Principles and Policies to Counter Deceptive Digital Politics

Ann M. Ravel (MapLight), Samuel C. Woolley (Institute for the Future), and Hamsini Sridharan (MapLight)

MapLight

INSTITUTE FOR THE FUTURE

About MapLight

MapLight is a nonpartisan 501(c)(3) nonprofit that seeks to achieve a government that (actually) works for the people. We illuminate the influence of money in politics, facilitate informed voting and civic engagement, and advance reforms that make government more responsive to the people. Our database, online tools, research, and policy work help to expose and counter the hidden influences on our democracy. MapLight is based in Berkeley, California.

About Institute for the Future

Institute for the Future is the world's leading futures thinking organization. For over 50 years, businesses, governments, and social impact organizations have depended upon IFTF global forecasts, custom research, and foresight training to navigate complex change and develop world-ready strategies. IFTF methodologies and toolsets yield coherent views of transformative possibilities across all sectors that together support a more sustainable future. Institute for the Future is a registered 501(c)(3) nonprofit organization based in Palo Alto, California.

The IFTF Digital Intelligence Laboratory is a social scientific research entity conducting work on the most pressing issues at the intersection of technology and society. We examine how new technologies and media can be used to both benefit and challenge democratic communication.

About the Authors

Ann M. Ravel is the Digital Deception Project Director at MapLight, where she leads the development and promotion of policies that tackle online political manipulation. She served on the Federal Election Commission from 2013 to 2017, holding the roles of chair and vice chair. Ann previously chaired the California Fair Political Practices Commission, acted as Deputy Assistant Attorney General for the U.S. Department of Justice, and served as Santa Clara County Counsel for over a decade. In 2014, she was named a California Attorney of the Year by California Lawyer magazine, and in 2007, the State Bar of California named her Public Attorney of the Year.

Samuel C. Woolley is the Research Director of the IFTF DigIntel Lab, where he leads cutting-edge social science research. He is one of the foremost experts in the study of automation and artificial intelligence, political communication, and information warfare. Sam is the co-founder and former director of the Computational Propaganda research team at the University of Oxford and the University of Washington. He has conducted foundational research on the topics of online disinformation and political manipulation, coining the terms "computational propaganda" and "political bot."

Hamsini Sridharan is the Program Director at MapLight, leading the organization's work to research and promote policies that reform the political process, from money in politics to digital deception. She has previously worked with nonprofits focusing on fair trade and financial transparency.

Acknowledgments

The authors gratefully acknowledge the Bright Horizon Fund and the Open Society Foundations, whose support made this project possible. Thanks also to Daniel G. Newman and Alec Saslow at MapLight and Katie Joseff and the communications team at IFTF for editing and communications help. Finally, thanks to Heather Caviston for sharing her design skills with us.

TABLE OF CONTENTS

INTRODUCTION

The rise of online political manipulation first attracted widespread public attention in the United States with the scandal of extensive Russian interference in the 2016 presidential election. As the 2018 midterms demonstrated, the problem remains endemic in U.S. politics, with manipulative behavior by foreign agents from Iran and Russia as well as domestic campaigns and conspiracy theory networks.[1, 2, 3] Since the 2016 election, research has illuminated the contours of the digital deception problem, and government and technology companies have taken cursory steps toward addressing it. Overall, however, their response has been inadequate. Policy solutions have been in especially short supply.

What is deceptive digital politics? In the U.S. and around the world, the online political ecosystem has been colonized by "computational propaganda": political bots, troll farms, fake social media accounts, networks of disinformation websites, and other methods that—in addition to paid digital advertising—seek to manufacture consensus and manipulate public opinion around political events.[4] With increasingly sophisticated uses of consumer and voter data, these tools can narrowly target particular geographic areas, social groups, and even specific individuals, creating a divisive information environment and making it difficult to identify (much less counter) this harmful political activity. When we refer to "digital deception," we mean the collection of opaque digital political advertising, malicious computational propaganda, and rampant disinformation spread by domestic and foreign actors that is destabilizing American democracy. The results can be seen in skewed voting results and voter suppression efforts targeting politically marginalized communities, increased divisiveness in political discourse, and diminished trust in democratic institutions.

This report was written to facilitate the development of concrete, achievable solutions to digital deception in politics. Above and beyond solutions from technology companies, interventions by government and civil society are desperately needed to meaningfully address the problem. These must be grounded in democratic principles. We propose a framework of six principles—transparency, accountability, standards, coordination, adaptability, and inclusivity—that can serve as an evergreen tool for evaluating policy proposals, when backed by empirical social science and computer science research (see Table 1).

