysis, searching the word "election" on the platform led to two times the amount of disinformation as correct information.[83]

Who Is Spreading Election Disinformation and Why?

Few who intentionally spread election disinformation would publicize this fact because the behavior is sometimes illegal and always despicable. The ability of individuals to anonymously spread election disinformation is part of the problem—and strengthening transparency laws as recommended later in this report is part of the solution. Nevertheless, here is what we know about those spreading election disinformation in recent years.

Both foreign and domestic actors have used—and likely will continue to use—election disinformation. During the 2016 elections, the Russian Internet Research Agency created numerous posts on multiple social media platforms. According to the U.S. Senate Select Committee on Intelligence, this foreign interference was "at the direction of the Kremlin" and created social media content in support of then-candidate Trump and against Hillary Clinton.[84] In particular, the content was "principally aimed at African-Americans in key metropolitan areas."[85] Russian disinformation efforts included the use of the Facebook page Blacktivist, which purported to be a Black empowerment page and garnered 11.2 million engagements with Facebook users.[86] Both advertisement and organic (non-ad) content was published through this program. This Russian social media content was designed to drive divisions between voters and cause general political instability in the United States, a tactic that differed from more direct efforts to disenfranchise voters used by some other purveyors of election disinformation.[87]

Russian disinformation efforts included the use of the Facebook page Blacktivist, which purported to be a Black empowerment page and garnered 11.2 million engagements with Facebook users.

Whereas Russia's 2016 election interference exploited fissures between U.S. social groups, foreign interference by Russia and others in our 2020 election primarily entailed amplifying existing election disinformation narratives created by other bad actors, including then-president Donald Trump. As noted previously, intimidating emails sent to voters in 2020 purported to be from the white supremacist Proud Boys organization, but the Department of Homeland Security investigated and accused Iran of producing them.[88] Russian media in 2020 capitalized on the false narratives Trump and others spread about a "rigged" election and vote by mail in particular.[89] A report from the director of National Intelligence found that in the 2020 elections, Iran and Russia "spread false or inflated claims about alleged compromises of voting systems to undermine public confidence in election processes and results."[90] These were the same claims that domestic malign actors—including then-president Donald Trump and his party—were actively spreading.

Notwithstanding some foreign involvement in the spread of election disinformation in the United States, **the vast majority of election disinformation that plagues our politics appears to originate with and is amplified by domestic sources.**

A number of social scientists are working to understand the psychology behind individuals spreading disinformation. In our observations, gleaned from over 15,000 volunteer hours spent monitoring social media for mis- and disinformation during the 2020 election cycle, we have found that election **misinformation** is often spread by those sincerely attempting to be helpful in a climate of uncertainty and distrust (particularly when it came to the USPS and its ability to manage vote by mail in the 2020 elections) and **disinformation** is spread by individuals with partisan goals, including intraparty contests, like the Democratic Presidential Primary **(see Figure 16).**[91]

Figure 16: Disinformation image circulated on Twitter with incorrect election date for Super Tuesday primaries, branded as coming from the Biden campaign.

In an age of hyperpartisanship, spreading election disinformation can both serve to attack your political opponents and show that you are aligned with other members of your political tribe. Election disinformation—in particular, the narrative of a rigged election and pervasive voter fraud committed by Democrats—existed long before the rise of Donald Trump but now has become party orthodoxy. You can signal that you are a Trump-supporting "MAGA Republican" (an acronym for Trump's campaign slogan "Make America Great Again") by spreading stories that reinforce a narrative (however false) about a political system rigged against other MAGA Republicans. This creates a negative feedback loop of distrust in government and elections: a September 2021 poll showed that 78% of Republicans believe that Joe Biden did not win the presidency.[92] Numerous states and counties are proceeding with sham ballot reviews—even in areas where Trump won decisively.[93] Among 15 Republican candidates currently running for secretary of state in five battleground states, 10 have "either declared that the 2020 election was stolen or called for their state's results to be invalidated or further investigated."[94] **Election disinformation is spread by activists and candidates in the same way that political messaging and issue priorities used to be.**

While disinformation is spread by a large number of social media platform users, highly influential accounts and pages matter most, as the social media algorithms are more likely to promote content created by a user with a large following. These algorithms have empowered a small number of disinformation "superspreaders" to instigate the bulk of disinformation about COVID-19.[95] There are a few accounts with strong influence on social media that made the biggest contributions to spreading disinformation, and they are almost exclusively conservative. For example, Douglass Mackey, who the *New York Times* describes as a "far-right Twitter troll" and "right-wing

provocateur"[96] with nearly 60,000 Twitter followers, is currently being prosecuted by the DOJ for spreading election disinformation in the weeks leading up to the 2016 presidential general election and seems to have been driven by partisan and anti-Black racist motives.[97] Mackey's stated goal for his Twitter disinformation campaign was to "drive up turnout with non-college whites, and limit black turnout," with memes intended to suppress the votes of Hillary Clinton supporters.[98]

According to the Stanford Election Integrity Partnership's report on mis- and disinformation, "Influential accounts on the political right rarely engaged in factchecking behavior, and were responsible for the most widely spread incidents of false or misleading information in our dataset."[99] That included 15 "verified" Twitter accounts including Eric Trump, Donald Trump, Donald Trump Jr., and social media influencers like James O'Keefe, Tim Pool, Elijah Riot, and Sidney Powell.[100] Similarly, an analysis by the advocacy group Avaaz concluded that Facebook missed an opportunity to dramatically limit election disinformation by acting early on a select few accounts and content. The report noted that "the top 100 false or misleading stories related to the 2020 elections" were viewed 162 million times in three months. Moreover, Avaaz researchers found that 100 of the top Facebook pages that have spread disinformation were viewed more than 10 billion times between March and October.[101]

Wealthy conservatives with partisan motives spend big money, both directly and through "dark money" groups, to spread election disinformation. Jane Mayer, a preeminent investigative journalist for the *New Yorker* covering money in politics and author of the 2017 bestseller book Dark Money, recently turned her attention to the funding of election disinformation.[102] Mayer cites the conservative Lynde and Harry Bradley Foundation, with its $850 million endowment, as a major funder of recent election disinformation efforts through numerous nonprofits, including the Heritage Foundation, American Legislative Exchange Council, Honest Elections Project, Election Integrity Project California, and FreedomWorks.[103] Mayer also cites multimillionaire founder of Overstock.com, Patrick Byrne, as a purveyor of election disinformation in the form of his film The Deep Rig, which "asserts that the 2020 Presidential election was stolen by supporters of Joe Biden, including by Antifa members who chatted about their sinister plot on a conference call."[104]

Wealthy conservatives with partisan motives spend big money, both directly and through "dark money" groups, to spread election disinformation.

Some Republican politicians are also superspreaders of election disinformation,[105] seemingly motivated by at least two factors, raising money and rationalizing new voter suppression laws—both of which will help them win future elections. As noted earlier, Donald Trump raised more than $100 million peddling the "Big Lie" in the first six months of 2021,[106] and other Republicans have jumped on Trump's election disinformation gravy train. The *New York Times* analyzed campaign finance data from the first quarter of 2021 and observed that "leaders of the effort to overturn Mr. Biden's electoral victory have capitalized on the outrage of their supporters to collect huge sums of campaign cash," singling out Senators Josh Hawley and Ted Cruz, and Representatives Marjorie Taylor Greene and Kevin McCarthy.[107] The authors concluded, "Far from being punished for encouraging the [January 6] protest that turned lethal, they have thrived in a system that

often rewards the loudest and most extreme voices, using the fury around the riot to build their political brands."[108]

Relatedly, since the beginning of the year, calls for "forensic audits" of the 2020 election have gained steam as a means for Trump supporters to allegedly collect evidence of election fraud and for those in right-wing spaces to profit off of these endeavors. The most infamous of these is the recently concluded sham ballot review in Maricopa County, Arizona, which cost up to $7 million and ended up affirming a Biden victory—as expected.[109] The election results in Maricopa County had been accurately counted, certified, and audited by the county, using processes that exist all around the United States to ensure the accuracy and integrity of our elections, before Arizona Senate Republican leaders launched their own Trump-inspired partisan review. In the following section, we profile the Arizona sham ballot review as a case study in election disinformation. And the "audit" push shows no signs of stopping. Ten other states are in various states of either conducting or instigating sham ballot reviews.[110] The end result of these sham ballot reviews isn't renewed confidence in elections but a calcified and further-reinforced belief on the part of Trump supporters that there is a "there" there, and to keep their attempts to undermine the election process going.

Disinformation Case Study: Arizona Sham Ballot Review

Late in September, national media outlets delivered expected news. A Republican-commissioned review of nearly 2.1 million ballots cast in Arizona's November 2020 election, carried out over many months by a wholly unqualified firm known as Cyber Ninjas, was finally over and reaffirmed what we already knew: Joe Biden won Maricopa County.[111] Arizona's sham ballot review illustrates the many facets and problems of election disinformation—a perfect case study.

Veteran voting rights advocate and lawyer Ralph Neas oversaw a study of the Arizona process for the nonpartisan Century Foundation and explained that though the process was a "farce," it may nonetheless have "extraordinary consequences."[112] Neas explained: "The Maricopa County audit exposes exactly what the Big Lie is all about. If they come up with an analysis that discredits the 2020 election results in Arizona, it will be replicated in other states, furthering more chaos. That will enable new legislation. Millions of Americans could be disenfranchised, helping Donald Trump to be elected again in 2024. That's the bottom line. Maricopa County is the prism through which to view everything. It's not so much about 2020—it's about 2022 and 2024."[113]

There has been, and will continue to be, a strategic effort to spread disinformation by bad actors about the 2020 election using the Arizona Maricopa County sham ballot review process. This disinformation is being promoted and amplified through major social media platforms, including Twitter and Facebook. Bad actors point to Facebook and Twitter disinformation content as evidence of the validity of their conspiracy theories and share this content on Telegram and other spaces where they are organizing their efforts, creating an echo chamber of disinformation.

We've found examples of disinformation about the Arizona sham ballot review on Twitter and Facebook, but also other platforms like Telegram. QAnon influencers and audit supporters repost the @ArizonaAudit Twitter account content and other misinformation to various other platforms, ranging from Instagram to Telegram.

A large portion of online organizing and chatter surrounding the review is happening on Telegram, where users can discuss the stolen election myth without fear of violating platform policies (Telegram has no prohibition against election disinformation).[114] A critical component of these discussions is the sharing of screenshots or original posts from Twitter. In the first example, the @ArizonaAudit tweet is shared on a popular QAnon influencer's Instagram account **(see Figure 17)**. In the second, an accusation about Arizona secretary of state Katie Hobbs is disseminated from Twitter into the rumor mill of Telegram **(see Figure 18)**.

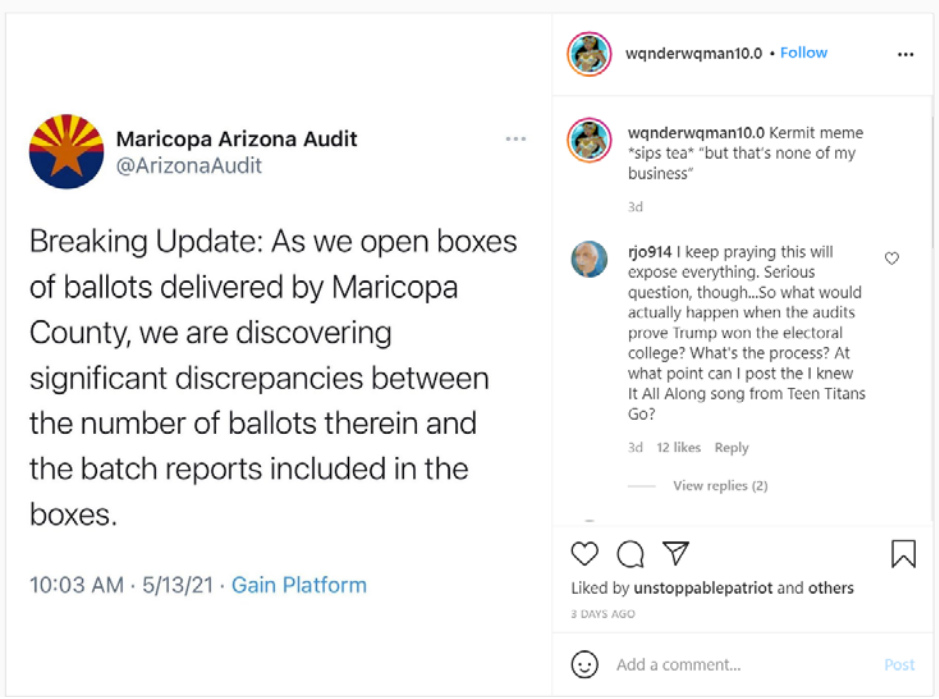

Figure 17: Instagram post of @ArizonaAudit tweet.

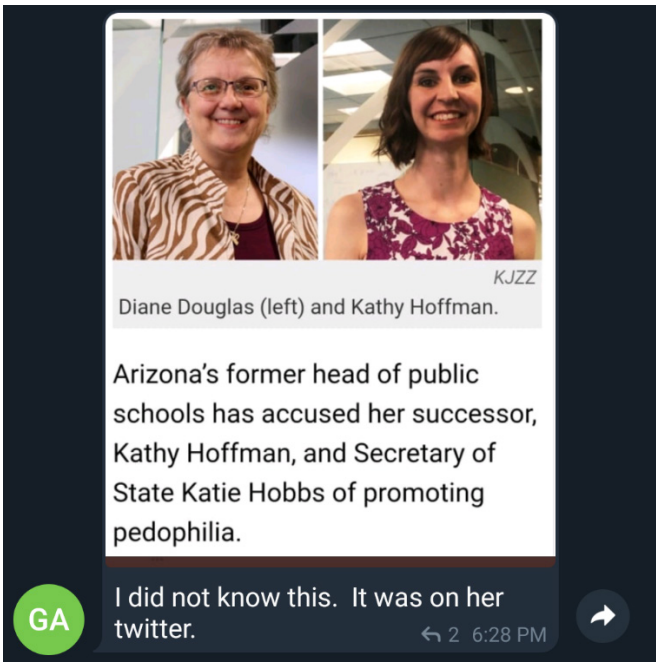

Figure 18: Telegram post republishing disinformation from Twitter.

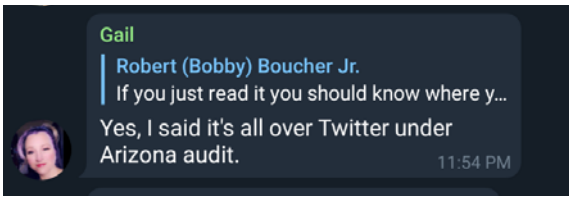

Figure 19: Telegram post referring to disinformation on Twitter.

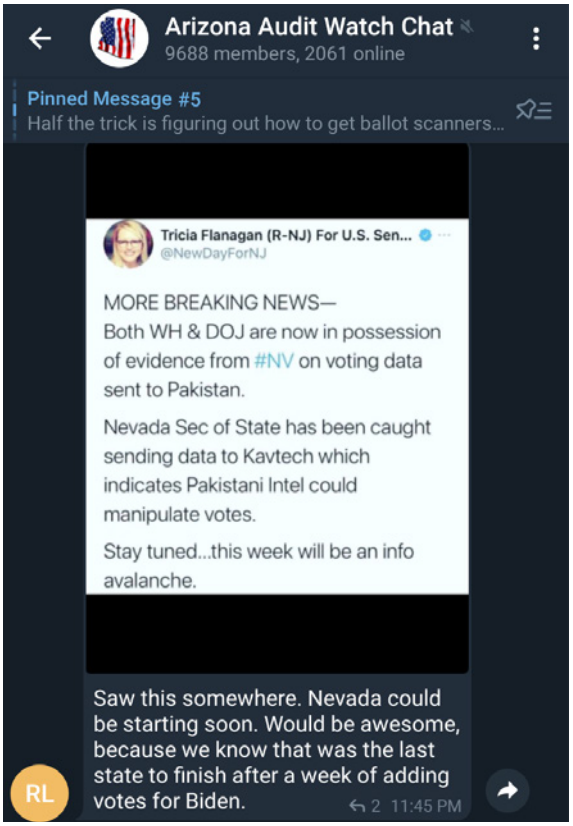

Figure 20: Telegram post sharing disinformation tweeted by congressional candidate.

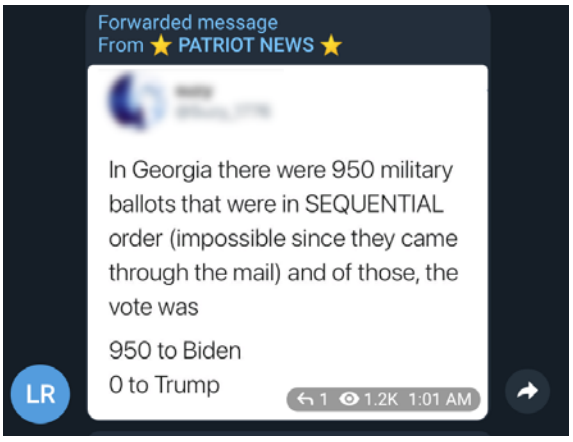

Figure 21: Telegram post forwarding debunked election disinformation.tweeted by congressional candidate.

Users on Twitter and Facebook are able to go viral making debunked claims[115] about the Arizona audit, such as the viral claim that there were 250,000 "illegal votes" found or that databases were deleted.[116]

This disinformation doesn't stay on Twitter or Facebook—it migrates to a new home on Telegram, where users add commentary and further radicalize. As seen in **Figure 19**, two users are debating in a Telegram chat for the Arizona audit (that boasts 14.3k members) where to find sources. One tells the other, "it's all over Twitter under Arizona audit." In **Figure 20**, a screenshot of viral disinformation from a verified congressional candidate account is shared in the same chat. In the third example, **Figure 21**, a forward of yet another debunked claim[117] is shared. Finally, CodeMonkeyZ (Ron Watkins, major QAnon influencer), shared Rep. Paul Gosar's (R-AZ) claims about fraudulent Arizona votes to his 245,000 followers on Telegram **(see Figure 22)**.

In some cases, they organize online actions, such as Twitter hashtags. For example, the hashtag #FraudVitiatesEverything is based on a saying coined by CodeMonkeyZ (Ron Watkins, major QAnon influencer), who says it as a claim that the election will be overturned due to fraud **(see Figure 23)**.

Figure 22: Telegram post republishing election disinformation tweeted by Rep. Gosar.

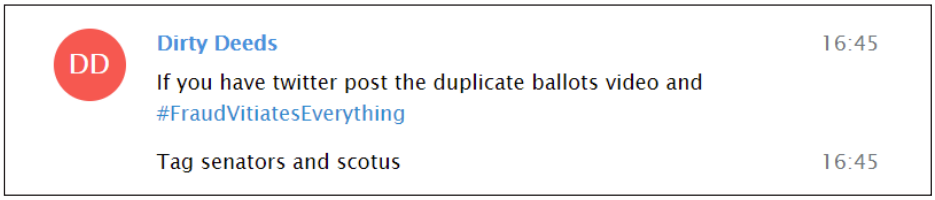

Figure 23: Disinformation hashtag campaign.

Disinformation spreads and jumps between social media platforms regularly. And those spreading disinformation point to mainstream platforms like Facebook and Twitter to show the efficacy of their efforts. A viral tweet or Facebook post is a trophy for a disinformation spreader. Because these platforms have more mainstream users and because they have an active content moderation regime that purports to remove some kinds of disinformation, it is far more dangerous to have disinformation spread on them as they appear to have the imprimatur of truth. In particular, Facebook algorithmically amplifies content to users, even if they didn't specifically ask to receive it, because of their recommendation engine. Facebook's own internal research, according to documents provided by whistleblower Frances Haugen, shows that the divisive, polarizing, angry content—like election disinformation—spreads better and faster than other content. Content is shown to users through algorithmic amplification—invitations to groups, suggested pages to follow and content promoted to users in their feed. Based on the content of the pages users follow, they will have content "pushed" to their newsfeed. According to Haugen, Facebook knows that this can lead users into an experience filled with extremist content—not from their own choosing but from simply following the recommendations of the platform.[118]

Disinformation spreads and jumps between social media platforms regularly.

If election disinformation were limited to a self-selected group of conspiracy theorists, it would continue to be a problem—but a much smaller and more manageable one than the mainstreaming of disinformation currently happening on Facebook and Twitter.