Building from this framework, we discuss 34 policy proposals that target specific aspects of deceptive digital politics. These proposals (summarized in Table 2) include both immediate actions that can be taken by government, technology companies, and civil society and necessary long-term systemic changes. To date, little work on digital deception has focused on policy-driven approaches that tackle the entirety of this complex problem. Responses to digital threats have been purely defensive and reactive. Our approach integrates the best thinking from multiple disciplines and is based on the recognition that all of society must be involved in responding comprehensively and systematically to these problems. To this end, this paper leverages a number of policy areas, tactics, and tools.

This policy "platform" is a starting point for deliberation, not a definitive set of proposals. As new developments emerge, it will be critical to continually re-evaluate specific approaches—while holding firm to underlying democratic principles.

PRINCIPLE	FUNCTION
Transparency	Ensures that people know who is seeking to influence them and how, so they can make informed political decisions.
Accountability	Establishes measures of answerability and enforcement for technology companies and political actors, putting control back into the hands of the people.
Standards	Sets high thresholds for the public interest that technology companies and other digital political actors, such as campaigns, must meet and promotes consistency in policy implementation across actors and jurisdictions.
Coordination	Increases cooperation and knowledge-sharing between and across technology companies and government agencies in the U.S. and globally, enabling the efficient detection of threats and enforcement of laws.
Adaptability	Emphasizes regulatory flexibility in response to a dynamic problem and rapidly evolving technologies.
Inclusivity	Brings civil society expertise to the table, including technical experts and the voices of the issue publics and social groups that are most harmed by deceptive digital politics.

Table 1: Principles to Protect Democracy

	POLICY AREA	PROPOSALS
Immediate Policy Proposals	***Campaign Finance***	1. Pass the Honest Ads Act 2. Expand and extend "electioneering communications" rules to cover online ads 3. Increase disclosure requirements for paid issue ads 4. Require political committees to disclose spending by subvendors 5. Adapt on-ad "paid for by" disclaimers for digital context 6. Create independent government authority to investigate financial flows in digital politics and enforce the law 7. Eliminate dark money in politics
	Data Usage and Privacy	8. Codify the Consumer Privacy Bill of Rights 9. Ensure data usage policies are truly accessible to users 10. Include all audience targeting information in on-ad disclaimers 11. Evaluate ad targeting options from a civil rights perspective 12. Educate the public about their data rights 13. Demonetize bad actors' revenue streams
	Automated and Fake Accounts	14. Require disclosure of automated accounts 15. Remove bots and fake accounts from follower counts, recommendation engines, and popularity-based algorithms 16. Require tech companies to disclose numbers of bots and fake accounts 17. Treat posts by bots as "public communications" per campaign finance law
	Platform Liability	18. Revise the Communications Decency Act so that platforms can be held accountable for disinformation tactics
	Multisector Infrastructure	19. Reinstate the Office of Technology Assessment 20. Reinstate a cybersecurity policy lead in the executive branch 21. Establish an agency, initiative, or task force to coordinate between federal agencies and technology companies
Systemic Changes	***Global Cooperation***	22. Establish a global cybersecurity accord 23. Share information openly between allies 24. Learn from policy models around the world 25. Promote democratic responses to digital deception around the world
	Research and Development	26. Require platforms to share data openly with third-party researchers 27. Develop better tools for detecting disinformation and bots 28. Incorporate civil rights perspective into product development 29. Invest in ethical technology design
	Media and Civic Education	30. Conduct multisector media literacy initiatives 31. Build media literacy and civics emphasis into public education 32. Support local newsrooms
	Competition	33. Review mergers and acquisitions more stringently 34. Investigate and enforce penalties for anti-competitive behavior by platforms

Table 2: Policy Proposals to Counter Deceptive Digital Politics

SIX PRINCIPLES TO PROTECT DEMOCRACY

Two features of the digital environment make deceptive digital politics especially harmful: anonymity and automation. The ease of online anonymity enables political actors to post misleading messages from false or obscured identities, eliminating important audience cues about the credibility of the speaker. Meanwhile, automation makes it possible for propaganda and disinformation to be amplified in ways that drown out the truth. Malicious actors exploit these features to drive wedges into American democracy, deceiving voters, exacerbating political polarization, and destabilizing trust in institutions such as government and the press. Solutions must be grounded in democratic principles in order to safeguard against self-interested and shortsighted interventions that further undermine our political processes.

The following framework is a rubric for developing and evaluating policies that tackle digital deception in politics. The principles we discuss are essential to a democracy that is resilient in the face of the challenges of online anonymity and automation. Transparency and accountability are basic tenets of democracy, while standards, coordination, adaptability, and inclusivity offer commonsense, efficacious means of achieving those ideals.

Transparency

Online anonymity combines with gaps in campaign finance disclosure laws and opaque "privacy" policies to produce a system in which technology companies and political actors have extensive and precise knowledge about individuals—but people don't know who is trying to influence them. It's like a one-way mirror: they can see the public, but the public cannot see them. Bringing greater transparency to deceptive digital politics is a necessary—and eminently achievable—first step toward restoring the balance of power.

In 1914, just before joining the Supreme Court, Justice Louis Brandeis 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."[5] Transparency is a long-held, widely accepted value in our democracy, making it a simple starting point for tackling digital deception. The public has a right to know who is attempting to influence their votes; transparency provides invaluable informational benefits to voters by offering them a heuristic for evaluating political messages. Transparency also deters corruption and enables enforcement of laws and regulations—the reasoning behind the Supreme Court's longstanding support of campaign finance disclosure.[6] Without transparency, there is little chance of meaningful political accountability by journalists, government watchdogs, and voters.

Digital political information must be disclosed to government and the public. True transparency entails making it easy for journalists and researchers to analyze information—and putting that information in the hands of the people in ways they can understand and use. Burying information in arcane databases and legalese-riddled terms of service is neither transparent nor useful to the public. Only by shining light on digital campaign finance, data usage by technology companies, and algorithmic opacity can we ensure that the public is informed and empowered to participate in democracy.

Accountability

Accountability is a central aspect of democratic self-government; public institutions and leaders must answer to the people so that the self-interest of representatives cannot dominate the public interest. To achieve accountability, information needs to be transparent to government agencies and watchdogs (including journalists and researchers, as well as the public more broadly), and there must be enforceable consequences for violating the public trust. Greater accountability is sorely needed in the digital realm.

Our political system has become more heavily influenced by digital technologies, but laws and regulations haven't followed this shift. As a result, self-interested technology companies and political actors wield considerable influence within our democracy, largely unchecked. Given their growing role in political life, technology companies need to be held accountable to the public interest via governmental mechanisms—which in turn must be accountable to the people. The tech sector's current efforts are voluntary and can be quietly withdrawn or weakened whenever it serves business interests to do so. Systems must also be put in place to identify and hold political actors accountable for malicious digital activities that manipulate public opinion.

Instead of leaving private actors—including technology companies and deceptive digital operatives—to their own devices, laws and regulations must be created and equitably enforced to ensure that their activities align with the public interest. Only by doing so can we put democracy back in the hands of the people.

Standards

In order to achieve meaningful transparency and accountability, the government needs to establish performance standards for technology companies and political actors. Only by doing so can we ensure that the public interest is being met and that all actors are consistently following the same rules.

Technology companies have thus far enjoyed an open, unconstrained regulatory environment. Their election security efforts show that public pressure and the threat of regulation can motivate these companies to react to digital deception—but only to a limited extent. This self-regulation isn't enough. Without government oversight, social media firms have produced systems for advertising transparency, data usage, content moderation, and so on that vary greatly and do only the bare minimum to serve the public interest. Only the most visible companies, such as Google, Facebook, and Twitter, have taken action at all. Governments have the power to require companies to disclose information—about political ad audience targeting, for example—that goes above and beyond what companies and advertisers are inclined to share on their own.

The federal government remains mired in debates about whether and how to act, but states and cities have begun to take matters into their own hands. This creates opportunities for policy experimentation and, realistically, more immediate action. Nonetheless, it is crucial that federal standards are developed to ensure that the public's needs are consistently met.

By establishing high standards for what is in the public interest and insisting that companies comply, government can guide the technology sector in a direction that better serves democracy.

Coordination

Thus far, efforts to address digital deception have been piecemeal and reactive rather than strategic and comprehensive. Technology companies and government agencies must instead cooperate within and across the public and private sectors—and globally—to share information about threats and craft comprehensive and effective responses.

Major technology companies and government agencies have engaged in a hodgepodge of public hearings and investigations meant to address deceptive digital politics—but these have all been on an ad hoc basis and focused on fragments of the problem, with little strategic coordination.[7] Deceptive digital operations often span multiple platforms and cannot be addressed by any one company. Instead, the industry must coordinate to share information and align policies to counteract multi-platform attacks. This already happens to some extent; in August 2018, representatives from several major platforms gathered in San Francisco to strategize in advance of the midterms, following a similar meeting in May.[8] However, such coordination has not been formalized.

Meanwhile, multiple agencies within the federal government—including Congress, the FEC, the FTC, intelligence agencies, and more, have nipped at aspects of this problem, but there is no single body tasked with organizing them.[9] This decentralized structure also hampers coordination with the private sector, except on an ad hoc, reactive basis.

Moreover, the impact of deceptive digital politics is not limited to the United States. Domestic and foreign computational propaganda has been deployed in elections around the world.[10] However, thus far, there has been little formal international coordination.