SECTION 2: STATE AND FEDERAL LAWS REGULATING ELECTION DISINFORMATION

Several different bodies of law provide tools for fighting election disinformation. A primary purpose of election disinformation is to suppress and sometimes intimidate voters. Consequently, election laws prohibiting voter intimidation and false election speech play an important role in fighting election disinformation. Several other bodies of law are also critically important to the fight. Strong campaign finance disclosure laws can shine the light of publicity on those seeking to undermine our elections from the shadows and help ensure existing laws are enforced. Communications laws, consumer protection laws, media literacy laws, and privacy laws can all play a part in effectively regulating and deterring election disinformation.

Federal and state laws of all these types are detailed in the following sections, highlighting some of the presently available legal tools for stopping election disinformation. To be certain, current laws across the United States are not entirely up to the task of preventing the increasingly sophisticated election disinformation tactics that will be deployed in 2022 elections and beyond. And there's no single "silver bullet" reform that would fix everything. But there are some important, effective laws on the books today that should be expanded to other jurisdictions and vigorously enforced. Such "best practices" are included in the final section of this report, along with other recommended reforms.

There's no single "silver bullet" reform that would fix everything. But there are some important, effective laws on the books today that should be expanded to other jurisdictions and vigorously enforced.

Voter Intimidation and False Election Speech Laws

Federal law and laws in nearly every state contain provisions explicitly prohibiting voter intimidation, with many of these laws being rightly interpreted as prohibiting election disinformation.

Some states have enacted laws explicitly prohibiting various types of false election-related speech—e.g., false statements about voting procedures/qualifications, candidates, incumbency, endorsements, veteran status, or ballot measure effects. In this report, we focus only on the first of these types: laws prohibiting false statements about voting procedures and qualifications such as where and when to vote. Our reasons are twofold and related to one another.

First, the veracity of statements about voting procedures and qualifications (e.g., the date of the election, the hours polls are open) is easily ascertainable, and determining such veracity can be done in an entirely nonpartisan, objective fashion. By contrast, determining the veracity of statements about a candidate (e.g., a candidate's stance on an issue) is often more subjective, as reflected by the rating systems some prominent fact-checkers use. For example, the Poynter Institute's PolitiFact uses a "truth-o-meter" with six grades: true, mostly true, half-true, mostly false, false, pants on fire.[119]

Second, and relatedly, courts have for years been divided on the constitutionality of laws prohibiting false speech characterizing candidates and ballot measures, with at least two federal appellate courts in recent years striking down such laws as unconstitutionally vague and overbroad.[120] Courts are much more likely to uphold as constitutionally permissible narrower laws prohibiting false statements about the procedures and qualifications of voting. As Professor Richard L. Hasen argued in a 2013 law review article, "The strongest case for constitutionality is a narrow law targeted at false election speech aimed at disenfranchising voters."[121]

The following section summarizes voter intimidation and false speech laws at the federal level and in numerous states. And the recommendations section at the end of this report identifies the best features of these laws, urging their adoption throughout the United States.

Federal Voter Intimidation and False Election Speech Laws

Federal government efforts to protect the right to vote and prevent voter intimidation date back to the period immediately following the Civil War and the creation of the DOJ in 1870[122] and the passage of the Ku Klux Klan Acts in 1870–71.[123] Several federal voting rights laws relate directly to election disinformation and voter intimidation. And though the DOJ has found some forms of voter intimidation to be "difficult to prosecute" because the intimidation is "both subtle and without witnesses,"[124] such is not the case for voter intimidation via election disinformation, which is often blatant and in full public view.

The National Voter Registration Act of 1993 makes it a crime to knowingly and willfully intimidate or threaten any person for voting, registering to vote, or aiding others to register and vote.[125] Another federal criminal statute similarly provides that "[w]hoever intimidates, threatens, coerces, or attempts to intimidate, threaten, or coerce, any other person for the purpose of interfering with the right of such other person to vote" in a federal election has committed a crime subject to fines or imprisonment.[126] The DOJ explains that this statute "criminalizes conduct intended to force prospective voters to vote against their preferences, or refrain from voting, through activity reasonably calculated to instill some form of fear."[127]

Conspiracy to "injure, oppress, threaten, or intimidate any person…in the free exercise or enjoyment of any right or privilege secured to him by the Constitution or laws of the United States"—including the right to vote—is a felony under federal law.[128] This criminal code provision covers voter suppression schemes, **including "providing false information to the public—or a particular segment of the public**—regarding the qualifications to vote, the consequences of voting in connection with citizenship status, the dates or qualifications for absentee voting, the date of an election, the hours for voting, or the correct voting precinct."[129]

In January 2021, the DOJ charged Twitter user Douglass Mackey (a.k.a. "Ricky Vaughn") with violation of this statute for conspiring "to injure, oppress, threaten and intimidate persons in the free exercise and enjoyment of a right and privilege secured to them by the Constitution and laws of the United States, to wit, the right to vote[.]"[130] The DOJ alleges that in the weeks leading up to the November 2016 presidential election, Mackey conspired with others to spread memes on Twitter falsely claiming that Hillary Clinton supporters could vote via text message to a specific phone number included in the memes **(see Figure 24).**[131] At least 4,900 individuals attempted to vote by texting "Hillary" to the number included in the memes.[132] *The New York Times* reported

Figure 24: Voter suppression Twitter meme.

that this "appeared to be the first criminal case in the country involving voter suppression through the spread of disinformation on Twitter" and that the "case will test the novel use of federal civil rights laws as a tool to hold people accountable for misinformation campaigns intended to interfere with elections[.]"[133] The case remains pending as of this writing.

In addition to the federal criminal code provisions detailed in the preceding paragraphs, the **Voting Rights Act of 1965 and other civil rights laws** also prohibit disinformation activities that amount to voter intimidation or suppression. The Voting Rights Act provides that no person "shall intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any person for voting or attempting to vote."[134] For example, this statute was successfully relied on by the DOJ to win a consent decree in a 1990 lawsuit against the North Carolina Republican Party, which had mailed disinformation postcards to 125,000 Black voters throughout the state, incorrectly stating that recipients could not vote if they had moved within 30 days of the election and threatening criminal prosecution.[135]

And as voting rights lawyer Michael Weingartner explains in a forthcoming law review article, recently, some plaintiff victims of election disinformation have turned to a provision of the Ku Klux Klan Acts that provides for an award of monetary damages to victims of conspiracies to prevent giving their "support or advocacy" to federal political candidates.[136] This statute, Weingartner argues, holds promise to "redress modern voter intimidation, deter bad actors, and provide an incentive to plaintiffs to bring suit."

State Voter Intimidation and False Election Speech Laws

The federal laws detailed earlier prohibiting voter intimidation and suppression—including some disinformation tactics—generally apply to any election with candidates for federal office on the ballot. Nearly every state, likewise, has laws prohibiting voter intimidation and suppression, applicable to elections even when no federal office candidates are on the ballot. A few states have laws explicitly regulating false election-related speech, and a few others have interpreted more general anti-intimidation laws to prohibit false election speech.

APPENDIX I summarizes the voter intimidation and false speech laws of several states. Among the best state laws worthy of emulating around the nation, **Colorado** law provides that no person shall knowingly or recklessly "make, publish, broadcast, or circulate or cause to be made, published, broadcasted, or circulated...any false statement designed to affect the vote on any issue submitted to the electors at any election or relating to any candidate for election to public office."[137] The Colorado attorney general's guidance makes clear that disinformation tactics—including "misleading phone calls, texts, or emails to a voter"—can constitute illegal voter intimidation."[138]

Similarly, **Hawaii** law provides that any person who "knowingly broadcasts, televises, circulates, publishes, distributes, or otherwise communicates...false information about the time, date, place, or means of voting with the purpose of impeding, preventing, or otherwise interfering with the free exercise of the elective franchise" has committed illegal election fraud.[139]

And **Virginia** explicitly outlaws communicating to a "registered voter, by any means, false information, knowing the same to be false, intended to impede the voter in the exercise of his right to vote," including information "about the date, time, and place of the election, or the voter's precinct, polling place, or voter registration status, or the location of a voter satellite office or the office of the general registrar."[140] Importantly, Virginia law includes a private right of action for registered voters to whom such false information is communicated, enabling them to seek an "injunction, restraining order, or other order, against the person communicating such false information."[141]

Campaign Finance Laws

In 1933, Supreme Court Justice Lewis D. Brandeis famously wrote, "Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."[142]

The Supreme Court cited this Brandeis quote in its 1976 seminal campaign finance law decision *Buckley v. Valeo* in which the Court upheld as constitutionally permissible federal campaign finance disclosure requirements.[143] While many of those spending money to spread election disinformation prefer to hide in the shadows, knowing that disclosure of their identity would dishonor them and make clear their partisan motivations, strong campaign finance laws can force them into the light of day. The Buckley Court explained that "disclosure provides the electorate with information...in order to aid the voters in evaluating those who seek federal office" and informing voters of the "sources of a candidate's financial support [to] alert the voter to the interests to which a candidate is most likely to be responsive[.]"[144] Disclosure laws also "deter actual corruption and avoid the appearance of corruption by exposing large contributions and expenditures to the light of publicity."[145] Such exposure, the Court reasoned, "may discourage those who would use money for improper purposes either before or after the election."[146]

For nearly a half-century, federal and state courts around the nation have stood by the Buckley Court's reasoning. Just last month, a federal appellate court upholding a challenged disclosure law wrote, "A well-informed electorate is as vital to the survival of a democracy as air is to the survival of human life."[147]

Federal Campaign Finance Disclosure Laws

Federal law imposes thorough disclosure requirements on candidates, political parties, and other political committees. They must disclose the name and other identifying information of any donor who contributes more than $200, as well as any recipient of a payment exceeding $200 from the candidate or committee.[148] They must also include a "paid for by" disclaimer on any public communication they pay to distribute.[149] Consequently, if a candidate, party, or other political committee is paying to distribute disinformation, the public can know about it.

However, federal law disclosure requirements are weak and ineffective with respect to individuals and nonpolitical committee organizations such as so-called 501(c)(4) social welfare organizations, labor unions, and trade associations like the U.S. Chamber of Commerce. Only a narrow range of political spending by such organizations triggers disclosure and disclaimer requirements. Unless an ad expressly advocates[150] the election or defeat of a candidate (e.g., vote for candidate Smith), mentions a candidate and is aired on TV or radio in close proximity to an election,[151] or solicits a contribution to a candidate or political committee,[152] such ads are not subject to federal campaign finance law disclosure and "paid for by" disclaimer requirements.

In other words, **federal law leaves plenty of opportunities for individuals and nonpolitical committee organizations to disseminate disinformation without triggering disclosure or disclaimer requirements**. As long as they stay off TV and radio, and avoid express phrases like "elect Jones," their disinformation campaigns go unregulated by campaign finance law. This is a campaign finance law problem. In the final section of this report, we recommend some solutions.

Another provision of federal campaign finance law related to election disinformation is a statute prohibiting a candidate or employee of a candidate from fraudulently misrepresenting that they are acting for or on behalf of any other candidate or political party in a manner that is damaging to such other candidate or party.[153] The same law likewise prohibits any person from fraudulently misrepresenting that they are "speaking, writing, or otherwise acting for or on behalf of any candidate or political party…for the purpose of soliciting contributions or donations."[154]

However, the Federal Election Commission (FEC) "has a long history of finding no misrepresentation where communications contain disclaimers accurately identifying the true sponsor," unless the body of the communication contains an explicit misrepresentation that "countermands an otherwise accurate disclaimer."[155] Even a technically deficient disclaimer may suffice, so long as the disclaimer accurately identifies the sponsor.[156, 157]

In short, so long as an implicitly misleading political communication contains the required fine print or quickly spoken "paid for by" language at the end, the FEC will likely conclude the communication **does not violate** the "fraudulent misrepresentation" law. This is another area of federal campaign finance law that needs to be strengthened to reduce the spread of election disinformation. We recommend some fixes in the final section of this report, including one reform with bipartisan support among FEC commissioners.

State Campaign Finance Disclosure Laws

Spending in state and local candidate and ballot measure elections is regulated entirely by state (and sometimes local) campaign finance laws. Like federal law, most states' campaign finance laws are quite effective concerning spending by candidates and political committees but deficient when it comes to spending by individuals and nonpolitical committee entities.

APPENDIX II summarizes several states' campaign finance disclosure laws relevant to election disinformation. **Alaska has enacted one of the nation's most effective laws for tracing the source of funds** spent on election advertising by groups, including those that do not qualify as political committees,[158] requiring such groups to disclose the identity of any contributor who has given the group more than $250 in the aggregate during the calendar year "for the purpose of influencing the outcome of an election," as well as all election-related contributions and expenditures made by such groups, including contributions to other such groups.[159] The purpose of this statute is to reveal contributors whose funds are transferred through multiple organizations before being spent on election advertising—contributors who would evade disclosure under most jurisdictions' laws.

California has likewise led the way in recent years, strengthening campaign finance disclosure laws applicable to common sources and types of election disinformation. In 2014, the state strengthened disclosure laws applicable to "multipurpose organizations" spending money to influence California elections (e.g., 501(c)(4) social welfare organizations, often referred to as "dark money" organizations because, in most jurisdictions, they are not required to publicly disclose their funders).[160] And in 2018, California took another step by enacting the "Social Media DISCLOSURE Act,"[161] strengthening disclosure requirements by requiring "paid for by" disclaimers on a broad array of political advertising disseminated via social media platforms. The state's campaign finance regulatory agency, the California Fair Political Practices Commission, has done a good job implementing these laws and continually monitoring evolving campaign finance practices in an effort to keep state campaign finance laws and policies up to date.

California has likewise led the way in recent years, strengthening campaign finance disclosure laws applicable to common sources and types of election disinformation.

Maryland,[162] **Minnesota,**[163] and **Rhode Island**[164] have also enacted legislation requiring certain tax-exempt organizations that are often the source of undisclosed "dark money" political spending in other jurisdictions to disclose their donors and political spending.

Finally, the state of **Washington has some of the strongest disclosure laws in the nation applicable to election disinformation and other digital political advertising**.[165] Washington Public Disclosure Commission regulations provide for modified "paid for by" disclaimers on certain digital ads[166] and require online platforms that sell paid political advertising to provide the public with access to detailed digital ad information.[167]

Federal Communications Laws

Section 230 of the federal Communications Decency Act has long provided digital platforms with legal protections to moderate content online without fear of liability.[168] Section 230 immunizes websites, including internet platforms such as Facebook and Twitter, from liability as a publisher of third-party content.[169] The statute's "Good Samaritan" provision has two primary components that are often described as a "shield and sword." First, Section 230 shields websites from lawsuits regarding content posted by third parties on their platform.[170] For example, Facebook would be protected from lawsuits under the statute for third-party user posts hosted on their platform. Second, the statute provides platforms with a sword to remove content they determine is obscene, violent, or otherwise objectionable without fear of liability.[171]

The broad protections the statute provides empower platforms to take down disinformation while also providing them cover should they choose to leave the misleading content in question up. However, because platforms have broad discretion to moderate content without fear of liability, they are more likely to leave offending content up instead of taking it down.[172] We saw this time and time again during the 2020 election season. A report on Facebook's content moderation failures from advocacy group Avaaz found that Facebook's failure to take down misinformation resulted in over 10.1 billion estimated views of content from top-performing pages that repeatedly shared misinformation over the eight months before the U.S. elections.[173] Common Cause's research found many examples of social media posts generating high engagement on provably false claims that are similar to posts that were labeled or removed months prior.[174]

A report on Facebook's content moderation failures from advocacy group Avaaz found that Facebook's failure to take down misinformation resulted in over 10.1 billion estimated views of content from top-performing pages that repeatedly shared misinformation over the eight months before the U.S. elections.

In the 117th Congress, both Democrats and Republicans have proposed to modify or outright repeal Section 230,[175] but as of this writing, none of these proposals have been passed into law. Introduced legislation generally falls into a few different categories: (1) bills that limit the scope of Section 230, (2) bills that impose new obligations on companies that want to use Section 230 as a defense, (3) bills that want to make changes to the "Good Samaritan" provision of Section 230, and (4) bills that repeal Section 230 outright.[176] A number of bills introduced by Republicans, like Representative Louie Gohmert's (R-TX) Abandoning Online Censorship Act[177] and Senator Bill Hagerty's (R-TN) 21st Century Foundation for the Right to Express and Engage in (FREE) Speech Act,[178] would repeal Section 230 outright. These proposals are often predicated on the false idea that social media platforms are "censoring" conservatives, and this is reflected in public statements from the sponsors of the legislation.[179] Other proposals are bipartisan and would make less drastic changes to Section 230. For example, the Platform Accountability and Consumer Transparency Act, introduced by Senator Brian Schatz (D-HI) and Senator John Thune (R-SD), would condition Section 230 immunity on the publication of an acceptable use policy that would detail the types of content the provider allows, explain how the provider enforces its content policies, and describe

how users can report policy-violating or illegal content.[180] Most recently, Representatives Frank Pallone (D-NJ), Mike Doyle (D-PA), Jan Schakowsky (D-ILL), and Anna Eshoo (D-CA) announced that they would be introducing legislation that would amend Section 230 to remove immunity for platforms that knowingly or recklessly use an algorithm or other technology to recommend content that materially contributes to physical or severe emotional injury.[181]

As demonstrated by the number of proposals introduced in the 117th Congress, no one has a silver bullet solution to reforming Section 230 given the challenges and unintended consequences amending the statute could create. If Congress amends the statute, it could significantly limit free expression online, diminish the internet as a tool for grassroots mobilization, and open the door to liability for smaller websites and online companies, further cementing the dominance of large social media platforms.[182] Therefore, any Section 230 reform deserves careful and nuanced consideration.

Federal Consumer Protection Laws

The Federal Trade Commission (FTC) is charged with protecting consumers and promoting competition.[183] Its primary consumer protection authority comes from Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[184] An "unfair" act or practice is defined as an act or practice that causes or is likely to cause substantial injury to consumers, cannot reasonably be avoided by consumers, and is not outweighed by countervailing benefits to consumers or competition.[185] A representation, omission, or practice is "deceptive" if it "is likely to mislead consumers acting reasonably under the circumstances and is material to consumers—likely to affect the consumer's conduct or decision with regard to a product or service."[186]

Historically, the FTC's Bureau of Consumer Protection has used its Section 5 authority to bring enforcement actions for a wide range of privacy and data security violations, such as deceptive data collection and failure by a company to adequately assess and address data security risks.[187] Remedies include requiring violators to implement comprehensive privacy and security programs, deletion of illegally obtained consumer information, and providing robust transparency and choice mechanisms for consumers.[188]

Bad actors have exploited unfair and deceptive data collection practices to help spread disinformation, and the FTC has used its authority to enforce against these actions. In 2016, for example, political data analytics and consulting company Cambridge Analytica used an app to collect the personal data of millions of Facebook users without their consent.[189] The company was able to find out where people worked, what they looked like, where they lived, what kind of car they drove, who they've voted for in past elections, what kind of music they liked, how much money they made, whether or not they were married, whether or not they owned a gun, and more all without their consent.[190] This data was then used to develop psychological profiles to

Bad actors have exploited unfair and deceptive data collection practices to help spread disinformation, and the FTC has used its authority to enforce against these actions.

help the Donald Trump and Ted Cruz presidential campaigns target voters with false or misleading political ads and allowed other bad actors to spread disinformation.[191]

The FTC launched an investigation into both Cambridge Analytica and Facebook for engaging in deceptive acts and practices in violation of Section 5 of the FTC Act. The investigation into Facebook culminated in a $5 billion penalty against the company for violating a 2012 consent decree, which prohibited Facebook from making misrepresentations about the privacy or security of its users' personal information.[192] Facebook had undermined user privacy preferences by deceiving users when the company shared the data of users' Facebook friends with third-party developers and by misrepresenting the ability of users to control the use of facial recognition technology with their accounts, among other violations.[193] The FTC also issued an opinion and order finding that Cambridge Analytica engaged in deceptive practices to harvest the personal information of tens of millions of Facebook users for voter profiting and targeting.[194] The FTC's order prohibits Cambridge Analytica from making misrepresentations about the extent it protects the privacy and confidentiality of personal information.[195]

The investigation into Facebook culminated in a $5 billion penalty against the company for violating a 2012 consent decree, which prohibited Facebook from making misrepresentations about the privacy or security of its users' personal information.

While the FTC has broad authority to enforce against unfair and deceptive practices, there are limits to the effectiveness of its current enforcement capabilities. First, the FTC is limited in its ability to seek civil penalties for first-time violations of Section 5, and in many cases, the agency levies penalty fines against companies for violations of consent decrees.[196] Second, the FTC is severely limited in its resources—its budget is roughly $350 million,[197] and it only has around 40 staffers working on privacy issues.[198] This pales in comparison to the budgets of other privacy enforcement agencies around the world.[199] If the FTC is to meaningfully protect consumers from a myriad of privacy violations, many of which lead to the spread of disinformation, it will need adequate funding. Finally, the FTC's current enforcement actions have proven inadequate in changing the business models and practices of the largest online companies. For example, Facebook's stock went up after the agency imposed a record-breaking $5 billion fine on the company.[200] As then-FTC commissioner Rohit Chopra noted in his dissenting statement, the $5 billion settlement imposes no meaningful changes to the company's structure nor does it include any changes to the company's surveillance and advertising practices that exposed millions of users to propaganda, manipulation, and discrimination.[201] Future FTC oversight and enforcement must be able to address corporate business models that lead to the spread of disinformation and other harmful content.

State Media Literacy Laws

People of all ages need media literacy skills now more than ever to tackle the myriad of problems caused by disinformation. In 2019, a Stanford University study found 52% of students assessed

believed a grainy video claiming to show ballot stuffing in the 2016 Democratic primaries (the video was actually shot in Russia) constituted "strong evidence" of voter fraud in the United States and concluded today's high school students "lack the skills to judge the reliability of information online."[202] Teaching media literacy in K–12 schools is critical to providing young people with the skills they need to navigate the internet, critically evaluate the content received and consumed online, and protect them from misinformation.[203]

Students are not the only cohort that needs media literacy skills. Older individuals have been found to engage with fake news at a disproportionately higher rate than younger people, and a study of Twitter during the final month of the 2016 presidential election showed users over 50 were overrepresented among users responsible for spreading 80% of fake content.[204] Given that older individuals are more likely to register and vote, it is equally as important that this group is able to learn media literacy skills.[205]

While not a silver bullet by any stretch of the imagination, a greater emphasis on the skills necessary to discern trustworthy from untrustworthy opinion, fact from opinion, news from infotainment, and real information from misinformation will go a long way toward protecting our democracy.[206]

As of August 2021, roughly 15 states have some variation of media or information literacy laws on the books. APPENDIX III summarizes several of these states' laws. States have taken a wide variety of approaches, including requiring media literacy classes in schools, providing resources for teachers, and developing state media literacy committees.[207] Earlier this year, for example, **Illinois** passed a media literacy law requiring every public high school in the state to include in its curriculum a unit of instruction on media literacy, **making it the first state to mandate media literacy classes**.[208] And in 2019, **Colorado** created a media literacy advisory committee within the Colorado Department of Education, which later that year submitted a report to the General Assembly recommending revision of Colorado academic standards, provision of materials and resources to teachers, and legislation to support effective implementation of media literacy programs in schools throughout the state.[209]

Earlier this year Illinois passed a media literacy law requiring every public high school in the state to include in its curriculum a unit of instruction on media literacy, making it the first state to mandate media literacy classes.

Media literacy laws have gained traction in the past few years because they do not run into the same First Amendment concerns that other laws designed to target misinformation may face.[210] Additionally, media literacy laws are often able to find bipartisan support, as most of the laws discussed earlier were enacted with support from both Republicans and Democrats in their respective state legislatures. State governments should study best practices around media literacy in collaboration with expert organizations like PEN America and experiment with legislation based on best practices.

State Privacy Laws

Privacy laws (or lack thereof) play an important role in how misinformation is allowed to spread on the internet and how we can combat it. Access to personal data gives bad actors the ability to target individuals with a precision that has never been seen before. Without detailed data about a user's political beliefs, age, location, and gender, it is far more difficult for bad actors to target them with disinformation.[211] To quote Alex Campbell in his piece for *Just Security,* "Fake news becomes a lot less scary if it can't choose its readers."[212]

While efforts to pass a comprehensive federal privacy law have stalled, a few states have passed legislation. These laws vary in scope, but each of them requires a company operating in the state to inform users if they are selling the users' data and gives users the right to access, delete, correct, or move their data.[213]

California became the first state with comprehensive consumer privacy laws on the books when its legislature passed the California Consumer Privacy Act of 2018 (CCPA) and expanded it in 2020 with the Consumer Privacy Rights Act. It provides consumers with the right to know about the personal information a business collects about them, the right to delete personal information collected from them, the right to opt out of the sale of their personal information, and the right to nondiscrimination for exercising their CCPA rights.[214] The CCPA applies to companies that generate more than $25 million a year in revenue; buy, receive, or sell the personal information of 50,000 or more California residents; or derive 50% or more of their annual revenue from selling California residents' personal information.[215] Companies that do not comply can be fined by the California Office of the Attorney General. **The CCPA is considered by advocates to be the strongest of the state privacy laws on the books,** in part because it contains a limited private right of action against certain types of breaches, which allows consumers to directly sue the company committing the breach.[216]

California became the first state with comprehensive consumer privacy laws on the books.

However, while CCPA has some strong elements, it is important to recognize where it (and the other state privacy laws) falls short. Strong, comprehensive privacy legislation should have data minimization requirements limiting what data entities can collect and how that data can be used, as well as civil rights protections that ensure fairness in both automated decision-making and prohibitions on the use of personal data to discriminate on the basis of race, gender, religion, national origin, sexual orientation, gender identity, disability, familial status, biometric information, or lawful source of income.

Colorado is the most recent state to enact privacy legislation, having passed the Colorado Privacy Act (CPA) in July of 2021.[217] The law shares similarities with the privacy laws of Virginia and California, as it also allows consumers to opt out of data collection while requiring companies to disclose what data they collect, what they do with that data, and how long they keep it.[218] Like Virginia's law, Colorado's law applies to entities that "control or process" the information of 100,000 or

more residents or entities that make 50% or more of their gross revenue from the sale of personal data if they hold the information of about 25,000 or more consumers.[219] Also, like the Virginia law, it only applies to "Colorado residents acting only in an individual or household context."[220] One place where the CPA differs slightly from Virginia's law (and California's) is in enforcement. Under the CPA, both the Colorado attorney general and district attorneys have enforcement authority and can bring actions against businesses that violate the law.[221]

The **Virginia** Consumer Data Protection Act (VCDPA) was passed by the Virginia General Assembly in 2021 with bipartisan support. The VCDPA gives consumers the same core rights California's CCPA does but applies to entities that "control or process" the information of 100,000 or more Virginia residents in a calendar year or entities that make 50% or more of their gross revenue from the sale of personal data if they hold information for about 25,000 or more Virginia residents.[222] It provides Virginia residents with the right to confirm if a controller has their data, the right to correct inaccuracies in the data the controller has, the right to have a controller delete personal data provided by or obtained about them, and the right to opt out of having their data used for targeted advertising.[223]

However, unlike California's law, the VCDPA does not contain a private right of action and is written more narrowly, as it only covers individuals acting on their own or in a "household context," not those acting in a "commercial or employment context."[224] The lack of a private right of action is problematic because it means the only party that can enforce the law is the Virginia Attorney General's Office, and the General Assembly only gave the Attorney General's Office $400,000 in additional funding to do so.[225]

SECTION 3: SELECT SOCIAL MEDIA CIVIC INTEGRITY POLICIES

Social media platforms from Facebook to Twitter and YouTube to TikTok have civic integrity policies in place designed to combat disinformation related to elections and other civic processes.[226] These policies often work in tandem with the platforms' other policies, which address things like fraud, violent content, hate speech, and other content the platform may find objectionable.[227] A piece of content may violate multiple policies at once, like a post advocating violence against a specific group.

Platform civic integrity policies primarily focus on prohibiting content that is misleading about how to participate in the civic process. This includes misleading statements or information about the official announced date or time of an election,[228] misleading information about requirements to participate in an election,[229] and content containing statements advocating for violence because of voting, voter registration, or the administration or outcome of an election.[230]

These policies are not exhaustive though and have significant loopholes that allow for certain disinformation-oriented content to stay up on the platforms. This includes narratives contributing to voter suppression, disinformation from world leaders/public figures, and political ads.

This is in part because platforms are frequently changing and updating their policies. For example, the Mozilla Foundation (Mozilla), a nonprofit whose advocacy work includes using data visualization and original reporting to track the ways the internet is helping and hurting users around the world, found that during the 2020 election cycle (October 2019 through January 2021), Facebook changed its election-related misinformation policies 21 times, Twitter changed its policies 16 times, and YouTube changed its policies 12 times.[231] Most of these changes involved adding, subsequently rolling back, and then reinstating new rules concerning key issues like mail-in voting fraud or false victory claims.[232]

During the 2020 election cycle (October 2019 through January 2021), Facebook changed its election-related misinformation policies 21 times, Twitter changed its policies 16 times, and YouTube changed its policies 12 times.

While Mozilla was able to track the policies of Facebook, Twitter, and YouTube during the 2020 election, it concluded that "there remains a persistent lack of data about how well these policies were enforced and their impact on election misinformation."[233] This reflects a gap in understanding between the public and the platforms about which policies were most effective and which were not.[234] It is also concerning because of how prevalent these platforms have become in our nation's politics and the way the Big Lie about how the 2020 election was "rigged and stolen" from Trump has metastasized via social media platforms throughout our national civic dialogue.

During the 2020 election specifically, mainstream social media platforms like Facebook, Twitter, and YouTube expanded their policies and enforcement against election-related disinformation, removing or labeling many dangerous false claims of widespread voter fraud.[235] These changes generally correlated with major events like the beginning of the impeachment inquiry into then-president Donald Trump, the death of George Floyd, Trump's first public claim that mail-in ballots would lead to election fraud, and his first public refusal to commit to accepting election results, Election Day, and when the Electoral College confirmed President Biden's victory.[236]

Next, we summarize only the policies that Facebook, Twitter, and YouTube implemented during the 2020 elections and soon after. We also discuss how inconsistent enforcement and policy loopholes led to the spread of disinformation during and after the election, how the actions taken (or not taken) by the platforms contributed to the insurrection at the Capitol complex on January 6, and how the platforms reacted in the aftermath.

Unfortunately, Facebook and Twitter have stopped enforcing existing policies to the degree they did during the 2020 election.[237] Our research shows that there are many pieces of content being left on the platform that would have been taken down months ago.[238]

Facebook

It has been well documented that Facebook is inconsistent in its enforcement of existing policies. In September of 2020, the *Wall Street Journal* flagged over 200 pieces of content for Facebook that appeared to violate the platform's rules against the promotion of violence and dangerous information, only to have Facebook respond by taking down around 30 pieces of flagged content and later conceding that more than half of the pieces of content should have been taken down for violating their policies.[239]

In addition to inconsistent enforcement, Facebook also had two major loopholes that contribute significantly to the spread of disinformation on the platform: the newsworthiness exemption and its policy of not fact-checking political ads.

In addition to inconsistent enforcement, Facebook also had two major loopholes that contribute significantly to the spread of disinformation on the platform: the newsworthiness exemption and its policy of not fact-checking political ads.

The newsworthiness exemption applies to any content that Facebook believes "should be seen and heard"[240] and meets a balancing test that weighs the public benefit of having the content up versus the harm keeping the content in question up could cause.[241] This is extremely subjective, and this subjectivity is reflected in Facebook's use of the newsworthiness exemption over time. Through 2020 and the first half of 2021, content from certain users, including politicians, was presumed to be newsworthy and left up.[242] However, following criticism from its oversight board, Facebook eliminated the presumption that posts by politicians are automatically considered newsworthy.[243] While this is a step forward, Facebook is still able to apply its newsworthiness exemption to any piece of content it chooses without giving much justification as to why the content is left up. This gives politicians and other bad actors with large public followings the ability to spread disinformation that Facebook may consider "newsworthy" with confidence that it is unlikely to be taken down.

Facebook's decision to exempt political ads has proven to be equally controversial, if not more, than their newsworthiness exemption. This loophole is straightforward: Facebook will not fact-check political advertisements on the platform.[244] During the 2020 election, then-candidate Donald Trump took advantage of this loophole several times and placed ads on Facebook intending to mislead voters about then-candidate Joe Biden and his son Hunter.[245] If Facebook is to get serious about cracking down on disinformation, this loophole is one of the first they need to address.

This laissez-faire approach to content moderation allowed bad actors to spread content that contributed to the January 6 insurrection.[246] Right-wing groups were able to use Facebook's Groups feature to plan their assault on the Capitol building, while prominent pages pushed harmful content delegitimizing the election and took advantage of relaxed enforcement of live videos to urge violence.[247]

This laissez-faire approach to content moderation allowed bad actors to spread content that contributed to the January 6 insurrection.

Following the insurrection on January 6 and significant criticism by both members of Congress and civil society, Facebook made a few different changes. This included suspending President Trump's account indefinitely (which was later reduced to two years after the indefinite suspension was appealed to Facebook's oversight board), increasing its monitoring for calls to violence and protest, and updating its election label to read, "Joe Biden has been elected President with results that were certified by all 50 states. The US has laws, procedures, and established institutions to ensure the peaceful transfer of power after an election."[248] *Additionally, the company put in place heightened penalties for public figures "during times of civil unrest and ongoing violence."*[249] However, it is important to note that while Facebook gives an example of actionable content (someone sharing a link to a statement from a terrorist group in the aftermath of an attack), they do not define what constitutes a period of "civil unrest and ongoing violence."[250]

Significant questions exist as to how seriously Facebook takes the threat of disinformation. Even the changes Facebook made following January 6 are riddled with loopholes. As Common Cause has documented, former president Trump is still able to run political ads on Facebook and solicit donations from supporters, even though he is suspended from the platform.[251] And as with most Facebook policies, the new rules put in place are arbitrary and subject to human discretion.

Twitter

Although Facebook tends to dominate the conversation about content moderation practices and the spread of disinformation on social media, Twitter is guilty of many of the same things: inconsistent enforcement of existing policies, loopholes in policies that allow for the spread of disinformation, and relatively weak policy responses to the January 6 insurrection. While Twitter may want to be viewed as better on content moderation than its peers, it has been equally as slow to deal with the misinformation that is found all over the platform.

Media Matters highlighted Twitter's inconsistent enforcement in a post discussing the platform's treatment of a doctored video of House Speaker Nancy Pelosi (D-CA) appearing to slur her words.[252]

While one version of the video on the platform has received a "manipulated media" tag, other versions of the video remained on the platform untouched.[253]

Just like Facebook's newsworthiness exemption, Twitter has a major loophole that contributes significantly to the spread of disinformation called the "public interest exception." This exception applies to tweets from elected and government officials that Twitter believes "directly contribute" to the understanding or discussion of a matter of public concern.[254] Tweets that are found to be in the public interest but break other rules may have a label put on them but will not be taken down.[255] Even though the platform insists that this does not mean public officials can post whatever they want (even tweets in violation of their rules), in reality, public officials are generally allowed to get away with posting whatever they want.[256] The consequences of this loophole were on full display when then-outgoing president Donald Trump live tweeted throughout the insurrection, adding gas to the fire by inciting his supporters while they stormed the Capitol.[257]

Twitter permanently suspended Donald Trump's account and CEO Jack Dorsey acknowledged the platform's role in the insurrection, but issues remain.[258] Today, public officials like Rep. Marjorie Taylor Greene (R-GA) are able to take advantage of this exemption, and if Twitter is serious about getting rid of disinformation on the platform, they also need to look into closing this loophole.[259]

YouTube

Compared to Facebook and Twitter, YouTube's policies have not been scrutinized to the same degree, but like the other social media platforms mentioned here, YouTube is also inconsistent in its enforcement of existing policies.[260] **However, instead of having one or two major loopholes in which disinformation is able to spread, YouTube's policies are overall far more permissive than that of Facebook and Twitter.**[261]

YouTube's inconsistency in policy enforcement is well documented. In 2019, the platform announced that it would be making changes to its hate speech policy and taking down thousands of videos that were in violation of the new policy, but Gizmodo found that many of the videos remained up.[262] To make matters worse, YouTube's own algorithm will frequently recommend content that violates its own policies.[263] One example of this is a user watching a music video from Art Garfunkel, one half of the popular 1960s pop duo Simon & Garfunkel, recommending a video titled *Trump Debate Moderator EXPOSED as having Deep Democrat Ties, Media Bias Reaches BREAKING Point.*[264] A study done by Mozilla found that nearly 200 videos YouTube's algorithm recommended to volunteers had a collective 160 million views before the platform took them down for violating YouTube's policies.[265]

Like its peers, YouTube took some actions following the January 6 insurrection. First, YouTube suspended Donald Trump's account until the risk of violence associated with the account had decreased.[266] Second, they introduced new rules, giving "strikes" to channels whose videos violate the platform's policies and permanently removing channels that receive three strikes within the same 90-day period.[267] Since YouTube has not explained what they mean by "risk of violence," it is unclear when and if they will let Donald Trump back on the platform or how they will apply this standard to other accounts in the future.

SECTION 4: RECOMMENDATIONS

Federal laws and the laws of many states contain important provisions to reduce the harmful impact of election disinformation. Social media company civic integrity policies are likewise critically important. These current laws and policies leave much room for improvement. There is no single policy solution to the problem of election disinformation. We need strong voting rights laws, strong campaign finance laws, strong communications and privacy laws, strong media literacy laws, and strong corporate civic integrity policies. In this section, we recommend reforms in all these policy areas, highlighting both pending legislation that should be passed and existing state laws that should be replicated in other jurisdictions.

There is no single policy solution to the problem of election disinformation. We need strong voting rights laws, strong campaign finance laws, strong communications and privacy laws, strong media literacy laws, and strong corporate civic integrity policies.

Statutory Reforms

Voter Intimidation and False Election Speech Reforms

The Voting Rights Act of 1965 and other federal laws prohibit voter intimidation and have been interpreted by the DOJ and courts as prohibiting certain forms of election disinformation.[268] **However, existing federal statutes and the statutes in most states do not explicitly prohibit election disinformation and should be amended to do so.** And as the *New York Times* wrote earlier this year in response to the DOJ prosecution of Douglass Mackey for disseminating election disinformation via Twitter, the "case will test the novel use of federal civil rights laws as a tool to hold people accountable for misinformation campaigns intended to interfere with elections[.]"[269] Rather than relying on courts to appropriately apply long-standing statutes to new modes of election disinformation, Congress and state legislatures should update statutes to explicitly prohibit election disinformation.

Congress should enact the Deceptive Practices and Voter Intimidation Prevention Act of 2021,[270] which would modernize federal law to address the worst election disinformation practices being used today. This bill has been incorporated into both the Freedom to Vote Act[271] and the For the People Act.[272] It twice-passed the House in 2019 as part of the For the People Act and the Stopping Harmful Interference in Elections for a Lasting Democracy (SHIELD) Act but died in the Senate. Among other things, this legislation would amend the anti-intimidation statute at 52 U.S.C. § 10101(b) to add a new subsection **explicitly outlawing false statements regarding federal elections**. Under this amendment, it would be illegal to knowingly disseminate materially false information within 60 days before a federal election regarding the time, place, or manner of holding any federal election or the qualifications or restrictions on voter eligibility—with the intent to impede or prevent another person from exercising the right to vote in an election.[273] Importantly, the bill not only contains criminal enforcement provisions but also would create a private right of action, enabling those harmed by disinformation to file a civil lawsuit against the

perpetrator.[274] Finally, the legislation would require the attorney general to communicate with the public to correct any materially false election information if state and local election officials have failed to do so.[275]

States should likewise enact legislation explicitly prohibiting dissemination of false election speech, modeled on the federal Deceptive Practices and Voter Intimidation Prevention Act of 2021[276] or similar legislation already enacted in Virginia prohibiting knowingly communicating false information "intended to impede the voter in the exercise of his right to vote," including information "about the date, time, and place of the election, or the voter's precinct, polling place, or voter registration status, or the location of a voter satellite office or the office of the general registrar."[277]

Congress should also adopt a proposed amendment to the National Defense Authorization Act, a military appropriations and policy bill, which would require national intelligence agencies to include in their regularly scheduled post-election report the identification of any Russian government official or agent who used "social or traditional media to spread significant amounts of false information to individuals in the United States" as a form of election interference.[278] And Congress should go beyond this Russia-specific amendment to require identification of any foreign government spreading disinformation to interfere in U.S. elections.