The result of this lack of coordination between companies, government agencies, and countries is insufficient information sharing and strategic planning for tackling this complex problem. Deceptive digital political actors seek out the interstices and loopholes of law and policy—the gaps created by this lack of cooperation. Without adequate infrastructure and knowledge sharing, democratic institutions will remain vulnerable to manipulation, and responses will be reactive rather than proactive.

Adaptability

Technology and the problems of digital deception are evolving quickly, but laws and regulations have not kept pace with the rate of change. There is a danger of creating policies that are out of touch with new developments, too broad or too narrow, or instantly obsolete.[11] This, however, is not a reason to avoid regulation; rather, it means government must craft policies that allow for flexibility as technology changes.

The dilemmas of applying law to new technologies are readily visible in the circumstances of deceptive digital politics. It has often been remarked—including by Facebook CEO Mark Zuckerberg—that we are in an "arms race" against manipulative actors, who continuously seek out new loopholes and exploit emerging technologies.[12] For example, when Facebook detected 32 likely Russian-operated profiles and pages engaged in political manipulation in July 2018, they noted that operatives had learned from the ways they were previously detected, using VPNs and internet phone services to cover their tracks and paying third parties to run ads for them.[13] New fronts in the battle for digital integrity will include the predicted rise of deepfake audio, video, and images

as well as other new technologies that will be manipulated in as yet-unforeseen ways. In dealing with deceptive digital politics, we confront opponents that are evolving and adapting based on our responses to them.

Strategies for building adaptability into policy include:

- Crafting flexible policies that leave the specifics of implementation up to technology companies, while mandating standards that need to be met.
- Requiring regular reviews of laws to respond to new developments in the field, such as advances in artificial intelligence and its use in faking images and videos.
- Charging a particular government agency or multisector task force with staying up to date on the latest developments in deceptive digital politics, in order to avoid being repeatedly caught off guard.
- Setting regulatory requirements based on the size of a platform's user base, such that small startups do not need to face the same regulations as giants such as Facebook and Google.

Inclusivity

We must call upon diverse perspectives and knowledge bases to address deceptive digital politics. Without the voices of civil society, action by governments and technology companies is likely to be insufficient or lead to unintended consequences.

These voices must include experts from a variety of disciplines, such as public interest technologists, social science researchers, and legal and policy scholars. Responses to deceptive digital threats need to be multidisciplinary as well as multisectoral and informed by critical debate, theory, and empirical evidence.

However, the civil society response must also go beyond the technical and academic realms to incorporate the experiences of those affected directly by digital deception. We must pay attention to the perspectives of politically marginalized communities, including women, people of color, immigrants, and others who are frequently the target of deceptive digital campaigns. For example, Russian propaganda in the 2016 and 2018 elections deliberately focused on infiltrating online communities of black or Latinx activists to suppress the votes of these communities and inflame political tensions around issues of racial justice in the broader online sphere.[14] We need to ensure that these groups' voices are represented in the policymaking process in order to enshrine equal protection from harm by any policies put in place and ascertain and prevent harmful unintended consequences. Facebook's May 2018 decision to submit to a third-party civil rights audit, which was the result of months of advocacy by groups such as the Center for Media Justice, Color of Change, Muslim Advocates, the NAACP Legal Defense Fund, and others, was a positive step in this direction.[15]

Bringing together the voices of experts in academia and think tanks with those of advocacy groups representing marginalized communities will ensure that solutions to digital deception truly serve the interests of the people.

APPLYING THE FRAMEWORK

The six principles outlined above lay the framework for action to defend democracy via democratic means. These principles should guide all policy proposals for addressing deceptive digital politics. Government and civil society must apply these principles to bring technology companies in line with the interests of a democratic system.

The market-based approach has failed. Eight-five percent of Americans think social media firms should be doing more to combat disinformation, but while companies have taken some measures to address this problem over the past two years, their efforts have been patchy, incomplete, and inconsistent—at best.[16] At worst, responses from leadership at companies like Facebook have exacerbated conspiracy theories and disinformation campaigns.[17] The private sector possesses technical expertise and capacity to implement solutions and is less likely to be hampered by the sweeping interpretations of free speech that federal courts currently use to constrain government. However, companies rely on capturing user attention and pursue the public interest only insofar as it aligns with their bottom line.[18]

Beyond this, technology companies have relied too heavily on "technological solutionism": the idea that simply by building more sophisticated, efficient digital tools, we can solve complex social and political problems.[19] For instance, Facebook leadership has put a fervent public emphasis on advancing artificial intelligence to detect problem behavior on its platforms.[20] Technology firms suggest black box solutions for problems that are human as well as technological, proposing to fight automation with more automation. However, these technologies are not capable of processing the full linguistic and cultural complexity of human expression, leaving them unable to reliably distinguish between false or misleading messages and other types of content.[21] Moreover, the algorithms used to police social media platforms are vulnerable to the biases and fallibility of their producers. Technology companies created the problems on their platforms that they now claim necessitate the use of technologies that haven't yet been realized—asking for trust that they have not earned. Without transparency or accountability to the people via government intervention, these companies cannot be relied on to act in the public interest.