Campaign Finance Reforms

Strong, up-to-date campaign finance disclosure laws are key to curbing the harmful impacts of election disinformation. Whereas social media and other internet platforms have become favored means of disseminating election disinformation, federal campaign finance disclosure laws and the laws of most states were written decades ago, before these avenues for disinformation existed. **Congress and state legislatures should update disclosure laws so that the public has easy access to accurate information regarding who is spending money on political advertising online and through more traditional modes of communication.**

Congress should pass the DISCLOSE Act of 2021[279] and the Honest Ads Act,[280] both of which have been incorporated into the Freedom to Vote Act[281] and the For the People Act.[282] The For the People Act passed the House in March 2021. The Freedom to Vote Act is Senate legislation that includes most of the core pillars of the For the People Act, including the DISCLOSE Act and the Honest Ads Act. The DISCLOSE Act would **shine a light on presently dark money in federal elections** by expanding the definition of what constitutes a reportable "campaign-related disbursement" to include certain ads that support or oppose candidates and transfers between organizations—a tactic used to evade disclosure under current law.[283] The DISCLOSE Act would also strengthen "paid for by" disclaimers for robocalls, a popular mode of communication for election disinformation.[284] The Honest Ads Act would require political ads sold online to be covered by the same rules as political ads sold on TV, radio, and satellite.[285] It would also expand disclosure rules to include any online ads that mention a candidate and require social media platforms and websites with 50 million or more unique monthly visitors that sell political advertising to maintain a database of all online political ads—both necessary reforms to improving transparency around online ads.[286]

Congress should also act on the FEC's recommendation to amend and strengthen the "fraudulent misrepresentation of campaign authority" statute by expanding the law to prohibit any

person—not just candidates and their agents—from fraudulently claiming to be acting on behalf of a candidate or political committee.[287]

And **Congress should restructure and strengthen the FEC to ensure more effective implementation and enforcement of all federal campaign finance laws,** as would result from the passage of the Restoring Integrity to America's Elections Act,[288] which was last introduced in 2019 but has been incorporated into both the For the People Act[289] and the Freedom to Vote Act.[290]

Similarly, states should follow the leads of Alaska, California, New York, Washington, and the handful of other states profiled earlier in this report that have enacted campaign finance disclosure laws to bring previously dark money spending on digital and other election advertising into the light. Alaska's[291] and California's[292] laws that enable voters to trace election spending to the source are similar to the reforms contained in the federal DISCLOSE Act, all providing models to emulate throughout the states. California,[293] New York,[294] and Washington[295] have enacted cutting-edge requirements for digital political ad "paid for by" disclaimers and public access to digital ad databases that can serve as models for the nation.

State Media Literacy Laws

Common Cause does not recommend any specific media literacy laws, but **we do encourage policymakers to experiment with best practices around media literacy** and advocacy groups interested in pushing for media literacy laws to work with stakeholders to determine the approach that best fits their state. This involves holding convenings and bringing to the table organizations like PEN America, which are already engaged in the issue and offering media literacy training to the public, to put together a set of principles and best practices on which to develop legislation.[296] Media Literacy Now has put together a model bill that established an advisory council within the respective state's Department of Education,[297] which is one example of an approach that could be taken.

State Privacy Laws

While California, Colorado, Virginia, and Washington have all successfully passed comprehensive privacy legislation, each bill was lacking in some respects. None of them have specific civil rights protections, and only California has a (very limited) private right of action. **Advocates interested in passing comprehensive privacy legislation should look to the Digital Fairness Act, which was introduced in the New York State Assembly this year, as a model.**[298] The Digital Fairness Act includes heightened protections for biometric information, strong civil rights protections by explicitly making it unlawful to process personal information or target advertising in ways that discriminate in employment, finance, health care, credit, insurance, housing, education opportunities, or public accommodations based on an individual's or class of individuals' actual or perceived age, race, creed, color, national origin, sexual orientation, gender identity or expression, sex, disability, predisposing genetic characteristics, or domestic violence victim status, as well as and a robust private right of action for consumers whose rights are violated.[299] **Any legislation considered needs to have strong civil rights protections, a strong private right of action, and strong data minimization provisions.** Further, if a state Attorney General's Office is going to play a meaningful role in enforcement, it must receive enough funding to be able to effectively bring lawsuits and protect consumers in their state.

Federal Legislative Reforms to Mitigate Platform Business Practices

Algorithmic Accountability

Social media algorithms have contributed to the spread of disinformation given that platforms have optimized them for user engagement, which has led users down a rabbit hole of hate speech, conspiracy theories, and harmful content.[300] Algorithms can also promote the amplification of disinformation as conspiracy theorists used the "stop the steal" moniker across platforms to organize and mobilize offline violence.[301] To hold platforms accountable for the algorithms they deploy, **we urge Congress to pass the Algorithmic Justice and Online Platform Transparency Act.**[302] The legislation would **prohibit discriminatory algorithms and create greater transparency about how these algorithms operate.** The bill also addresses election disinformation specifically by prohibiting online platforms from processing personal information "in a manner that intentionally deprives, defrauds, or attempts to deprive or defraud any individual of their free and fair exercise of the right to vote in a Federal, state, or local election."[303]

Comprehensive Privacy Legislation

Comprehensive federal privacy legislation is key to placing limits on the collection and sharing of personal data, which has contributed to the spread of disinformation. As discussed, social media platforms collect vast amounts of data on their users, and bad actors exploit these data practices by targeting harmful content. For example, the Trump campaign used Facebook to target millions of Black voters with deceptive information to deter them from voting.[304]

At a minimum, federal legislation should (1) require companies to minimize the data they collect; (2) prohibit predatory and discriminatory data practices on the basis of protected characteristics with respect to access to credit, housing, education, employment, and public accommodations; (3) provide for fairness in automated decision-making; (4) grant a private right of action to allow consumers to sue companies that violate their privacy rights; and (5) define permissible and impermissible uses for collecting, sharing, and using personal data.[305]

Strengthening Local Media

Local media plays a critical role in supporting civic engagement and provides communities with vital information on issues such as public safety, economic development, and health care. Unfortunately, the decade-long decline in local media has robbed communities of critical news and information, creating an "infodemic" that has helped disinformation flourish.[306] The economic decline in local news can be attributed in part to large social media platforms that are now dominating the advertising market, making the ad-driven business model for journalism unsustainable.[307]

Congress can pass **legislation that funds local media and community and public media of all kinds.** Funds should be targeted at preserving newsrooms and reporting jobs at local commercial and nonprofit news outlets, as well as investments to address the civic information needs of communities most affected by the long-term decline of local news. In addition to short-term spending, we need long-term solutions about how journalism can meet the civic information needs of communities in the 21st century. To that end, Congress should pass the Future of Local News Act, which would **create a committee to study the state of local journalism and offer recommendations to Congress.**[308] The bill would provide a first step in determining what transformative investments are needed to create a sustainable local journalism landscape.

Empowering Researchers and Watchdog Journalists

Transparency is more important now than ever, as political campaigns and disinformation agents use manipulative tactics to target voters on social media platforms. Ensuring researchers can study the major platforms without fear of interference is crucial to understanding how misinformation spreads and for developing policies that address the many harms to society the platforms have caused.

Congress should **pass legislation that ensures researchers and watchdog journalists have sufficient access to social media data and protect them from retaliation by the platforms.** New York University researcher Laura Edelson, whose account was banned by Facebook while she was researching ad transparency and the spread of misinformation, recommended in her recent congressional testimony that there be universal digital ad transparency, a researcher safe harbor law, and greater access to public content with "meaningful reach or content from public figures with meaningful audiences."[309] Members of Congress have also put forward their own legislative solutions. Representative Lori Trahan (D-MA) has introduced legislation that would require covered platforms to grant academic researchers and the FTC access to an ad library with select information about each ad.[310]

Executive and Regulatory Agency Reforms

In addition to legislative reforms to fight election disinformation, there are regulatory tools and other actions federal and state executive branch agencies can take to combat disinformation, including stronger enforcement of existing laws and promulgation of new regulations to rein in social media business practices that bad actors exploit to spread and amplify harmful content that interferes with our democracy. As a general matter, statutory reform is preferable to executive and regulatory agency reform because some types of executive and regulatory agency reform can easily be reversed when a new president's or governor's administration comes into power. Nevertheless, executive branch reforms may be easier to attain than the passage of legislation and can play an important role in reducing election disinformation.

Presidential and Gubernatorial Leadership

The White House under the Biden administration must play a leading role in combating election disinformation. A recently published report from the U.S. surgeon general shows that the Biden administration has already recognized that the spread of COVID-19 misinformation poses serious risks to the nation's public health.[311] The surgeon general's report identified several recommendations the government, social media platforms, and other stakeholders can take to stop the spread of false content related to the pandemic.[312] Similarly, the Biden administration should take a whole-of-government approach to combating election disinformation. To start, the administration can issue an executive order directing federal agencies with enforcement, rule-making, and investigatory authorities to use these capabilities in combating election disinformation.

Next, the administration should create a federal interagency task force that would identify tools to combat election disinformation and harmful online speech.[313] The task force, composed of senior officials from executive agencies such as the DOJ and Department of Commerce and independent agencies such as the FTC, among others, would develop initiatives to mitigate the impact of disinformation, particularly on African American communities and other communities

of color that are disproportionately targeted by disinformation campaigns.[314] Given the scope and complexity of how disinformation spreads, a whole-of-government approach is necessary, and the White House must lead on this initiative.

Similarly, governors in states around the nation can and should play a leading role in stopping election disinformation, establishing task forces like the one described earlier, and using all available resources of state agencies under their control.

U.S. DOJ and State Law Enforcement Agencies

Existing statutes give federal and state law enforcement officials many tools to fight election disinformation. The federal DOJ, for example, has long interpreted voting rights laws as prohibiting election disinformation that interferes with the fundamental right to vote.[315] However, the DOJ prosecution begun earlier this year against Twitter user Douglass Mackey[316] for illegally disseminating election disinformation in 2016 appears to be the first criminal prosecution in the United States involving voter suppression through the spread of disinformation on Twitter.[317] **The DOJ should be more aggressive in its criminal prosecution and civil litigation against those who use disinformation to intimidate voters and interfere with their voting rights.**

State law enforcement officials should likewise use state laws prohibiting voter intimidation, election interference, and false statements regarding elections—including those that do not explicitly name election disinformation as a form of illegal interference—to stem the tide of election disinformation and hold perpetrators accountable.

FTC Reforms

There are several different actions the FTC could take to improve its role as the country's privacy enforcement agency. Under the current administration, the FTC could expand the scope of its rule-making and enforcement practices. Senate Democrats[318] and civil society groups[319] have both asked the FTC to **initiate rule-making to regulate unfair and deceptive commercial data practices**. This rule-making would consider strong protections for members of marginalized communities, data minimization practices, prohibitions on certain practices, opt-in consent rules on the use of personal data, and global opt-out standards.[320] In addition to rule-makings, the FTC can conduct workshops and issue informal guidance on how platforms can provide greater transparency in their content moderation practices.

State law enforcement officials should likewise use state laws prohibiting voter intimidation, election interference, and false statements regarding elections.

FEC and State Election Agency Reforms

The FEC has an important role to play in combating disinformation in federal elections. The FEC is our nation's frontline enforcer of campaign finance disclosure laws in federal elections. Yet, despite the proliferation of online political advertising over the past decade-plus, the FEC has failed to update its "paid for by" disclaimer rules for digital ads. In October 2011, the Commission

published an advance notice of proposed rule-making on "internet communication disclaimers"[321] and has, over the decade, invited public comment on the issue several times. Common Cause filed comments in 2018 on behalf of more than 25,000 members and supporters urging the Commission to adopt regulations applying to digital ads the full disclaimer requirements now applicable to radio, television, and print ads.[322] But today, more than a decade after the rule-making began, the Commission still has not adopted final regulations. With bad actors continuing to target Black and other communities of color with election disinformation using digital political ads, **it is long past time for the FEC to promulgate clear and enforceable disclaimer rules for online political advertising.**

State campaign finance agencies similarly have an important role to play in implementing and enforcing effective disclosure laws to shine a light on those trying to undermine our elections with disinformation. All states' campaign finance enforcement agencies should follow the leads of the Washington Public Disclosure Commission, the California Fair Political Practices Commission, and others that have worked hard to effectively apply campaign finance laws to the digital landscape.

Social Media Corporation Policy Reforms

While self-regulation on its own has proven ineffective in curbing the spread of disinformation, **social media platforms must take additional steps to strengthen their policies on combating content designed to undermine our democracy.** The recommendations that follow focus on how platforms can improve their efforts to provide users with authoritative information concerning voting and elections, reduce the spread and amplification of election disinformation, and provide greater transparency regarding their content moderation policies and practices. While not an exhaustive list, these recommendations represent the basic steps all social media platforms should take.

Provide Users With Authoritative Information About Voting and Elections

Platforms should help users identify official voting information such as registering or updating their registration, tracking ballots in the mail, and identifying in-person polling sites. *Platforms should direct their users to authoritative sources of information regarding voting and elections. Authoritative sources come from state and local election officials.*

Consistent Enforcement of Civic Integrity Policies During Both Election and Nonelection Cycles

Platforms have failed to consistently enforce the civic integrity policies they have in place to combat the spread of election disinformation.[323] Further, enforcement tends to become more relaxed during nonelection cycles. **Platforms must commit to upholding their own civic integrity policies** and consistently enforce them throughout election, as well as nonelection, cycles. Consistent enforcement includes rapid removal, labeling, and de-prioritizing of content that violates civic integrity policies.

Platforms should also **close loopholes in their civic integrity policies** bad actors exploit to spread disinformation. For example, platforms should apply third-party fact-checkers to political adver-

tisements and remove exemptions for public figures that allow them to spread disinformation with impunity.

Reducing the Spread and Amplification of Disinformation

Platforms must **reduce the spread and amplification of disinformation caused by the algorithms they deploy**. As discussed, platforms optimize their algorithms to maximize user engagement. Content that generates the most engagement and gets amplified tends to focus on lies, conspiracy theories, and incitements of violence. Platforms can take steps to limit amplification by fashioning artificial intelligence systems and algorithms so that engagement does not prioritize disinformation. Further, platforms should conduct third-party human and civil rights audits of their algorithms to ensure voter suppression content is not getting amplified.

Provide Researchers and Watchdog Journalists Greater Access to Social Media Data

Platforms must **provide researchers and watchdog journalists with sufficient and reliable access to social media data.** As discussed, researchers and watchdog journalists play a critical role in shedding light on how platforms enforce and interpret their content moderation policies in practice. For example, researchers exposed numerous instances where Facebook failed to properly disclose election advertisements[324] despite their policies and the ability of campaigns to use manipulative targeting practices to reach voters on the platform.[325] Further, watchdog journalists have uncovered how Facebook deliberately designed its algorithms to optimize for engagement,[326] incentivizing the spread of disinformation and selectively choosing to apply its content moderation policies.[327] Unfortunately, platforms have resisted providing researchers and watchdog journalists greater access to data, likely because of the risk of embarrassment from failure to adhere to their own policies and public statements.[328] Giving researchers and watchdog journalists greater access to data will not only provide a better picture of how disinformation gets spread, targeted, and amplified but also ensure the integrity of our elections.

Invest Greater Resources in Combating Disinformation Targeting Non-English-Speaking Communities

Platforms must invest greater resources in combating election disinformation in non-English-speaking communities. Research has shown that non-English-language disinformation has continued to spread.[329] Further, disparities exist in the level of enforcement between English and non-English disinformation, leaving non-English-speaking communities more vulnerable to disinformation. **Platforms can remedy these disparities in enforcement by investing greater resources to combating non-English disinformation**, including hiring more content moderators to monitor and combat disinformation in languages other than English.

CONCLUSION

For decades, Common Cause Education Fund has worked on public education and systemic reforms to build a better democracy. The harmful impact of election disinformation makes it clear that our core programmatic work is needed now more than ever. We must and will educate and mobilize our communities to curb the harmful, rapid growth of election disinformation. Doing so will help deliver on America's promise of a functioning 21st-century democracy that's open, accessible, responsive, and accountable to the people. We need your support and your activism to fix the problem of election disinformation. Together, we can build a democracy that works for everyone.

APPENDIX I—STATE VOTER INTIMIDATION AND FALSE ELECTION SPEECH LAWS

Under **Arizona** law, it is a criminal misdemeanor to knowingly "make use of force, violence or restraint, or to inflict or threaten infliction...of any injury, damage, harm or loss, or in any manner to practice intimidation upon or against any person, in order to induce or compel such person to vote or refrain from voting for a particular person or measure" or to "impede, prevent or otherwise interfere with the free exercise of the elective franchise of any voter."[330] Other Arizona laws apply specifically to employer intimidation of their employees[331] and voter interference within a 75-foot buffer zone outside of polling places.[332]

California (among other states[333]) invites candidates and committees to sign a voluntary "Code of Fair Campaign Practices" that includes a promise not to "use or permit any dishonest or unethical practice that tends to corrupt or undermine our American system of free elections, or that hampers or prevents the full and free expression of the will of the voters including acts intended to hinder or prevent any eligible person from registering to vote, enrolling to vote, or voting."[334]

In **Colorado**, it is illegal to "impede, prevent, or otherwise interfere with the free exercise of the elective franchise of any elector."[335] Colorado law also explicitly provides that **no person shall knowingly or recklessly "make, publish, broadcast, or circulate or cause to be made, published, broadcasted, or circulated...any false statement designed to affect the vote** on any issue submitted to the electors at any election or relating to any candidate for election to public office."[336] Colorado attorney general guidance makes clear that disinformation tactics—including "misleading phone calls, texts, or emails to a voter"—can constitute illegal voter intimidation. Examples of illegal voter intimidation include "texting voters deliberately false information about voting locations" and "calling voters to tell them that they must have an identification card or be vaccinated in order to vote."[337]

Under **Florida's** "Voter Protection Act," it's a felony to "directly or indirectly use or threaten to use force, violence, or intimidation or any tactic of coercion or intimidation to induce or compel an individual" to register or vote or refrain from doing so.[338] Importantly, it's a **felony under Florida law to "knowingly use false information"** to "challenge an individual's right to vote" or "induce or attempt to induce an individual to refrain from voting or registering to vote."[339]

Georgia law makes it a felony to use or threaten "violence in a manner that would prevent a reasonable elector from voting or actually prevents any elector from voting."[340] It is likewise a felony in Georgia to use or threaten "violence, or act[] in any other manner to intimidate" another person to vote or refrain from voting or registering to vote.[341]

Hawaii law provides that any person who "knowingly broadcasts, televises, circulates, publishes, distributes, or otherwise communicates, including by electronic means or advertisement, false information about the time, date, place, or means of voting with the purpose of impeding, preventing, or otherwise interfering with the free exercise of the elective franchise" has committed illegal election fraud.[342] It is also a crime in Hawaii to "in any way practice[] intimidation upon or against any person in order to induce or compel the person to vote or refrain from voting" or to

impede, prevent, or otherwise interfere with voting.[343] And earlier this year, Hawaii extended its "no campaigning" zone to protect from harassment voters waiting in lines extending far outside voting centers.[344]

Maine law makes it a crime to "interfere[] with a voter attempting to cast a vote"[345] or to "knowingly cause[] a delay in the registration…of another or…in the delivery of an absentee ballot or absentee ballot application with the intent to prevent a person from voting or to render that person's vote ineffective."[346]

Maryland law makes it a crime to knowingly and willfully "influence or attempt to influence a voter's voting decision through the use of force, threat, menace, [or] intimidation" or to "influence or attempt to influence a voter's decision whether to go to the polls to cast a vote" through use of force, fraud, or threat.[347] It is also a crime to "engage in conduct that results or has the intent to result in the denial or abridgement of the right of any citizen of the United States to vote on account of race, color, or disability."[348]

Michigan law makes it a felony to "attempt, by means of bribery, menace, or **other corrupt means** or device, either directly or indirectly, to influence an elector in giving his or her vote, or to deter the elector from, or interrupt the elector in giving his or her vote at any election held in this state."[349] It is also **illegal in Michigan to knowingly disseminate an "assertion, representation, or statement of fact concerning a candidate…that is false, deceptive, scurrilous, or malicious**, without the true name of the author being subscribed" to the statement.[350]

Minnesota law prohibits directly or indirectly using or threatening "force, coercion, violence, restraint, damage, harm, loss, including loss of employment or economic reprisal, undue influence, or temporal or spiritual injury against an individual to compel the individual to vote for or against a candidate or ballot question."[351] Further, "fraud may not be used to obstruct or prevent the free exercise of the right to vote."[352]