While we work to build such policies, we must also guard against reactive, authoritarian responses to the problem of digital deception. As we have seen around the world, state actors can take advantage of perceived crises to appoint themselves as the arbiters of truth, coopting accusations of "digital disinformation" or "fake news" to discredit political dissent—even as those same regimes deploy the tactics of digital deception to advance propaganda.[22] Without guidance from government and civil society to find the right balance, technology companies could as easily overcorrect and become private censorship bodies. Responses to deceptive digital politics must not further entrench the problem or give fodder for political despots to exert control over the media. Rather, any solution must hew to democratic tenets and be implemented after deliberation over potential consequences.

Digital deception strikes at the heart of our political system and necessitates the involvement of public institutions and civil society to reinstate democratic self-government. Government must step in to enact sensible policies that safeguard democracy, compelling compliance and enforcing penalties for violators. Civil society—including researchers, the media, think tanks, advocacy groups, public interest technologists, and individual members of the public—has a major role to play in influencing government and technology companies to action and ensuring that the policies enacted serve the public interest.

In the following sections, we examine policy proposals and recommend specific interventions that merit discussion and advocacy. These proposals can be evaluated against the rubric established above by asking two sets of questions:

1. **Democratic principles:** Does this measure increase transparency, helping the public know who is seeking to influence them? Does it promote accountability by bringing political actors and technology companies under democratic control?

2. **Effectiveness:** Does it set adequate standards, foster coordination to tackle the complexity of the problem, allow for adaptability, and include all necessary perspectives?

We have subdivided our proposals into two broad categories: immediate policy proposals, which can and should be considered in the short term, and long-term systemic changes, which are necessary but cannot adequately protect our elections within the next election cycle. We are not the first to suggest many of these proposals; other sources have identified various policy subsets that we discuss below, and we ourselves have discussed the campaign finance angle in depth elsewhere. Our hope is that by compiling the most promising options, in keeping with the principles laid out above, this paper can serve as an organized jumping-off point for debate and deliberation, with the goal of achieving both immediate and systemic changes needed to protect our democracy.

IMMEDIATE POLICY PROPOSALS

While deceptive digital politics will certainly require ongoing research to understand completely and solve, it is imperative that we rapidly respond to protect our democracy in time for the pivotal 2020 U.S. presidential election. The federal government, technology companies, and civil society need to mobilize on campaign finance reform, data usage and privacy, automated and fake accounts, platform liability, and multisector infrastructure, tackling the most immediate threats to our democracy.

Campaign Finance

The problems with online political advertising—including discriminatory and manipulative microtargeting, foreign interference, and the overall lack of transparency—can largely be attributed to gaps in campaign finance laws and regulations. Campaign finance may at first glance seem like a narrow framework, but in fact these rules and regulations offer important tools for tackling deceptive digital politics, from paid political ads to supposedly "free" posts made by paid operatives. Closing these gaps and ensuring transparency for all paid political activity would be a considerable improvement and could be achieved quickly and at low cost.

The Federal Election Commission (FEC), Congress, and major technology platforms have all taken cursory steps in this area, but there is much more to be done to truly safeguard democracy. The FEC is currently evaluating proposals for updating its disclaimer requirements for online political ads (which have previously been reviewed on a case-by-case basis).[23] However, the commission moves slowly and is severely limited by partisan deadlock.

Meanwhile, Congress is considering the Honest Ads Act, a bill introduced by Senators Amy Klobuchar (D-Minn.), Mark Warner (D-Va.), and the late John McCain (R-Ariz.).[24] This act would require online platforms with more than 50 million monthly visitors to maintain public records of all political ad purchases over $500, including copies of the ad, descriptions of the target audience, the amount of the purchase, the name of the candidate or office being supported or opposed, and contact information for the purchaser. In addition, it would require platforms to ensure that they are not selling election ads to foreign agents.[25] This would be a marked improvement to the problem of microtargeted "dark ads" and would institute a modicum of accountability for major advertising platforms like Facebook and Google.

Facebook, Twitter, and Google have each introduced purchase verification requirements to prevent foreign entities from buying campaign ads, launched political advertising databases similar to the Honest Ad Act requirements, and added disclaimers to political advertising.[26, 27, 28] However, the platforms haven't provided the same degree of information that government regulation could require. For example, verification requirements are easily gamed by hiring third parties or using front-group names (also a common tactic in dark money spending); in fact, ad buyers can fill in virtually any name to get an ad approved.[29, 30] Moreover, the platforms don't share detailed information about the specific audiences targeted and amounts spent by ad buyers.[31] They all cover election-related ads, but provide variable information about so-called "issue ads," which are just as important in elections. Automated approaches to identifying political ads have resulted in false positives (blocking nonpolitical content) and false negatives (allowing political content to escape labeling).[32]

The federal government has failed to make progress on these issues, but some states and cities are forging ahead with laws similar to the Honest Ads Act. These include Maryland, Washington, New York, and California, as well as Seattle, where an investigation by a reporter at The Stranger uncovered an existing law that requires political advertising disclosure from the technology platforms—a discovery that has sent Facebook to court.[33, 34]

Proposals: (building on Sridharan and Ravel's previous report)[35]

1. Pass the Honest Ads Act mandating that major technology platforms publish political ad files in order to increase transparency for money in digital politics and dark advertising. Ensure that the data provided is standardized across platforms and provides the necessary level of detail regarding target audiences and ad spends. Records should remain publicly available for several years to facilitate enforcement.

2. Expand the definition of "electioneering communications" to include online ads, and extend the window for communications to qualify as "electioneering." Electioneering communications are ads on hot-button issues that air near an election and reference a candidate, but do not explicitly advocate for or against that candidate. Online ads are currently exempted from the disclosure rules for this type of advertising, which apply to TV, radio, and print. However, online ads that satisfy the definition of electioneering communications ought to be regulated. Moreover, with political ads running earlier and earlier each election cycle, it is important to extend the window of time that electioneering regulations apply for online advertising.

3. Increase disclosure requirements for paid issue ads, which frequently implicitly support or oppose candidates and are intended to motivate political action, but receive little oversight. This is one area where the government is hampered by court interpretations of free speech, but where technology companies could successfully intervene with civil society guidance.

4. Increase transparency for the full digital advertising ecosystem by requiring all political committees to disclose spending by subvendors to the FEC. Right now, committees must report payments made to consultants and vendors, but aren't required to disclose payments made by those consultants and vendors for purchases of ads, ad production, voter data, or other items—meaning much digital activity goes unreported. California has a rule that requires political committees to report all payments of $500 or more made by vendors and consultants on their behalf.[36] Similar rules should be adopted at the federal level.

5. Adapt on-ad "paid for by" disclaimer regulations to apply to digital advertising. Digital political ads should be clearly labeled as promoted content and marked with the name of whoever purchased them. They must contain a one-step mechanism, such as a hyperlink or pop-up, for accessing more detailed disclaimer information, including explicit information about whom the ad is targeting. There should be no exceptions to this rule based on the size of ads; unlike with pens or buttons, technology companies can adapt the size of digital ads to meet legal requirements.

6. Create an independent authority that is empowered to investigate the flows of funding in digital political activity. This equivalent to the Financial Industry Regulatory Authority would be charged with following political money to its true sources, making it easier for the FEC to identify violations and illegal activity and enforce penalties.

7. Eliminate dark money in politics. The policies above would improve transparency and accountability in our political system, but so long as dark money goes unchecked, their impact will be limited. Political donors will continue to hide their identities, disclosing only the misleading names of front groups. While congressional and judicial options would ultimately be needed to accomplish this, another avenue might be for technology companies to require ad purchasers to list their true top funders.[37]

Data Usage and Privacy

Access to and usage of data is a key component of deceptive digital politics. Like oil or gold in the analog days, data is the primary resource of the digital economy. Data about voters plays a major role in politics; campaigns and political organizations want to know everything about people, from their demographics to their voting behavior and political leanings to their interests, personalities, and beyond.[38] Social media platforms are rich sources of this information, which they mine to sell advertising—while legitimate and illegitimate political actors capitalize on it to influence and manipulate the voting public. Microtargeting and dark ads function through the use of data to define narrow groups that can be targeted with exquisitely specific messaging—an issue at the heart of both the Russian interference and Cambridge Analytica scandals.

In the U.S., there is no comprehensive federal data privacy law. The Obama administration put forth a "Consumer Privacy Bill of Rights" in 2012, outlining seven key principles: individual control over data collection and use; transparency about privacy and security policies; data use in context; security; access and accuracy; limits on personal data collection by companies; and accountability.[39] However, this was never codified, leaving Americans' digital privacy to be governed by an uneven patchwork of federal and state departments.[40] In the wake of the Cambridge Analytica scandal, Senators Edward J. Markey (D-Mass.) and Richard Blumenthal (D-Conn.) introduced the Customer Online Notifications for Stopping Edge-provider Network Transgressions (CONSENT) Act, to be enforced by the Federal Trade Commission (FTC), which would require companies like Facebook and Google to obtain opt-in consent from users for all data collection and sharing, implement data security practices, and notify users of data breaches.[41] However, like the Honest Ads Act, the CONSENT Act faces an uphill battle in Congress.