Under **Nevada** law, it is illegal to impede or prevent by "fraudulent contrivance, the free exercise of the franchise by any voter."[353] It is likewise a felony to use or threaten to use any force, intimidation, coercion or undue influence, or to "inflict any mental injury, damage, harm or loss upon" a person on connection with registering or voting in an election.[354]

New Mexico law makes it a felony to use or threaten "force, violence, infliction of damage, harm or loss or any form of economic retaliation, upon any voter…for the purpose of impeding or preventing the free exercise of the elective franchise."[355] Guidance from New Mexico's secretary of state explains that "disseminating false or misleading election information" is a form of voter intimidation, stating, "It is unlawful to disseminate misleading information about elections, including flyers or other communication that purposely misstate the time and date of an election, where it will be held, and how voting will happen."[356]

North Carolina law makes it illegal for any person to "intimidate or oppose any legally qualified voter on account of any vote such voter may cast or consider or intend to cast, or not to cast, or which that voter may have failed to cast."[357]

Pennsylvania law prohibits using "coercion, threats of bodily injury or intimidation" to intentionally prevent or attempt to prevent someone from registering to vote.[358] The Pennsylvania Department of State elaborates on guidance that it is likewise illegal to use such intimidation to compel or prevent someone from voting and that "[d]isseminating false or misleading election information, including information on voting eligibility, polling place procedures, polling place hours, or voting methods" is a form of illegal voter intimidation.[359]

Virginia law makes it a crime to "hinder, intimidate, or interfere with any qualified voter so as to prevent the voter from casting a secret ballot"[360] or to interfere or attempt to interfere with a person registering to vote.[361] Virginia explicitly outlaws communicating to a "registered voter, by any means, false information, knowing the same to be false, intended to impede the voter in the exercise of his right to vote," including information "about the date, time, and place of the election, or the voter's precinct, polling place, or voter registration status, or the location of a voter satellite office or the office of the general registrar."[362] Virginia law includes a private right of action for registered voters to whom such false information is communicated, enabling them to seek an "injunction, restraining order, or other order, against the person communicating such false information."[363]

Wisconsin law prohibits the use or threat of force, violence, duress, or any fraudulent device or contrivance to "impede or prevent the free exercise of the franchise at an election."[364] Wisconsin law also provides that no person "may knowingly make or publish, or cause to be made or published, a false representation pertaining to a candidate or referendum which is intended or tends to affect voting at an election."[365]

APPENDIX II—STATE CAMPAIGN FINANCE DISCLOSURE LAWS

Alaska has enacted one of the nation's most effective laws for tracing the source of funds spent on election advertising by groups, including those that do not qualify as political committees,[366] requiring such groups to disclose the identity of any contributor who has given the group more than $250 in the aggregate during the calendar year "for the purpose of influencing the outcome of an election," as well as all election-related contributions and expenditures made by such groups, including contributions to other such groups.[367] The purpose of this statute is to reveal contributors whose funds are transferred through multiple organizations before being spent on election advertising—contributors who would evade disclosure under most jurisdictions' laws.

California has led the way in recent years in strengthening campaign finance disclosure laws applicable to common sources and types of election disinformation. In 2014, the state strengthened disclosure laws applicable to nonpolitical committee groups spending money to influence California elections (e.g., 501(c)(4) social welfare organizations, 501(c)(5) labor organizations, 501(c)(6) trade associations).[368] Under the 2014 reform, so-called multipurpose organizations that spend more than $50,000 during a 12-month period or more than $100,000 in a period of four consecutive years to influence California elections must register with the state and disclose the donors whose funds were used for the California political spending. And in 2018, California took another step by enacting a "Social Media DISCLOSURE Act,"[369] strengthening disclosure requirements by requiring "paid for by" disclaimers on a broad array of political advertising disseminated via social media platforms.

Maryland has enacted legislation requiring certain tax-exempt organizations that are the source of undisclosed "dark money" political spending in many jurisdictions—501(c)(4), 501(c)(6), and 527 organizations—that make aggregate election-related disbursements of $10,000 or more in an election cycle, to file a report disclosing the identity of each person that made cumulative donations of $10,000 or more to the organization during the period covered by the report.[370]

Minnesota law requires likewise targets' would-be "dark money" with specific donor disclosure requirements for "associations" that contribute more than $5,000 in a calendar year to independent expenditure or ballot measure committees. Such associations must disclose the "name, address, and amount attributable to each person that paid the association dues or fees, or made donations to the association that, in total, aggregate more than $5,000 of the contribution from the association to the independent expenditure or ballot question political committee or fund."[371]

New York has enacted legislation imposing disclosure requirements on paid internet and digital political ads and requiring the state board of elections to maintain a publicly available database of such ads.[372] New York explicitly permits modified "paid for by" disclaimers for digital political advertising, so long as the ad "contains a link to another webpage where the "paid for by" statement is prominently displayed."[373]

Rhode Island law stems the flow of "dark money" with a disclosure requirement not only for independent political expenditures but also for certain transfers of funds between organizations

(defined in the statute as a "covered transfer") exceeding $1,000 in a calendar year for such political spending.[374]

Finally, the state of Washington has some of the strongest disclosure laws in the nation applicable to election disinformation and other digital political advertising. Washington's overall campaign finance disclosure regime is appropriately broad in its application and mandates on-ad identification of top donors to the sponsor for certain political advertising.[375] Washington Public Disclosure Commission regulations provide for modified "paid for by" disclaimers on certain digital ads[376] and require online platforms that sell paid political advertising (digital "commercial advertisers") to provide the public with access to detailed digital ad information.[377]

APPENDIX III—STATE MEDIA LITERACY LAWS

California's media literacy law, passed in 2018 with bipartisan support in the assembly, requires the Department of Education to list instructional materials and resources on how to evaluate trustworthy media sources.[378]

In 2019, the **Colorado** General Assembly passed legislation creating a media literacy advisory committee within the Colorado Department of Education. The committee submitted a report to the Colorado General Assembly in December of the same year and recommended revising Colorado academic standards, providing materials and resources to teachers, and enacting further legislation directing Colorado to take action to support effective implementation of media literacy programs in schools throughout the state.[379]

Florida's law, which was passed in 2008 and strengthened in 2013, requires media literacy to be integrated into the standards for all subjects in K–12 public schools.[380]

Illinois passed a media literacy law in 2021 requiring every public high school in the state to include in its curriculum a unit of instruction on media literacy, **making it the first state to mandate media literacy classes.**[381]

A **Minnesota** state law passed in 2006 requires the state's education commissioner to embed technology and information literacy standards into the state's academic standards and graduation requirements.[382]

New Mexico has had a law in place since 2009 allowing for media literacy to be offered as an elective in schools.[383]

ENDNOTES

1 Aberjhani and Luther E. Vann, *Elemental: The Power of Illuminated Love* (Columbia, SC: Soar Publishing, 2008).

2 Chris Cillizza, "The Big Lie Is (Unfortunately) Winning," *Washington Post*, September 15, 2021, https://www.cnn.com/2021/09/15/politics/big-lie-republican-belief-trump/index.html.

3 Cillizza, "The Big Lie Is (Unfortunately) Winning," *Washington Post*, September 15, 2021, https://www.cnn.com/2021/09/15/politics/big-lie-republican-belief-trump/index.html.

4 "The national, nonpartisan Election Protection coalition works year-round to ensure that all voters have an equal opportunity to vote and have that vote count. Made up of more than 100 local, state and national partners, Election Protection uses a wide range of tools and activities to protect, advance and defend the right to vote." Election Protection Coalition, "About," https://866ourvote.org/about/.

5 Common Cause, the Lawyers' Committee for Civil Rights Under Law, and the Century Foundation, *Deceptive Practices 2.0: Legal and Policy Responses* (Washington, DC: Self-Published, 2008), https://www.commoncause.org/wp-content/uploads/2018/03/0064.pdf.

6 Common Cause and Lawyers Committee for Civil Rights Under Law, *Deceptive Election Practices and Voter Intimidation: The Need for Voter Protection* (Washington, DC: Self-Published, 2012), https://lawyerscommittee.org/wp-content/uploads/2015/07/DeceptivePracticesReportJuly2012FINALpdf.pdf.

7 Davey Alba, "How Voting by Mail Tops Election Misinformation," *New York Times*, September 30, 2020, https://www.nytimes.com/2020/09/30/technology/how-voting-by-mail-tops-election-misinformation.html.

8 Jon Lloyd et al., "Misinformation in the 2020 US Elections: A Timeline of Platform Changes," Mozilla Foundation, March 8, 2021, https://foundation.mozilla.org/en/blog/misinformation-in-the-2020-us-elections-a-timeline-of-platform-changes/.

9 Jon Lloyd et al., "Misinformation in the 2020 US Elections: A Timeline of Platform Changes," Mozilla Foundation, March 8, 2021, https://foundation.mozilla.org/en/blog/misinformation-in-the-2020-us-elections-a-timeline-of-platform-changes/.

10 *See*, e.g., Matt Viser, "Inside the 'Malarkey Factory,' Biden's Online War Room," *Washington Post*, October 19, 2020, https://www.washingtonpost.com/politics/biden-trump-campaign-disinformation/2020/10/18/99774228-0fdd-11eb-8074-0e943a91bf08_story.html.

11 Common Cause, the Lawyers' Committee for Civil Rights Under Law, and the Century Foundation, *Deceptive Practices 2.0: Legal and Policy Responses*, (Washington, DC: Self-Published, 2008), https://www.commoncause.org/wp-content/uploads/2018/03/0064.pdf; Common Cause and Lawyers Committee for Civil Rights Under Law, *Deceptive Election Practices and Voter Intimidation: The Need for Voter Protection* (Washington, DC: Self-Published, 2012), https://lawyerscommittee.org/wp-content/uploads/2015/07/DeceptivePracticesReportJuly2012FINALpdf.pdf; Liz Kennedy, Stephen Spaulding, Tova Wang, Jenny Flanagan and Anthony Kammer, *Bullies at the Ballot Box: Protecting the Freedom to Vote Against Wrongful Challenges and Intimidation* (Washington, DC: Common Cause and Demos, 2012), https://www.commoncause.org/wp-content/uploads/2018/03/BulliesAtTheBallotBox-Final.pdf.

12 Mason Walker and Katerina Eva Matsa, "News Consumption Across Social Media in 2021," Pew Research Center, September 20, 2021, https://www.pewresearch.org/journalism/2021/09/20/news-consumption-across-social-media-in-2021/.

13 Claire Wardle, "Understanding Information Disorder," First Draft, September 22, 2020, https://firstdraftnews.org/long-form-article/understanding-information-disorder/.

14 *See*, e.g., Stephen Collinson, "Trump's Big Lie Is Changing the Face of American Politics," CNN, September 16, 2021, https://www.cnn.com/2021/09/16/politics/trump-big-lie-gop-election/index.html.

15 Tom Kertscher, "Postal Service Says Its Policy Is to Deliver Even Mail Ballots Lacking Postage," *PolitiFact*, July 23, 2020, https://www.politifact.com/factchecks/2020/jul/23/facebook-posts/postal-service-says-its-policy-deliver-even-mail-b/.

16 S. 2747, Freedom to Vote Act, 117th Cong. (2021), Sec. 1304, "Carriage of Election Mail," https://www.congress.gov/bill/117th-congress/senate-bill/2747/text.

17 Storm Gifford, "Jersey Postal Worker Mails It in Before Quitting, Dumps Undelivered Post on Street," *N.Y. Daily News*, October 4, 2018, https://www.nydailynews.com/news/national/ny-news-postal-carrier-quits-job-on-spot-20181004-story.html.

18 Craig Timberg and Beth Reinhard, "As Recount Politics Heat Up, Two Florida Election Officials Are the Targets of Online Harassment," *Washington Post*, November 13, 2018, https://www.washingtonpost.com/technology/2018/11/13/recount-politics-heat-up-two-florida-election-officials-are-targets-online-harassment/.

19 Linda So and Jason Szep, "U.S. Election Workers Get Little Help from Law Enforcement as Terror Threats Mount," *Reuters*, September 8, 2021, https://www.reuters.com/investigates/special-report/usa-election-threats-law-enforcement/.

20 Linda So, "Trump-Inspired Death Threats Are Terrorizing Election Workers," *Reuters*, June 11, 2021, https://www.reuters.com/investigates/special-report/usa-trump-georgia-threats/.

21 Johnny Kauffman, "'You Better Run': After Trump's False Attacks, Election Workers Faced Threats," *NPR*, February 5, 2021, https://www.npr.org/2021/02/05/963828783/you-better-run-after-trumps-false-attacks-election-workers-faced-threats.

22 Matthew Brown, "Fact Check: Georgia 'Suitcase' Video Is Missing Context," *USA Today*, December 14, 2020, https://www.usatoday.com/story/news/factcheck/2020/12/14/fact-check-georgia-suitcase-video-missing-context/3892640001/.

23 Linda So, "Trump-Inspired Death Threats Are Terrorizing Election Workers," *Reuters*, June 11, 2021, https://www.reuters.com/investigates/special-report/usa-trump-georgia-threats/.

24 "Election Officials Under Attack," Brennan Center for Justice and the Bipartisan Policy Center, June 16, 2021, https://www.brennancenter.org/our-work/policy-solutions/election-officials-under-attack.

25 Salvador Rizzo, "Trump's Fusillade of Falsehoods on Mail Voting," *Washington Post*, September 11, 2020, https://www.washingtonpost.com/politics/2020/09/11/trumps-fusillade-falsehoods-mail-voting/.

26 Reid J. Epstein and Stephanie Saul, "Trump Says Mail Voting Means Republicans Would Lose Every Election. Is That True? No.," *Chicago Tribune*, April 10, 2020, https://www.chicagotribune.com/nation-world/ct-nw-nyt-mail-voting-ballots-20200410-qfnxhakicve3ndpxz64lcsqzr4-story.html.

27 Davey Alba, "How Voting by Mail Tops Election Misinformation," *New York Times*, September 30, 2020, https://www.nytimes.com/2020/09/30/technology/how-voting-by-mail-tops-election-misinformation.html.

28 Justin Baragona, "Fox Host Tomi Lahren Claims 'Only Thing' That Will Save Gavin Newsom Is 'Voter Fraud,'" *Daily Beast*, September 8, 2021, https://www.thedailybeast.com/fox-host-tomi-lahren-claims-only-thing-that-will-save-gavin-newsom-is-voter-fraud.

29 Lara Korte, "Larry Elder Prepares for California Recall Loss with Lawyers, Voter Fraud Website," *Sacramento Bee*, September 10, 2021. https://www.sacbee.com/news/politics-government/capitol-alert/article254078633.html.

30 Ben Tobin and Billy Kobin, "'Absurd' and 'Ridiculous': What Officials, Experts Say about Bevin's Voter Fraud Claims," *Courier Journal*, November 7, 2019, https://www.courier-journal.com/story/news/politics/elections/kentucky/2019/11/07/kentucky-governor-election-fact-check-matt-bevins-voter-fraud-claims/2516391001/.

31 Lis Power, "In 2 Weeks after It Called the Election, Fox News Cast Doubt on the Results Nearly 800 Times," Media Matters for America, January 14, 2021, https://www.mediamatters.org/fox-news/2-weeks-after-it-called-election-fox-news-cast-doubt-results-nearly-800-times.

32 Atlantic Council's DFRLab, "#StopTheSteal: Timeline of Social Media and Extremist Activities Leading to 1/6 Insurrection," *Just Security*, February 10, 2021, https://www.justsecurity.org/74622/stopthesteal-timeline-of-social-media-and-extremist-activities-leading-to-1-6-insurrection/.

33 Isaac Stanley-Becker and Anu Narayanswamy, "Trump Has More than $100 Million in Political Cash after First Six Months of 2021," *Washington Post*, August 1, 2021, https://www.washingtonpost.com/politics/2021/07/31/trump-committees-fundraising-2021-fec/.

34 Michael Scherer and Josh Dawsey, "Trump, Talked Out of Announcing a 2024 Bid for Now, Settles on a Wink-and-Nod Unofficial Candidacy," *Washington Post*, October 4, 2021, https://www.washingtonpost.com/politics/trump-2024-campaign-candidacy/2021/10/03/73af3b12-21f8-11ec-b3d6-8cdebe60d3e2_story.html.

35 Scott Pelley, "Whistleblower: Facebook Is Misleading the Public on Progress Against Hate Speech, Violence, Misinformation," *60 Minutes*, October 4, 2021, https://www.cbsnews.com/news/facebook-whistleblower-frances-haugen-misinformation-public-60-minutes-2021-10-03/.

36 Common Cause and Lawyers Committee for Civil Rights Under Law, *Deceptive Election Practices and Voter Intimidation: The Need for Voter Protection* (Washington, DC: Self-Published, 2012), https://lawyerscommittee.org/wp-content/uploads/2015/07/DeceptivePracticesReportJuly2012FINALpdf.pdf.

37 "PolitiFact's Guide to Fake News Websites and What They Peddle," PolitiFact, April 20, 2017, https://www.politifact.com/article/2017/apr/20/politifacts-guide-fake-news-websites-and-what-they/

38 *See* Casey McDermott, Twitter post, September 8, 2020, 11:50am, https://twitter.com/caseymcdermott/status/1303359983728418816 ("Exeter and Bedford, both with pretty big voting populations, wrongly say on their websites 'election officials are not authorized to accept absentee ballots at the polls.' State officials say they're addressing the error. Again, you can still vote absentee at the polls today.").

39 Danny Sullivan, "How We Keep Search Relevant and Useful," *The Keyword* (blog), July 5, 2019,

40 https://blog.google/products/search/how-we-keep-google-search-relevant-and-useful/.

41 Rand Fishkin, "The State of Searcher Behavior Revealed Through 23 Remarkable Statistics," *Moz* (blog), March 14, 2017, https://moz.com/blog/state-of-searcher-behavior-revealed.

42 Online voting presents enormous risks to voter privacy, ballot secrecy, integrity of election results, and, consequently, national security. The option to vote online is not available to the general public. Thirty-three states do offer some form of online voting to overseas and military voters, and a few are now allowing it for people with disabilities. *See*, e.g., Kaleigh Rogers, "New Laws Let Americans With Disabilities Vote Online. They've Also Resurrected the Debate About Voting Access vs. Election Security," *FiveThirtyEight*, July 7, 2021, https://fivethirtyeight.com/features/new-laws-let-americans-with-disabilities-vote-online-theyve-also-resurrected-the-debate-about-voting-access-vs-election-security/; *see also* Eric Geller, "Some States Have Embraced Online Voting. It's a Huge Risk," *Politico*, June 8, 2020, https://www.politico.com/news/2020/06/08/online-voting-304013.

43 Leanna Garfield, "Don't Fall for These Online Voting Scams Circulating the Internet," *Business Insider*, November 8, 2016, https://www.businessinsider.com/online-text-voting-scams-hillary-trump-election-2016-11.

44 Alexa Corse and Dustin Volz, "No, You Can't Vote Via Text or Tweet," *Wall Street Journal*, August 11, 2018, https://www.wsj.com/articles/no-you-cant-vote-via-text-or-tweet-1533985201.

45 Danny Sullivan, "How We Keep Search Relevant and Useful," *The Keyword* (blog), July 15, 2019, https://blog.google/products/search/how-we-keep-google-search-relevant-and-useful/.

46 "How Google autocomplete predictions work," Google Help Center, https://support.google.com/websearch/answer/7368877?hl=en.

47 "How Google Autocomplete Predictions Work," Google Help Center, https://support.google.com/websearch/answer/7368877?hl=en.

48 Amber Phillips, "What Is Ballot 'Harvesting,' and Why Is Trump so against It?," *Washington Post*, May 26, 2020,

49 https://www.washingtonpost.com/politics/2020/05/26/what-is-ballot-harvesting-why-is-trump-so-against-it/.

50 Lily Ray, "2020 Google Search Survey: How Much Do Users Trust Their Search Results?," *Moz* (blog), March 2, 2020, https://moz.com/blog/2020-google-search-survey.

51 Robert Epstein and Ronald E. Robertson, "The Search Engine Manipulation Effect (SEME) and Its Possible Impact on the Outcomes of Elections," Proceedings of the National Academy of Sciences of the United States of America (PNAS), August 4, 2015, https://www.pnas.org/content/pnas/112/33/E4512.full.pdf.

52 "Search Engine Market Share United States Of America," Statcounter GlobalStats, https://gs.statcounter.com/search-engine-market-share/all/united-states-of-america.

53 "Google Pushing Scam Ads on Americans Searching for How to Vote," Tech Transparency Project, June 29, 2020, https://www.techtransparencyproject.org/articles/google-pushing-scam-ads-americans-searching-how-vote.

54 "Google Fails to Stop Exploitative Ads Targeting American Voters," Tech Transparency Project, October 5, 2020, https://www.techtransparencyproject.org/articles/google-fails-stop-exploitative-ads-targeting-american-voters.

55 Ellen Nakashima, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg, "U.S. Government Concludes Iran Was behind Threatening Emails Sent to Democrats," *Washington Post*, October 22, 2020, https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/.

56 Ellen Nakashima, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg, "U.S. Government Concludes Iran Was behind Threatening Emails Sent to Democrats," *Washington Post*, October 22, 2020, https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/.

57 Sec. Jocelyn Benson, Twitter Post, August 27, 2020, 12:12 p.m., https://twitter.com/JocelynBenson/status/1299017044554326019?s=20.

58 *Example of False Information Being Used to Suppress Voting in Detroit*, YouTube video, 0:37, posted by Michigan Department of State/Secretary of State, August 27, 2020, https://youtu.be/JVodAUh9kL0.

59 Will Sommer, "Jacob Wohl Accused of Starting a Voter Suppression Scheme," *Daily Beast*, August 27, 2020, https://www.thedailybeast.com/jacob-wohl-accused-of-starting-a-voter-suppression-scheme?ref=scroll.

60 Meryl Kornfield, "Robocall Targets Battleground States with Falsehoods about Mail-in Voting," *Washington Post*, August 27, 2020, https://www.washingtonpost.com/politics/2020/08/27/robocalls-michigan-penn-voting-jacob-wohl/.

61 Stephanie Saul, "Deceptive Robocalls Try to Frighten Detroit residents about Voting by Mail," *New York Times*, August 27, 2020, https://www.nytimes.com/2020/08/27/us/elections/deceptive-robocalls-try-to-frighten-detroit-residents-about-voting-by-mail.html.

62 Federal Communications Commission, "FCC Proposes $5 Million Robocalling Fine Against Jacob Wohl and John Burkman," news release, August 24, 2021, https://docs.fcc.gov/public/attachments/DOC-375180A1.pdf.

63 William Davies, "What's Wrong with WhatsApp," *The Guardian*, July 2, 2020, https://www.theguardian.com/technology/2020/jul/02/whatsapp-groups-conspiracy-theories-disinformation-democracy.

64 Brooke Auxier and Monica Anderson, "Social Media Use in 2021," Pew Research Center, April 7, 2021, https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/.

65 Elisa Shearer and Amy Mitchell, "News Use Across Social Media Platforms in 2020," Pew Research Center, January 12, 2021, https://www.pewresearch.org/journalism/2021/01/12/news-use-across-social-media-platforms-in-2020/.

66 Sheera Frenkel, "How Misinformation 'Superspreaders' Seed False Election Theories," *New York Times*, November 23, 2020, https://www.nytimes.com/2020/11/23/technology/election-misinformation-facebook-twitter.html.

67 "VoterFraud2020," Jacobs Technion-Cornell Institute at Cornell Tech, https://voterfraud2020.io/.

68 Salvador Rodriguez, "Mark Zuckerberg Shifted Facebook's Focus to Groups after the 2016 Election, and It's Changed How People Use the Site," *CNBC*, February 16, 2020. https://www.cnbc.com/2020/02/16/zuckerbergs-focus-on-facebook-groups-increases-facebook-engagement.html.

69 Jordan Davis, "Making Groups Privacy Settings Easier to Understand," Facebook, August 14, 2019, https://about.fb.com/

news/2019/08/groups-privacy-settings/.

70 Dave Johnson, "What Is Telegram? A Quick Guide to the Fast and Secure Messaging Platform," *Business Insider*, March 24, 2021, https://www.businessinsider.com/what-is-telegram.

71 Michael Schwirtz, "Telegram, Pro-Democracy Tool, Struggles Over New Fans From Far Right," *New York Times*, January 26, 2021, https://www.nytimes.com/2021/01/26/world/europe/telegram-app-far-right.html.

72 Ashley Carman, "Peloton Is Blocking the #StopTheSteal Hashtag from Being Created or Used," *The Verge*, January 11, 2021, https://www.theverge.com/2021/1/11/22225197/peloton-stop-the-steal-tag-banned-donald-trump.

73 Center for an Informed Public, Digital Forensic Research Lab, Graphika, & Stanford Internet Observatory, "The Long Fuse: Misinformation and the 2020 Election," Stanford Digital Repository: Election Integrity Partnership v1.3.0, 2021, https://purl.stanford.edu/tr171zs0069.

74 "A Look at Facebook and US 2020 Elections," Facebook, December 2020, https://about.fb.com/wp-content/uploads/2020/12/US-2020-Elections-Report.pdf.

75 Galen Stocking et al., "YouTube News Consumers about as Likely to Use the Site for Opinions as for Facts," Pew Research Center, September 28, 2020, https://www.pewresearch.org/journalism/2020/09/28/youtube-news-consumers-about-as-likely-to-use-the-site-for-opinions-as-for-facts/.

76 Casey Newton, "How YouTube Failed the 2020 Election Test," *Platformer*, March 3, 2021, https://www.platformer.news/p/how-youtube-failed-the-2020-election.

77 Sheera Frenkel, "Election Misinformation Often Evaded YouTube's Efforts to Stop It," *New York Times*, November 18, 2020, https://www.nytimes.com/2020/11/18/technology/election-misinformation-often-evaded-youtubes-efforts-to-stop-it.html.

78 Craig Silverman, "This Pro-Trump YouTube Network Sprang Up Just After He Lost," *BuzzFeed News*, January 8, 2021, https://www.buzzfeednews.com/article/craigsilverman/epoch-times-trump-you-tube.

79 "Supporting the 2020 U.S. Election," YouTube Official Blog (blog), December 9, 2020, https://blog.youtube/news-and-events/supporting-the-2020-us-election/.

80 "Supporting the 2020 U.S. Election," YouTube Official Blog (blog), December 9, 2020, https://blog.youtube/news-and-events/supporting-the-2020-us-election/.

81 "YouTube Still Awash in False Voter Fraud Claims," Tech Transparency Project, December 22, 2020, https://www.techtransparencyproject.org/articles/youtube-still-awash-false-voter-fraud-claims.

82 Shannon Bond, "Twitter Says Steps to Curb Election Misinformation Worked," *NPR*, November 12, 2020, https://www.npr.org/sections/live-updates-2020-election-results/2020/11/12/934267731/twitter-says-steps-to-curb-election-misinformation-worked.

83 Makena Kelly, "TikTok Removed More than 300,000 Videos for Election Misinformation," *The Verge*, February 24, 2021, https://www.theverge.com/2021/2/24/22298024/tiktok-election-misinformation-disinformation-transparency-report.

84 Jessica Bursztynsky, "TikTok Says 1 Billion People Use the App Each Month," *CNBC*, September 27, 2021, https://www.cnbc.com/2021/09/27/tiktok-reaches-1-billion-monthly-users.html; Kari Paul, "TikTok: False Posts about US Election Reach Hundreds of Thousands," *The Guardian*, November 5, 2020, https://www.theguardian.com/technology/2020/nov/05/tiktok-us-election-misinformation.

85 Ellie House, "Rumble Sends Viewers Tumbling Toward Misinformation," *Wired*, May 11, 2021, https://www.wired.com/story/rumble-sends-viewers-tumbling-toward-misinformation/.

86 United States Senate Select Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election," Vol. 2, 116th Cong. (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

87 United States Senate Select Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election," Vol. 2, 116th Cong. (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

88 Tim Mak, "Senate Report: Russians Used Social Media Mostly to Target Race In 2016," *NPR*, October 8, 2019, https://www.npr.org/2019/10/08/768319934/senate-report-russians-used-used-social-media-mostly-to-target-race-in-2016.

89 Scott Shane, "These Are the Ads Russia Bought on Facebook in 2016," *New York Times*, November 1, 2017, https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html.

90 Ellen Nakashima et al., "U.S. Government Concludes Iran Was Behind Threatening Emails Sent to Democrats," *Washington Post*, October 22, 2020, https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/.

91 Jen Kirby, "Yes, Russia Is Interfering in the 2020 Election," Vox, September 21, 2020, https://www.vox.com/2020/9/21/21401149/russia-2020-election-meddling-trump-biden.

92 "Intelligence Community Assessment: Foreign Threats to the 2020 US Federal Elections (Declassified)," National Intelligence Council, March 10, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

93 Carrie Levine, "Online Misinformation during the Primaries: A Preview of What's to Come?," Center for Public Integrity, March 11, 2020, https://publicintegrity.org/politics/elections/online-misinformation-during-the-primaries-a-preview-of-whats-

to-come/.

94 Jennifer Agiesta and Ariel Edwards-Levy, "CNN Poll: Most Americans Feel Democracy Is under Attack in the US," *CNN*, September 15, 2021, https://www.cnn.com/2021/09/15/politics/cnn-poll-most-americans-democracy-under-attack/index.html.

95 Allie Morris, "Hours after Trump Calls for Audit of 2020 Texas Election, State Says It's Auditing 4 Urban Counties," *Dallas Morning News*, September 23, 2021, https://www.dallasnews.com/news/politics/2021/09/23/trump-to-abbott-add-2020-election-audit-bill-to-texas-legislatures-special-session/.

96 Tim Reid and Nathan Layne, Jason Lange, "Special Report: Backers of Trump's False Fraud Claims Seek to Control next Elections," *Reuters*, September 22, 2021, https://www.reuters.com/world/us/backers-trumps-false-fraud-claims-seek-control-next-us-elections-2021-09-22/.

97 Shannon Bond, "Just 12 People Are Behind Most Vaccine Hoaxes On Social Media, Research Shows," *NPR*, May 14, 2021, https://www.npr.org/2021/05/13/996570855/disinformation-dozen-test-facebooks-twitters-ability-to-curb-vaccine-hoaxes.

98 Nicole Hong, "Twitter Troll Tricked 4,900 Democrats in Vote-by-Phone Scheme, U.S. Says," *New York Times*, January 27, 2021, https://www.nytimes.com/2021/01/27/nyregion/douglass-mackey-arrested-far-right-twitter.html.

99 *U.S. v. Douglas Mackey*, Complaint 1 (E.D.N.Y. January 22, 2021), https://www.justice.gov/opa/press-release/file/1360816/download.

100 *U.S. v. Douglas Mackey*, Complaint 21 (E.D.N.Y. January 22, 2021), https://www.justice.gov/opa/press-release/file/1360816/download.

101 Center for an Informed Public, Digital Forensic Research Lab, Graphika, & Stanford Internet Observatory, "The Long Fuse: Misinformation and the 2020 Election," Stanford Digital Repository: Election Integrity Partnership v1.3.0 (2021), https://purl.stanford.edu/tr171zs0069.

102 Center for an Informed Public, Digital Forensic Research Lab, Graphika, & Stanford Internet Observatory, "The Long Fuse: Misinformation and the 2020 Election," Stanford Digital Repository: Election Integrity Partnership v1.3.0 (2021), https://purl.stanford.edu/tr171zs0069.

103 "Facebook: From Election to Insurrection," Avaaz, March 18, 2021, https://secure.avaaz.org/campaign/en/facebook_election_insurrection/.

104 Jane Mayer, "The Big Money Behind the Big Lie," *New Yorker*, August 9, 2021, https://www.newyorker.com/magazine/2021/08/09/the-big-money-behind-the-big-lie.

105 Jane Mayer, "The Big Money Behind the Big Lie," *New Yorker*, August 9, 2021, https://www.newyorker.com/magazine/2021/08/09/the-big-money-behind-the-big-lie.

106 Jane Mayer, "The Big Money Behind the Big Lie," *New Yorker*, August 9, 2021, https://www.newyorker.com/magazine/2021/08/09/the-big-money-behind-the-big-lie.

107 U.S. Rep. Zoe Lofgren (D-CA) has published a 1,939-page catalog of disinformation and misinformation social media posts by Republican members of the House of Representatives who voted to overturn the 2020 presidential election in service of former president Trump's "Big Lie." *See* Rep. Zoe Lofgren, "Social Media Review: Members of the U.S. House of Representatives Who Voted to Overturn the 2020 Presidential Election," https://housedocs.house.gov/lofgren/SocialMediaReview8.pdf.

108 Isaac Stanley-Becker and Anu Narayanswamy, "Trump Has More than $100 Million in Political Cash after First Six Months of 2021," *Washington Post*, August 1, 2021, https://www.washingtonpost.com/politics/2021/07/31/trump-committees-fundraising-2021-fec/.

109 Luke Broadwater, Catie Edmondson and Rachel Shorey, "Fund-Raising Surged for Republicans Who Sought to Overturn the Election," *New York Times*, April 17, 2021, https://www.nytimes.com/2021/04/17/us/politics/republicans-fund-raising-capitol-riot.html.

110 Luke Broadwater, Catie Edmondson and Rachel Shorey, "Fund-Raising Surged for Republicans Who Sought to Overturn the Election," *New York Times*, April 17, 2021, https://www.nytimes.com/2021/04/17/us/politics/republicans-fund-raising-capitol-riot.html.

111 Nicholas Reimann, "Arizona Audit Cost Trump Supporters Nearly $6 Million—Only to Assert Biden Won by Even More," *Forbes*, September 24, 2021, https://www.forbes.com/sites/nicholasreimann/2021/09/24/arizona-audit-cost-trump-supporters-nearly-6-million-only-to-assert-biden-won-by-even-more/?sh=72519b1e2410.

112 "What Happened in Arizona Did Not Stay in Arizona," States United Action, Fair Fight Action, United to Protect Democracy, https://notanaudit.com/.

113 Rosalind S. Helderman, "Arizona Ballot Review Commissioned by Republicans Reaffirms Biden's Victory," *Washington Post*, September 24, 2021, https://www.washingtonpost.com/politics/arizona-ballot-review-draft-report/2021/09/24/7c19ac08-1562-11ec-b976-f4a43b740aeb_story.html.

114 Jane Mayer, "The Big Money Behind the Big Lie," *The New Yorker*, August 9, 2021, https://www.newyorker.com/magazine/2021/08/09/the-big-money-behind-the-big-lie.

115 Jane Mayer, "The Big Money Behind the Big Lie," *The New Yorker*, August 9, 2021, https://www.newyorker.com/magazine/2021/08/09/the-big-money-behind-the-big-lie.

116 Telegram, "Terms of Service," accessed October 19, 2021, https://telegram.org/tos.

117 Tom Kertscher, "No Truth to the Claim That Arizona Audit Found Trump up by 250,000 votes," PolitiFact, May 7, 2021, https://www.politifact.com/factchecks/2021/may/07/facebook-posts/no-truth-claim-arizona-audit-found-trump-250000-vo/.

118 Reuters Fact Check, "Fact Check—Maricopa County Database Was not Deleted," *Reuters*, May 21, 2021, https://www.reuters.com/article/factcheck-maricopa-database/fact-check-maricopa-county-database-was-not-deleted-idUSL2N2N8266.

119 Daniel Funke, "Fact Check: Georgia Military, Overseas Ballots not Evidence of Election Fraud," *USA Today*, May 29, 2021, https://www.usatoday.com/story/news/factcheck/2021/05/29/fact-check-georgia-military-overseas-ballots-not-evidence-fraud/7450430002/.

120 Keith Zubrow, "Facebook Whistleblower Says Company Incentivizes 'Angry, Polarizing, Divisive Content,'" *CBS News*, October 4, 2021, https://www.cbsnews.com/news/facebook-whistleblower-frances-haugen-60-minutes-polarizing-divisive-content/.

121 PolitiFact, "How We Determine Truth-O-Meter Ratings," last updated October 27, 2020, https://www.politifact.com/article/2018/feb/12/principles-truth-o-meter-politifacts-methodology-i/.

122 *See 281 Care Committee v. Arneson*, 766 F.3d 774 (8th Cir. 2014) (holding unconstitutional Minn. Stat. § 211B.06, which prohibited dissemination of false paid political advertising about the personal or political character or acts of a candidate, or about the effect of a ballot question); *see also Susan B. Anthony List v. Driehaus*, 814 F.3d 466 (2016) (holding unconstitutional Ohio Rev. Code Ann. §3517.21(B)(9)-(10), which made it illegal to "[m]ake a false statement concerning the voting record of a candidate or public official," or to "[p]ost, publish, circulate, distribute, or otherwise disseminate a false statement concerning a candidate").

123 Richard L. Hasen, "A Constitutional Right to Lie in Campaigns and Elections?," 74 Mont. L. Rev. 53, 71 (2013), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2151618.

124 Act to Establish the Department of Justice, ch. 150, 16 Stat. 162 (1870).

125 *See* U.S. Senate, "The Enforcement Acts of 1870 and 1871," https://www.senate.gov/artandhistory/history/common/generic/EnforcementActs.htm.

126 U.S. Dept. of Justice, "Federal Prosecution of Election Offenses," 50, 8th ed. December 2017, https://www.justice.gov/criminal/file/1029066/download.

127 52 U.S.C. § 20511(1).

128 18 U.S. Code § 594.

129 U.S. Dept. of Justice, "Federal Prosecution of Election Offenses," 52, 8th ed. December 2017, https://www.justice.gov/criminal/file/1029066/download.

130 18 U.S.C. § 241.

131 U.S. Dept. of Justice, "Federal Prosecution of Election Offenses," 56, 8th ed. December 2017, https://www.justice.gov/criminal/file/1029066/download.

132 *U.S. v. Douglas Mackey*, Complaint 1 (E.D.N.Y. January 22, 2021), https://www.justice.gov/opa/press-release/file/1360816/download.

133 Tasneem Nashrulla and Ryan Mac, "The Racist Guy Behind One of the Most Influential Pro-Trump Twitter Accounts Was Arrested for Election Interference," *BuzzFeed News*, January 27, 2021, https://www.buzzfeednews.com/article/tasneemnashrulla/ricky-vaughn-twitter-troll-arrested-election-interference.

134 *U.S. v. Douglas Mackey*, Complaint 23 (E.D.N.Y. January 22, 2021), https://www.justice.gov/opa/press-release/file/1360816/download.

135 Nicole Hong, "Twitter Troll Tricked 4,900 Democrats in Vote-by-Phone Scheme, U.S. Says," *New York Times*, January 27, 2021, https://www.nytimes.com/2021/01/27/nyregion/douglass-mackey-arrested-far-right-twitter.html.

136 52 U.S.C. § 10307(b); *see also* 52 U.S.C. § 10101(b).

137 *United States v. North Carolina Republican Party*, 5:92-cv-00161 (E.D.N.C. 1992).

138 Michael Weingartner, "Remedying Intimidating Voter Disinformation Through § 1985(3)'s Support or Advocacy Clauses," Georgetown L. Rev. (forthcoming 2021), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3914719; *citing* 42 U.S.C. § 1985.

139 Colo. Rev. Stat. § 1-13-109.

140 Colorado Attorney General Phil Weiser, "Public Advisory on Voter Intimidation Crimes and Poll Security," October 19, 2020, https://coag.gov/app/uploads/2020/10/Public-Advisory-Voter-Intimidation-10.19.2020.pdf.

141 Haw. Rev. Stat. § 19-3(12).

142 Va. Code Ann. § 24.2-1005.1(A).

143 Va. Code Ann. § 24.2-1005.1(C).

144 L. Brandeis, Other People's Money 62 (National Home Library Foundation ed. 1933).

145 *Buckley v. Valeo*, 424 U.S. 1, 67 (1976).

146 *Buckley*, 424 U.S. at 66-67.

147 *Buckley*, 424 U.S. at 67.

148 *Buckley*, 424 U.S. at 67.

149 *Gaspee Project v. Mederos*, Case No. 20-1944 (1st Cir. September 14, 2021).

150 52 U.S.C. § 30104(a)-(b).

151 52 U.S.C. § 30120.

152 52 U.S.C. § 30101(17).

153 52 U.S.C. § 30104(f).

154 52 U.S.C. § 30120.

155 52 U.S.C. § 30124(a).

156 52 U.S.C. § 30124(b).