As with campaign finance reform, the states are taking action. California recently passed a landmark privacy protection law, the California Consumer Privacy Act, which is the most stringent in the country. The California law, as with Europe's GDPR and the proposed CONSENT Act, provides that consumers have a right to know what data companies are collecting about them and with whom it is shared, the right to request that their data be deleted, the ability to opt out of the sale of their data, and the ability to access data in a portable format.[42]

Protections such as these ensure that individuals are able to control how their information is used or sold, providing a shield against microtargeting. However, opting out of data collection, sharing, or sales requires action on the part of individuals, and most people may not use the protections available to them without education about the benefits and drawbacks and user-friendly interfaces for doing so.

Proposals:

8. Codify the Consumer Privacy Bill of Rights. We need uniform federal legislation and stronger FTC oversight to protect Americans' privacy and political integrity, rather than relying on the present mishmash of protections. People should have control over how their data is collected and used.

9. Ensure companies' data usage policies are truly accessible and transparent to users. Once charged with this task, the FTC must make sure that consumers have meaningful and easy access to and control over their information, rather than confusing systems that merely adhere to the letter of the law.

10. Include targeting information in on-ad disclaimers with greater specificity than what the platforms are already doing. We should ensure that targeting information for political ads is included not only in the political ad files discussed in the previous section, but also in any on-ad disclaimers.

11. Evaluate targeting options from a civil rights perspective. Targeting political ads based on categories such as gender or race—or using proxies for them such as individuals' interests in black history or Latin hip hop—allows for divisive messaging. Platforms must work with civil rights groups to determine how to best prevent these harms without stifling pro-social efforts such as "get out the vote" drives.

12. Educate the public about their rights and the benefits and drawbacks of allowing their data to be used. Consumers are apt to unthinkingly accept complex privacy and data usage policies in order to access attractive online services. A public education campaign should seek to help people be more informed consumers who understand what is at stake in their choices.

13. Demonetize bad actors on social media. Technology companies should be required to shut down the advertising revenue streams for known malicious or deceptive actors.

Automated and Fake Accounts

Thus far, our policy proposals have focused on paid online advertising and targeted posts. However, as discussed in earlier sections of the paper, coordinated online political manipulation extends beyond such tactics to include the use of political bots and trolls to manipulate and falsify public opinion. To address the challenges posed by computational propaganda, it is necessary to bring greater transparency to the world of automation and algorithms. In order to evaluate the messages that they see on social media, the public needs to trust that messages are not being falsely amplified.

Bots can provide useful informational benefits to the public. Simply banning automated activity on social media would unnecessarily limit expression. Any policy proposal that tackles political bots must distinguish between those that are benevolent and those that are deployed by malicious actors. Transparency can be a useful mechanism for doing so.

Lawmakers at the federal and state levels have introduced legislation attempting to do just that. In Congress, Senator Dianne Feinstein (D-Calif.) recently introduced the Bot Disclosure and Accountability Act, which would require social media companies, under FTC oversight, to label bots on their platforms; prohibit political candidates and parties from using bots to advertise; and restrict the use of bots by political action committees, corporations, and unions.[43]

In California, a new law prohibits the use of bots to mislead people around commercial or political activities and requires that all bots disclose that they are automated accounts.[44]

Tech companies themselves have taken some steps towards reducing the impact of computational propaganda, with varying degrees of effectiveness. Facebook is deploying machine learning to identify fake accounts for removal, as well as introducing a new feature that shows users where a page's administrators are located.[45] Twitter has implemented a new policy of removing suspicious accounts (often but not always bots) from users' follower counts and is suspending accounts at astronomical rates (70 million between May and June 2018).[46]

Proposals:

14. Require disclosure of automated accounts. Bots should be clearly labeled as such, and there should be limits placed on their use for electioneering purposes. This would defang accounts that attempt to impersonate humans in order to deceive the public for political or commercial purposes, without harming the vast majority of bots that serve the public good.

15. Remove automated and fake accounts from follower counts, recommendation engines, and popularity-based algorithms. Social media users need to know what real people on Facebook and Twitter are talking about and how influential a public figure actually is, not what an active botnet or troll army wants them to see. That said, there is some value to anonymous or pseudonymous political speech in the context of supporting dissent in authoritarian regimes; more needs to be done to determine how to enable legitimate anonymity while neutralizing harmful fakery.

16. Require technology companies to disclose what percentage of their users are automated or fake accounts and how successful they have been at removing them. This measure, which could be enforced by the FTC, would enable the public to evaluate the scale of the problem on any given platform.