157 Policy Statement of Commissioner Lee E. Goodman on the Fraudulent Misrepresentation Doctrine, February 16, 2018, https://www.fec.gov/resources/cms-content/documents/Commissioner_Lee_E._Goodman_Policy_Statement_-_Fraudulent_Misrepresentation.pdf.

158 Policy Statement of Commissioner Lee E. Goodman on the Fraudulent Misrepresentation Doctrine, February 16, 2018, https://www.fec.gov/resources/cms-content/documents/Commissioner_Lee_E._Goodman_Policy_Statement_-_Fraudulent_Misrepresentation.pdf.

159 By contrast, the FEC has on occasion taken enforcement action when the required disclaimer was omitted entirely. For example, in *FEC v. Novacek*, 739 F. Supp. 2d 957 (N.D. Tex. 2010), a federal court at the commission's urging ordered a defendant to pay a $47,414 civil penalty for fraudulently misrepresenting themselves as acting on behalf of a political party when soliciting funds and failing to include in their communications the required disclaimer. A summary of the case and litigation documents can be found on the FEC website here: https://www.fec.gov/legal-resources/court-cases/fec-v-novacek/.

160 Alaska applies disclosure requirements to "nongroup entities," defined to mean "a person, other than an individual, that takes action the major purpose of which is to influence the outcome of an election" and that "cannot participate in business activities," "does not have shareholders who have a claim on corporate earnings," and is "independent from the influence of business corporations." Alaska Stat. § 15.13.400(13).

161 Alaska Stat. § 15.13.040(j).

162 Cal. Gov. Code § 84222.

163 Cal. Assembly Bill 2188, signed September 26, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB2188.

164 Md. Code, Elec. Law § 13-309.2.

165 Minn. Stat. Ann. § 10A.27 Subd.15(b).

166 17 R.I. Gen. Laws § 17-25.3-1.

167 Wash. Rev. Code § 42.17A.320.

168 Wash. Admin. Code § 390-18-030.

169 Wash. Admin. Code § 390-18-050.

170 47 U.S.C. § 230.

171 John Bergmayer, "What Section 230 Is and Does—Yet Another Explanation of One of the Internet's Most Important Laws," Public Knowledge, May. 14, 2019, https://www.publicknowledge.org/blog/what-section-230-is-and-does-yet-another-explanation-of-one-of-the-internets-most-important-laws/.

172 47 U.S.C § 230(c)(1) (stating that platforms and users may not "be treated as the publisher or speaker of any information provided by another").

173 47 U.S.C. § 230(c)(2) (stating that platforms may not be held liable for "good faith" attempts "to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable").

174 *See* Jesse Littlewood and Emma Steiner, "Trending in the Wrong Direction: Social Media Platforms' Declining Enforcement of Voting Disinformation," Common Cause, September 2, 2021, https://www.commoncause.org/wp-content/uploads/2021/09/Disinfo_WhitePaperv3.pdf; "Facebook: From Election to Insurrection, Avaaz, March 18, 2021, https://avaazimages.avaaz.org/facebook_election_insurrection.pdf; Rachel Lerman, "Facebook Says It Has Taken Down 7 Million Posts for Spreading Coronavirus Misinformation," *Washington Post*, August 11, 2020, https://www.washingtonpost.com/technology/2020/08/11/facebook-covid-misinformation-takedowns/.

175 "Facebook: From Election to Insurrection, Avaaz, March 18, 2021, https://avaazimages.avaaz.org/facebook_election_insurrection.pdf.

176 Jesse Littlewood and Emma Steiner, "Trending in the Wrong Direction: Social Media Platforms' Declining Enforcement of

Voting Disinformation," Common Cause, September 2, 2021, https://www.commoncause.org/wp-content/uploads/2021/09/Disinfo_WhitePaperv3.pdf.

177 Harold Feld, "What Is Next for Section 230 Reform," *Pro Market*, November 18, 2020, https://promarket.org/2020/11/18/what-next-for-section-230-reform-court-fcc/.

178 Kiran Jeevanjee et al., "All the Ways Congress Wants to Change Section 230," *Slate*, March 23, 2021, https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html.

179 H.R. 874, Abandoning Online Censorship Act, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/874/text?q=%7B%22search%22%3A%5B%22section+230%22%5D%7D&r=1&s=3.

180 S. 1384, 21st Century Foundation for the Right to Express and Engage Speech Act, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1384/text.

181 Senator Bill Hagerty, "Hagerty Introduces Bill to Combat Big Tech Censorship; Treat Big Tech Corporations as Common Carriers," news release, April 27, 2021, https://www.hagerty.senate.gov/press-releases/2021/04/27/hagerty-introduces-bill-to-combat-big-tech-censorship-treat-big-tech-corporations-as-common-carriers/.

182 S. 797, Platform Accountability and Online Transparency Act, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/797/text.

183 House Committee on Energy and Commerce, "E&C Leaders Announce Legislation to Reform Section 230," news release, October 14, 2021, https://energycommerce.house.gov/newsroom/press-releases/ec-leaders-announce-legislation-to-reform-section-230.

184 Letter from public interest and civil rights groups to White House and 117th Congress, January 27, 2021, https://cdn.vox-cdn.com/uploads/chorus_asset/file/22261662/Section_230_Letter___Jan_27___2021____1_.pdf.

185 Federal Trade Commission," Our History," https://www.ftc.gov/about-ftc/our-history.

186 15 U.S.C. § 45.

187 Federal Trade Commission, "FTC Policy Statement on Unfairness, Federal Trade Commission," December 17, 1980, https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

188 Federal Trade Commission, "Enforcement Policy Statement on Deceptively Formatted Advertisements," https://www.ftc.gov/system/files/documents/public_statements/896923/151222deceptiveenforcement.pdf.

189 Federal Trade Commission, "Federal Trade Commission 2020 Privacy and Data Security Update," 2020, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf.

190 Federal Trade Commission, "Federal Trade Commission 2020 Privacy and Data Security Update," 2020 https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf.

191 Rosalie Chan, "The Cambridge Analytica Whistleblower Explains How the Firm Used Facebook Data to Sway Elections," *Business Insider*, October 5, 2019, https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10.

192 Christopher Wylie, "How I Helped Hack Democracy," *New York Intelligencer*, October 4, 2019, https://nymag.com/intelligencer/2019/10/book-excerpt-mindf-ck-by-christopher-wylie.html.

193 Rosalie Chan, "The Cambridge Analytica Whistleblower Explains How the Firm Used Facebook Data to Sway Elections," *Business Insider*, October 5, 2019, https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10.

194 Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," news release, July 24, 2019, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

195 Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," news release, July 24, 2019, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

196 Federal Trade Commission, "FTC Issues Opinion and Order Against Cambridge Analytica for Deceiving Consumers About the Collection of Facebook Data, Complain with EU-U.S. Privacy Shield," news release, December 6, 2019, https://www.ftc.gov/news-events/press-releases/2019/12/ftc-issues-opinion-order-against-cambridge-analytica-deceiving.

197 Federal Trade Commission, "FTC Issues Opinion and Order Against Cambridge Analytica for Deceiving Consumers About the Collection of Facebook Data, Complain with EU-U.S. Privacy Shield," news release, December 6, 2019, https://www.ftc.gov/news-events/press-releases/2019/12/ftc-issues-opinion-order-against-cambridge-analytica-deceiving.

198 Chris Jay Hoofnagle, Woodrow Hartzog and Daniel J. Solove, "The FTC Can Rise to the Privacy Challenge, but not Without Help from Congress," Brookings Institution, August 8, 2019, https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/.

199 Federal Trade Commission, "Congressional Budget Justification Fiscal Year 2022," May 28, 2021, https://www.ftc.gov/

system/files/documents/reports/fy-2022-congressional-budget-justification/fy22cbj.pdf.

200 Federal Trade Commission, "FTC Report on Resources Used and Needed for Protecting Consumer Privacy and Security," 2020, https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportresourcesprivacydatasecurity.pdf.

201 Chris Jay Hoofnagle, Woodrow Hartzog and Daniel J. Solove, "The FTC Can Rise to the Privacy Challenge, but not Without Help from Congress," Brookings Institution, August 8, 2019, https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/.

202 Nilay Patel, "Facebook's $5 billion FTC Fine Is an Embarrassing Joke," *The Verge*, July 12, 2019, https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke.

203 Rohit Chopra, "Dissenting Statement of Commissioner Rohit Chopra," July 24, 2019, https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

204 Joel Breakstone et. al, "Students' Civic Online Reasoning: A National Portrait," Stanford History Education Group, November 14, 2019, https://purl.stanford.edu/gf151tb4868.

205 Michael Copps, "Learning Digital Literacy Is Key," Democracy Wire (blog), March 11, 2021, https://www.commoncause.org/democracy-wire/learning-digital-literacy-is-key/.

206 Paula Span, "Getting Wise to Fake News," *New York Times*, October 14, 2020, https://www.nytimes.com/2020/09/11/health/misinformation-social-media-elderly.html.

207 Paula Span, "Getting Wise to Fake News," *New York Times*, October 14, 2020, https://www.nytimes.com/2020/09/11/health/misinformation-social-media-elderly.html.

208 Michael Copps, "Learning Digital Literacy Is Key," Democracy Wire (blog), March 11, 2021, https://www.commoncause.org/democracy-wire/learning-digital-literacy-is-key/.

209 Sarah Schwartz, "More States Say They're Teaching Media Literacy, but What That Means Varies," *Education Week*, January 08, 2020, https://www.edweek.org/teaching-learning/more-states-say-theyre-teaching-media-literacy-but-what-that-means-varies/2020/01.

210 Peter Medlin, "Illinois State Law Is the First to Have High Schools Teach News Literacy, *NPR*, August 12, 2021, https://www.npr.org/2021/08/12/1026993142/illinois-is-the-first-state-to-have-high-schools-teach-news-literacy.

211 Media Literacy Advisory Committee, "Media Literacy Advisory Committee Report," Colorado Department of Education, December 2019, https://www.cde.state.co.us/cdedepcom/medialiteracyadvisorycommitteereport.

212 Matthew Ingram, "Section 230 Critics Are Forgetting About the First Amendment," *Columbia Journalism Review*, July 29, 2021, https://www.cjr.org/the_media_today/section-230-critics-are-forgetting-about-the-first-amendment.php.

213 Alex Campbell, "How Data Privacy Laws Can Fight Fake News," *Just Security*, August 15, 2019, https://www.justsecurity.org/65795/how-data-privacy-laws-can-fight-fake-news/.

214 Alex Campbell, "How Data Privacy Laws Can Fight Fake News," *Just Security*, August 15, 2019, https://www.justsecurity.org/65795/how-data-privacy-laws-can-fight-fake-news/.

215 Thorin Klosowski, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)," *New York Times*, September 6, 2021, https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

216 Attorney General Bob Bonta, "California Consumer Privacy Act (CCPA)," State of California Department of Justice, https://oag.ca.gov/privacy/ccpa.

217 Attorney General Bob Bonta, "California Consumer Privacy Act (CCPA)," State of California Department of Justice, https://oag.ca.gov/privacy/ccpa.

218 Thorin Klosowski, "The State of Consumer Data Privacy Laws in the US (and Why It Matters)," *New York Times*, September 6, 2021, https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

219 Saja Hindi, "New Data Privacy Laws Lets Coloradans Choose Whether Companies Can Collect Information," *Denver Post*, July 7, 2021, https://www.denverpost.com/2021/07/07/data-privacy-colorado-new-law/.

220 Saja Hindi, "New Data Privacy Laws Lets Coloradans Choose Whether Companies Can Collect Information," *Denver Post*, July 7, 2021, https://www.denverpost.com/2021/07/07/data-privacy-colorado-new-law/.

221 Sarah Rippy, "Colorado Privacy Act Becomes Law," International Association of Privacy Professionals (IAPP), July 8, 2021, https://iapp.org/news/a/colorado-privacy-act-becomes-law/.

222 Sarah Rippy, "Colorado Privacy Act Becomes Law," International Association of Privacy Professionals (IAPP), July 8, 2021, https://iapp.org/news/a/colorado-privacy-act-becomes-law/.

223 Sarah Rippy, "Colorado Privacy Act Becomes Law," International Association of Privacy Professionals (IAPP), July 8, 2021, https://iapp.org/news/a/colorado-privacy-act-becomes-law/.

224 Kate Cox, "Virginia Is About to Get a Major California-Style Data Privacy Law," *Ars Technica*, February 11, 2021, https://arstechnica.com/tech-policy/2021/02/virginia-is-about-to-get-a-major-california-style-data-privacy-law/.

225 Kate Cox, "Virginia Is About to Get A Major California-Style Data Privacy Law," *Ars Technica*, February 11, 2021, https://

arstechnica.com/tech-policy/2021/02/virginia-is-about-to-get-a-major-california-style-data-privacy-law/.

226 Kate Cox, "Virginia Is About to Get A Major California-Style Data Privacy Law," *Ars Technica*, February 11, 2021, https://arstechnica.com/tech-policy/2021/02/virginia-is-about-to-get-a-major-california-style-data-privacy-law/.

227 Hayley Tsukayama, "Improving Enforcement in State Consumer Privacy Laws," Electronic Frontier Foundation, July 7, 2021, https://www.eff.org/deeplinks/2021/07/improving-enforcement-state-consumer-privacy-laws.

228 *See* Twitter, "Civic Integrity Policies," https://help.twitter.com/en/rules-and-policies/election-integrity-policy.

229 *See* Facebook, "Community Standards," https://transparency.fb.com/policies/community-standards/.

230 YouTube, "How Does YouTube Support Civic Engagement and Stay Secure, Impartial, and Fair During Elections?," https://www.youtube.com/howyoutubeworks/our-commitments/supporting-political-integrity/.

231 Twitter, "Civic Integrity Policies," https://help.twitter.com/en/rules-and-policies/election-integrity-policy.

232 Facebook, "Community Standards," https://transparency.fb.com/policies/community-standards/

233 Jon Lloyd et al., "Misinformation in the 2020 US Elections: A Timeline of Platform Changes," Mozilla Foundation, March 8, 2021, https://foundation.mozilla.org/en/blog/misinformation-in-the-2020-us-elections-a-timeline-of-platform-changes/.

234 Jon Lloyd et al., "Misinformation in the 2020 US Elections: A Timeline of Platform Changes," Mozilla Foundation, March 8, 2021, https://foundation.mozilla.org/en/blog/misinformation-in-the-2020-us-elections-a-timeline-of-platform-changes/.

235 Jon Lloyd et al., "Misinformation in the 2020 US Elections: A Timeline of Platform Changes," Mozilla Foundation, March 8, 2021, https://foundation.mozilla.org/en/blog/misinformation-in-the-2020-us-elections-a-timeline-of-platform-changes/.

236 Jon Lloyd et al., "Misinformation in the 2020 US Elections: A Timeline of Platform Changes," Mozilla Foundation, March 8, 2021, https://foundation.mozilla.org/en/blog/misinformation-in-the-2020-us-elections-a-timeline-of-platform-changes/.

237 Jesse Littlewood and Emma Steiner, "Trending in the Wrong Direction: Social Media Platforms' Declining Enforcement of Voting Disinformation," Common Cause, September 2, 2021, https://www.commoncause.org/wp-content/uploads/2021/09/Disinfo_WhitePaperv3.pdf.

238 Jon Lloyd et al., "Misinformation in the 2020 US Elections: A Timeline of Platform Changes," Mozilla Foundation, March 8, 2021, https://foundation.mozilla.org/en/blog/misinformation-in-the-2020-us-elections-a-timeline-of-platform-changes/.

239 Jesse Littlewood and Emma Steiner, "Trending in the Wrong Direction: Social Media Platforms' Declining Enforcement of Voting Disinformation," Common Cause, September 2, 2021, https://www.commoncause.org/wp-content/uploads/2021/09/Disinfo_WhitePaperv3.pdf.

240 Jesse Littlewood and Emma Steiner, "Trending in the Wrong Direction: Social Media Platforms' Declining Enforcement of Voting Disinformation," Common Cause, September 2, 2021, https://www.commoncause.org/wp-content/uploads/2021/09/Disinfo_WhitePaperv3.pdf.

241 Jeff Horwitz, "Facebook Has Made Lots of New Rules This Year. It Doesn't Always Enforce Them.," *Wall Street Journal*, October 15, 2020, https://www.wsj.com/articles/facebook-has-made-lots-of-new-rules-this-year-it-doesnt-always-enforce-them-11602775676.

242 Alex Heath, "Facebook to End Special Treatment for Politicians After Trump Ban," *The Verge*, June 3, 2021, https://www.theverge.com/2021/6/3/22474738/facebook-ending-political-figure-exemption-moderation-policy.

243 Facebook, "Our Approach to Newsworthy Content," July 29, 2021, https://transparency.fb.com/features/approach-to-newsworthy-content/.

244 Alex Heath, "Facebook to End Special Treatment for Politicians After Trump Ban," *The Verge*, June 3, 2021, https://www.theverge.com/2021/6/3/22474738/facebook-ending-political-figure-exemption-moderation-policy.

245 Alex Heath, "Facebook to End Special Treatment for Politicians After Trump Ban," *The Verge*, June 3, 2021, https://www.theverge.com/2021/6/3/22474738/facebook-ending-political-figure-exemption-moderation-policy.

246 Mike Isaac and Cecilia Kang, "Facebook Says It Won't Back Down from Allowing Lies in Political Ads," *New York Times*, September 4, 2020, https://www.nytimes.com/2020/01/09/technology/facebook-political-ads-lies.html.

247 Mike Isaac and Cecilia Kang, "Facebook Says It Won't Back Down from Allowing Lies in Political Ads," *New York Times*, September 4, 2020, https://www.nytimes.com/2020/01/09/technology/facebook-political-ads-lies.html.

248 Mike Isaac, "Whistler-Blower to Accuse Facebook of Contributing to Jan. 6 Riot, Memo Says," *New York Times*, October 13, 2021, https://www.nytimes.com/2021/10/02/technology/whistle-blower-facebook-memo.html.

249 Mike Isaac, "Whistler-Blower to Accuse Facebook of Contributing to Jan. 6 Riot, Memo Says," *New York Times*, October 13, 2021, https://www.nytimes.com/2021/10/02/technology/whistle-blower-facebook-memo.html.

250 Jesse Littlewood and Emma Steiner, "Trending in the Wrong Direction: Social Media Platforms' Declining Enforcement of Voting Disinformation," Common Cause, September 2, 2021, https://www.commoncause.org/wp-content/uploads/2021/09/Disinfo_WhitePaperv3.pdf.

251 Nick Clegg, "In Response to Oversight Board, Trump Suspended for Two Years; Will Only Be Reinstated if Conditions Permit," Facebook, June 4, 2021, https://about.fb.com/news/2021/06/facebook-response-to-oversight-board-recommendations-trump/.

252 Nick Clegg, "In Response to Oversight Board, Trump Suspended for Two Years; Will Only Be Reinstated if Conditions Permit,"

Facebook, June 4, 2021, https://about.fb.com/news/2021/06/facebook-response-to-oversight-board-recommendations-trump/.

253 Common Cause, "Common Cause and Over 20 Organizations Demand Facebook Close Loophole That Allows Trump to Stay on Platform Despite Ban," news release, July 26, 2021, https://www.commoncause.org/press-release/common-cause-and-over-20-organizations-demand-facebook-close-loophole-that-allows-trump-to-remain-on-platform-despite-ban/.

254 Parker Molloy, "Twitter's Enforcement Inconsistency Undermines Its Efforts at Policy Reforms," Media Matters for America, August 7, 2020, https://www.mediamatters.org/twitter/twitters-enforcement-inconsistency-undermines-its-efforts-policy-reforms.

255 Parker Molloy, "Twitter's Enforcement Inconsistency Undermines Its Efforts at Policy Reforms," Media Matters for America, August 7, 2020, https://www.mediamatters.org/twitter/twitters-enforcement-inconsistency-undermines-its-efforts-policy-reforms.

256 Twitter, "About Public-Interest Exceptions on Twitter," https://help.twitter.com/en/rules-and-policies/public-interest.

257 Sara Morrison, "Facebook and Twitter Made Special World Leader Rules for Trump. What Happens Now?," *Vox*, January 20, 2021, https://www.vox.com/recode/22233450/trump-twitter-facebook-ban-world-leader-rules-exception.

258 Twitter, "About Public-Interest Exceptions on Twitter," https://help.twitter.com/en/rules-and-policies/public-interest.

259 Courtney Subramanian, "A Minute-by-Minute Timeline of Trump's Day as the Capitol Siege Unfolded on Jan. 6," *USA Today*, February 11, 2021, https://www.usatoday.com/story/news/politics/2021/02/11/trump-impeachment-trial-timeline-trump-actions-during-capitol-riot/6720727002/.

260 Kate Conger, "Jack Dorsey Says Twitter Played a Role in U.S. Capitol Riot," *New York Times*, March 25, 2021, https://www.nytimes.com/2021/03/25/business/jack-dorsey-twitter-capitol-riot.html.

261 Daniel Dale, "Fact Check: 11 False Claims Rep. Marjorie Taylor Greene Has Tweeted in the Past Month," CNN, January 21, 2021, https://www.cnn.com/2021/01/21/politics/fact-check-marjorie-taylor-greene-twitter-election-capitol/index.html.

262 "YouTube Regrets," Mozilla Foundation, July 2021, https://foundation.mozilla.org/en/campaigns/regrets-reporter/findings/.

263 Casey Newton, "How YouTube Failed the 2020 Election Test," *The Verge*, March 4, 2021, https://www.theverge.com/2021/3/4/22313213/youtube-2020-election-misinformation-report-long-fuse.

264 Aaron Sankin, "YouTube Said It Was Getting Serious About Hate Speech. Why Is It Still Full of Extremists?," *Gizmodo*, July 25, 2019, https://gizmodo.com/youtube-said-it-was-getting-serious-about-hate-speech-1836596239.

265 "YouTube Regrets," Mozilla Foundation, July 2021, https://foundation.mozilla.org/en/campaigns/regrets-reporter/findings/.

266 "YouTube Regrets," Mozilla Foundation, July 2021, https://foundation.mozilla.org/en/campaigns/regrets-reporter/findings/.

267 "YouTube Regrets," Mozilla Foundation, July 2021, https://foundation.mozilla.org/en/campaigns/regrets-reporter/findings/.

268 Tripp Mickle, "Trump Is Still Banned on YouTube. Now the Clock Is Ticking.," *Wall Street Journal*, May 6, 2021, https://www.wsj.com/articles/trump-is-still-banned-on-youtube-that-could-change-11620293402.

269 Katie Canales, "YouTube Says Videos That Violate Its Policies Will Now Receive a 'Strike.' Channels That Receive 3 Strikes in a 90-Day Period Will Be Permanently Removed," *Business Insider*, January 7, 2021, https://www.businessinsider.com/youtube-three-strikes-permanently-delete-channels-policy-violations-trump-capitol-2021-1.

270 *See* Section 2 "Federal Voter Intimidation & False Election Speech Laws"; *see also* 52 U.S.C. § 10307(b); 52 U.S.C. § 10101(b); *United States v. North Carolina Republican Party*, 5:92-cv-00161 (E.D.N.C. 1992).

271 Nicole Hong, "Twitter Troll Tricked 4,900 Democrats in Vote-by-Phone Scheme, U.S. Says," *New York Times*, January 27, 2021, https://www.nytimes.com/2021/01/27/nyregion/douglass-mackey-arrested-far-right-twitter.html.

272 S. 1840, Deceptive Practices and Voter Intimidation Prevention Act of 2021, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1840/text.

273 S. 2747, Freedom to Vote Act, 117th Cong. (2021), Sec. 3201-3206, "Deceptive Practices and Voter Intimidation Prevention Act of 2021," https://www.congress.gov/bill/117th-congress/senate-bill/2747/text.

274 S. 1, For the People Act, 117th Cong. (2021), Sec. 1301-1304, "Prohibiting Deceptive Practices and Preventing Voter Intimidation," https://www.congress.gov/bill/117th-congress/senate-bill/1/text.

275 S. 1840, Deceptive Practices and Voter Intimidation Prevention Act of 2021, 117th Cong. (2021), Sec. 3, "Prohibition on Deceptive Practices in Federal Elections," https://www.congress.gov/bill/117th-congress/senate-bill/1840/text.

276 S. 1840, Deceptive Practices and Voter Intimidation Prevention Act of 2021, 117th Cong. (2021), Sec. 3, "Prohibition on Deceptive Practices in Federal Elections," https://www.congress.gov/bill/117th-congress/senate-bill/1840/text.

277 S. 1840, Deceptive Practices and Voter Intimidation Prevention Act of 2021, 117th Cong. (2021), Sec. 4, "Corrective Action," https://www.congress.gov/bill/117th-congress/senate-bill/1840/text.

278 S. 1840, Deceptive Practices and Voter Intimidation Prevention Act of 2021, 117th Cong. (2021), https://www.congress.gov/

bill/117th-congress/senate-bill/1840/text.

279 Va. Code Ann. § 24.2-1005.1(A).

280 Amendment to Rules Comm. Print 117-13, Offered by Congressman Brad Sherman (CA-30), September 14, 2021, https://amendments-rules.house.gov/amendments/SHERMA_056_xml%20(Revised%20NDAA%20Amendment%20746)210917132434404.pdf.

281 S. 443, Democracy Is Strengthened by Casting Light On Spending in Elections (DISCLOSE) Act of 2021, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/443/text.

282 S. 1356, Honest Ads Act, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/1356/text.

283 S. 2747, Freedom to Vote Act, 117th Cong. (2021), Sec. 6001-6022, "DISCLOSE Act" and Sec. 6101-6110 "Honest Ads Act," https://www.congress.gov/bill/117th-congress/senate-bill/2747/text.

284 S. 1, For the People Act, 117th Cong. (2021), Sec. 4100-4122, "DISCLOSE Act" and Sec. 4201-4210 "Honest Ads Act," https://www.congress.gov/bill/117th-congress/senate-bill/1/text.

285 S. 443, Democracy Is Strengthened by Casting Light on Spending in Elections (DISCLOSE) Act of 2021, 117th Cong., Sec. 202-203, https://www.congress.gov/bill/117th-congress/senate-bill/443/text.

286 S. 443, Democracy Is Strengthened by Casting Light on Spending in Elections (DISCLOSE) Act of 2021, 117th Cong. (2021), Sec. 303, https://www.congress.gov/bill/117th-congress/senate-bill/443/text.

287 Honest Ads Act, S. 1356, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/1356/text.

288 Honest Ads Act, S. 1356, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/1356/text.

289 Federal Election Commission, "Legislative Recommendations of the Federal Election Commission 2021," Adopted May 6, 2021, https://www.fec.gov/resources/cms-content/documents/legrec2021.pdf.

290 H.R. 1272, Restoring Integrity to America's Elections Act, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/1272/text.

291 H.R. 1, For the People Act, 117th Cong. (2021), Sec. 6001-6011, "Restoring Integrity to America's Elections," https://www.congress.gov/bill/117th-congress/house-bill/1/text.

292 S. 2747, Freedom to Vote Act, 117th Cong. (2021), Sec. 7101-7110, "Restoring Integrity to America's Elections," https://www.congress.gov/bill/117th-congress/senate-bill/2747/text.

293 *See* Alaska Stat. §§ 15.13.400(13), 15.13.040(j).

294 *See* Cal. Gov. Code § 84222.

295 *See* Cal. Assembly Bill 2188, signed September 26, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB2188.

296 *See* NY Elec. Law §§ 14-107(2), 14-107(5-a), 14-106(4) and 14-107-b.

297 *See* Wash. Rev. Code § 42.17A.320; Wash. Admin. Code §§ 390-18-030 and 390-18-050.

298 Media Literacy Toolkit, PEN America, December 21, 2020, https://pen.org/media-literacy-toolkit/.

299 Eric McNeill, "Media Literacy Now launches next phase of media literacy campaign with model bill and new national coalition partners," Media Literacy Now, January 2, 2017, https://medialiteracynow.org/media-literacy-now-launches-next-phase-of-media-literacy-campaign-with-model-bill-and-new-national-coalition-partners/.

300 N.Y. Assembly Bill 6042.

301 N.Y. Assembly Bill 6042.

302 Katherine J. Wu, "Radical Ideas Spread through Social Media. Are the Algorithms to Blame?" *PBS*, March 28, 2019, https://www.pbs.org/wgbh/nova/article/radical-ideas-social-media-algorithms/.

303 Sheera Frenkel, "How Misinformation 'Superspreaders' Seed False Election Theories," *New York Times*, November 23, 2020, https://www.nytimes.com/2020/11/23/technology/election-misinformation-facebook-twitter.html.

304 S. 1896, Algorithmic Justice and Online Transparency Act, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1896/text; H.R. 3611, Algorithmic Justice and Online Platform Transparency Act, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/3611/text?r=2&s=1.

305 S. 1896, Algorithmic Justice and Online Transparency Act, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1896/text; H.R. 3611, Algorithmic Justice and Online Platform Transparency Act, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/3611/text?r=2&s=1.

306 Channel 4 News Investigations Team, "Revealed: Trump Campaign Strategy to Deter Millions of Black Americans from Voting in 2016," Channel 4, September 28, 2020, https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016.

307 "The Leadership Conference on Civil and Human Rights Transition Priorities," Leadership Conference on Civil and Human Rights, November 24, 2020, http://civilrightsdocs.info/pdf/policy/task-force-priorities/Transition-TaskForceTopPriorities-The%20Leadership%20Conference-November2020-FINAL.pdf.

308 "Letter from Common Cause, Free Press and PEN America to Congress," April 8, 2020, https://www.commoncause.org/press-release/congress-must-include-local-news-funding-in-next-covid-19-stimulus/.

309 Yosef Getachew and Jonathan Walter, "Restore Local Journalism with US Funding, Oversight Promoting Inclusiveness," *The Press of Atlantic City*, May 19, 2021, https://pressofatlanticcity.com/opinion/columnists/restore-local-journalism-with-us-funding-oversight-promoting-inclusiveness-by-yosef-getachew-and-jonathan-walter/article_602f794e-b416-11eb-ae1d-2f96f242750e.html.

310 Senator Brian Schatz, "Schatz, Veasey, Bennet, Klobuchar Reintroduce Legislation to Bolster Local Journalism," news release, May 13, 2021, https://www.schatz.senate.gov/news/press-releases/schatz-veasey-bennet-klobuchar-reintroduce-legislation-to-bolster-local-journalism.

311 "The Disinformation Black Box: Researching Social Media Data," Hearing Before the Subcomm. on Investigations and Oversight of the H. Comm. on Science, Space, and Technology, 117th Cong. (2021) (testimony of Laura Edelson, NYU Cybersecurity for Democracy).

312 H.R. 3451, Social Media DATA Act, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/3451/text?r=1&s=1.

313 Vivek H. Murthy, "Confronting Health Misinformation: The U.S. Surgeon General's Advisory on Building a Healthy Information Environment," 2021, https://www.hhs.gov/sites/default/files/surgeon-general-misinformation-advisory.pdf.

314 Vivek H. Murthy, "Confronting Health Misinformation: The U.S. Surgeon General's Advisory on

315 Building a Healthy Information Environment," 2021, https://www.hhs.gov/sites/default/files/surgeon-general-misinformation-advisory.pdf.

316 "Letter from Public Interest Groups to White House," April 29, 2021, https://pen.org/letter-white-house-must-establish-disinformation-defense-and-free-expression-task-force/.

317 "Letter from Public Interest Groups to White House," April 29, 2021, https://pen.org/letter-white-house-must-establish-disinformation-defense-and-free-expression-task-force/.

318 *See, e.g., United States v. North Carolina Republican Party*, 5:92-cv-00161 (E.D.N.C. 1992) (DOJ lawsuit against the North Carolina Republican Party, which had mailed disinformation postcards to 125,000 Black voters throughout the state incorrectly stating that recipients could not vote if they had moved within 30 days of the election and also threatening criminal prosecution).

319 *U.S. v. Douglas Mackey*, Complaint 1 (E.D.N.Y. January 22, 2021), https://www.justice.gov/opa/press-release/file/1360816/download.

320 Nicole Hong, "Twitter Troll Tricked 4,900 Democrats in Vote-by-Phone Scheme, U.S. Says," *New York Times*, January 27, 2021, https://www.nytimes.com/2021/01/27/nyregion/douglass-mackey-arrested-far-right-twitter.html.

321 Letter from Senate Democrats to Lina Khan, Chair, Federal Trade Commission, September 20, 2021, https://www.blumenthal.senate.gov/imo/media/doc/2021.09.20%20-%20FTC%20-%20Privacy%20Rulemaking.pdf.

322 Letter from Public Interest Groups to Lina Khan, Chair, Federal Trade Commission, August 4, 2021, https://www.publicknowledge.org/documents/public-interest-group-ftc-privacy-letter/.

323 Letter from Senate Democrats to Lina Khan, Chair, Federal Trade Commission, September 20, 2021, https://www.blumenthal.senate.gov/imo/media/doc/2021.09.20%20-%20FTC%20-%20Privacy%20Rulemaking.pdf; Letter from Public Interest Groups to Lina Khan, Chair, Federal Trade Commission, August 4, 2021, https://www.publicknowledge.org/documents/public-interest-group-ftc-privacy-letter/.

324 Federal Election Commission, "Advance Notice of Proposed Rulemaking: Internet Communication Disclaimers," 76 Fed. Reg. 63567, October 13, 2011.

325 Common Cause, Comments in Response to FEC Notice of Proposed Rulemaking 2018-06, May 24, 2018, https://www.commoncause.org/wp-content/uploads/2018/05/CC-Comments_NPRM-2018-06-Internet-Disclaimers_FINAL-5.24.18.pdf.

326 Jesse Littlewood and Emma Steiner, "Trending in the Wrong Direction: Social Media Platforms' Declining Enforcement of Voting Disinformation," Common Cause, September 2, 2021, https://www.commoncause.org/wp-content/uploads/2021/09/Disinfo_WhitePaperv3.pdf.

327 Craig Silverman and Ryan Mac, "Facebook Promised to Label Political Ads, But Ads for Biden, the Daily Wire, and Interest Groups Are Slipping Through," *BuzzFeed News*, October 22, 2020, https://www.buzzfeednews.com/article/craigsilverman/facebook-biden-election-ads.

328 Jeremy B. Merrill and Jamiles Lartey, "Trump's Crime and Carnage Ad Blitz Is Going Unanswered on Facebook," The Marshall Project, September 23, 2020, https://www.themarshallproject.org/2020/09/23/trump-s-crime-and-carnage-ad-blitz-is-going-unanswered-on-facebook.

329 Keach Hagey and Jeff Horwitz, "Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead," *Wall Street Journal*, September 15, 2021, https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215?mod=article_inline.

330 Jeff Horwitz, "Facebook Says Its Rules Apply to All. Company Documents Reveal a Secret Elite That's Exempt.," *Wall Street Journal*, September 13, 2021, https://www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353?mod=article_inline.

331 Common Cause, "Facebook Shutdown of NYU Ad Observatory Project Researchers Undermines Democracy," news release, August 4, 2021, https://www.commoncause.org/press-release/facebook-shutdown-of-nyu-ad-observatory-project-researchers-undermines-democracy/.

332 Kari Paul, "Facebook Has a Blind Spot': Why Spanish-Language Misinformation Is Flourishing," *The Guardian*, March 3, 2021, https://www.theguardian.com/technology/2021/mar/03/facebook-spanish-language-misinformation-covid-19-election.

333 Ariz. Rev. Stat. § 16-1013.

334 Ariz. Rev. Stat. § 16-1012.

335 Ariz. Rev. Stat. § 16-515.

336 Other states offering candidate pledges related to false statements include Arkansas (Ark. Code § 7-6-102), Illinois (10 ILCS § 5/29B-10), Maine (Me. Stat. tit. 21-A, § 1101 et seq.), Minnesota (Minn. Stat. § 211B), Nevada (Nev. Rev. Stat. § 294A.290), and Texas (Tex. Elec. Code § 255.004-06).

337 Cal. Elec. Code § 20440.

338 Colo. Rev. Stat. § 1-13-713.

339 Colo. Rev. Stat. § 1-13-109.

340 Colorado Attorney General Phil Weiser, "Public Advisory on Voter Intimidation Crimes and Poll Security," October 19, 2020, https://coag.gov/app/uploads/2020/10/Public-Advisory-Voter-Intimidation-10.19.2020.pdf.

341 Fla. Stat. § 104.0615(2).

342 Fla. Stat. § 104.0615(3).

343 Ga. Code Ann. § 21-2-566(4).

344 Ga. Code Ann. § 21-2-567(a).

345 Haw. Rev. Stat. § 19-3(12).

346 Haw. Rev. Stat. § 19-3(4).

347 Haw. Rev. Stat. § 11-132(5).

348 Me. Stat. tit. 21, § 674(1)(B).

349 Me. Stat. tit. 21, § 674(3)(A).

350 Md. Code, Com. Law § 16-201(a)(5)-(6).

351 Md. Code, Com. Law § 16-201(a)(7).

352 Mich. Elec. Laws § 168.932(a).

353 Mich. Elec. Laws § 168.931(3).

354 Minn. Stat. § 211B.07.

355 Minn. Stat. § 211B.07.

356 Nev. Rev. Stat. § 293.710(1)(d).

357 Nev. Rev. Stat. § 293.710(1)(a)-(b).

358 N.M. Stat. § 1-20-14.

359 New Mexico Secretary of State Maggie Toulouse Oliver, "Guidance on Voter Intimidation and Discriminatory Conduct," https://www.sos.state.nm.us/voting-and-elections/voter-information-portal/guidance-on-voter-intimidation-and-discriminatory-conduct/.

360 N.C. Gen. Stat. § 163-274(7).

361 25 Pa. Cons. Stat. § 1711.

362 Pa. Department of State, "Guidance on Voter Intimidation and Discriminatory Conduct," October 2020, https://www.dos.pa.gov/VotingElections/OtherServicesEvents/Documents/DOS%20Voter%20Intimidation%20Guidance%2010.14.16.pdf.

363 Va. Code Ann. §§ 24.2-607 and 24.2-1005.

364 Va. Code Ann. § 24.2-1002.

365 Va. Code Ann. § 24.2-1005.1(A).

366 Va. Code Ann. § 24.2-1005.1(C).

367 Wis. Stat. § 12.09.

368 Wis. Stat. § 12.05.

369 Alaska applies disclosure requirements to "nongroup entities," defined to mean "a person, other than an individual, that takes action the major purpose of which is to influence the outcome of an election" and that "cannot participate in business activities," "does not have shareholders who have a claim on corporate earnings" and is "independent from the influence of business corporations." Alaska Stat. § 15.13.400(13).

370 Alaska Stat. § 15.13.040(j).

371 Cal. Gov. Code § 84222.

372 Cal. Assembly Bill 2188, signed September 26, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB2188.

373 Md. Code, Elec. Law § 13-309.2.

374 Minn. Stat. Ann. § 10A.27 Subd.15(b).

375 NY Elec. Law §§ 14-107(2), 14-107(5-a) and 14-107-b.

376 NY Elec. Law § 14-106(4).

377 17 R.I. Gen. Laws § 17-25.3-1.

378 Wash. Rev. Code § 42.17A.320.

379 Wash. Admin. Code § 390-18-030.

380 Wash. Admin. Code § 390-18-050.

381 "U.S. Media Literacy Policy Report 2020," Media Literacy Now, January 2020, https://medialiteracynow.org/wp-content/uploads/2020/01/U.S.-Media-Literacy-Policy-Report-2020.pdf.

382 Media Literacy Advisory Committee, "Media Literacy Advisory Committee Report," Colorado Department of Education, December 2019, https://www.cde.state.co.us/cdedepcom/medialiteracyadvisorycommitteereport.

383 "U.S. Media Literacy Policy Report 2020," Media Literacy Now, January 2020, https://medialiteracynow.org/wp-content/uploads/2020/01/U.S.-Media-Literacy-Policy-Report-2020.pdf.

384 Peter Medlin, "Illinois State Law is the First to Have High Schools Teach News Literacy," *NPR*, August 12, 2021, https://www.npr.org/2021/08/12/1026993142/illinois-is-the-first-state-to-have-high-schools-teach-news-literacy.

385 "U.S. Media Literacy Policy Report 2020," Media Literacy Now, January 2020, https://medialiteracynow.org/wp-content/uploads/2020/01/U.S.-Media-Literacy-Policy-Report-2020.pdf.

386 "U.S. Media Literacy Policy Report 2020," Media Literacy Now, January 2020, https://medialiteracynow.org/wp-content/uploads/2020/01/U.S.-Media-Literacy-Policy-Report-2020.pdf.

Education Fund

805 15th Street, NW, Suite 800
Washington, DC 20005
202.833.1200
commoncause.org/education-fund/