17. Treat posts by bots as a form of public communication for the purposes of campaign finance law. Bots have been deployed as a way for political campaigns and outside spending groups to share information, but by law, these entities are not supposed to coordinate in any way.[47] Moreover, if automated activity is paid for by a political campaign, it should fall under campaign finance disclosure obligations.

Platform Liability

The Communications Decency Act of 1996 was intended to tackle pornographic, obscene, and indecent material on the internet. It contained a provision—Section 230—that immunizes online service providers from legal liability for content posted by third parties.[48] This provision ensures that providers, such as social media platforms, can set rules governing the content allowed on their sites without being considered "publishers" that have editorial control over—and liability for—that content. Its goals are to promote innovation and protect free expression online. However, this provision has also shielded technology companies from having to confront the harmful activities, such as deceptive digital politics, that are enabled—and shaped—by their services.

Modifying Section 230 would bring a measure of accountability to online service providers, requiring them to be vigilant about addressing digital deception even once public attention

has shifted from present scandals. The counterargument to doing so is that this could cause technology companies to overcorrect and become censorious. However, it is likely possible to craft modifications in such a way as to prevent that. Researcher Tim Hwang has analyzed the options for working with, amending, or eliminating this provision and recommends carving out exceptions to platforms' immunity, incentivizing them to tackle distribution tactics such as foreign interference, automation-based fraud, and microtargeting.[49]

Proposal:

18. Amend Section 230 of the Communications Decency Act to eliminate the liability exemption for online service providers, requiring them to deter foreign election interference, harmful microtargeting, and automation-based political fraud.

Multisector Infrastructure

Digital threats to our democracy have thus far been dealt with on an ad hoc basis by an alphabet soup of federal agencies. Federal infrastructure for dealing with such problems has steadily weakened over time; the Trump administration recently eliminated top cybersecurity policy positions, the Global Engagement Center (a State Department initiative meant to address Russian interference) is strapped for cash, and the Office of Technology Assessment, which used to provide Congress with authoritative analyses of scientific and technological issues, was defunded in 1995.[50, 51]

Meanwhile, technology companies are coordinating around election security—but in private and with little guarantee of ongoing knowledge sharing over time due to competitive pressures.

In addition to requiring Congress to act and empowering the FEC and the FTC to protect voters and consumers online, we must build a robust multisector infrastructure for proactively tackling deceptive digital politics. One newly introduced Senate bill would create an "emerging technology policy lab" tasked with analyzing and making recommendations regarding the use of new technologies such as artificial intelligence by the federal government; it might be possible to include measures related to deceptive digital politics under this agency's purview.[52] Beyond information sharing, coordination, and analysis, such a body could potentially have enforcement capabilities.

Proposals:

19. Reinstate the Office of Technology Assessment to ensure that Congress is up to date on developments in digital and other technologies. The legislative branch's lack of objective technical expertise is hampering its ability to govern in the face of technological advances, creating gaps that will only become more dangerous with time.

20. Reinstate a cybersecurity policy lead in the executive branch. National Security Council senior directors are currently doing this work; however, it merits a dedicated expert to lead efforts.[53]

21. Establish a central agency or task force to coordinate information sharing between federal agencies and technology companies. This entity could detect and counter threats, enforce or advise on enforcement of related laws and regulations, and remain up-to-date on relevant technological and geopolitical developments. This could be a new body or, more efficiently, an expansion in scope for an existing agency.

SYSTEMIC CHANGES

In parallel to tackling deceptive digital threats in the short term, we must work as a society towards systemic changes to prevent or mitigate present and future threats. These efforts may take years to have measurable impact, but they are needed to structure a more resilient democracy. Beyond advocating for the immediate and urgent steps outlined above, civil society has a major role to play in advancing these measures.

Global Cooperation

In order to protect democracy at the global level, the U.S. must convene and take part in international conversations about deceptive digital politics. Democracies around the world are grappling with computational propaganda, but despite the global scale and interconnectedness of the problem, there has been little international coordination to resolve it. Several countries have attempted to regulate the problem on their own, with varying degrees of success. Some have taken markedly authoritarian approaches, further destabilizing democracy rather than safeguarding it.[54] Effective approaches to improve coordination in this area will likely take time due to the complexities of geopolitical strategy and the foreign policy incentives involved; however, they are necessary to future-proof democracy in the long term.

The European Union has taken a strong regulatory approach to technology companies in some areas. From the GDPR to antitrust regulations and fines, the EU has acted rapidly to protect consumer privacy and weaken perceived monopolies—often at significant cost to technology companies.[55] However, when it comes to election protection, the EU has thus far taken a weaker tack. In September 2018, Facebook, Google, Twitter, and other major companies signed onto a European Commission Code of Practice agreeing to address political advertising transparency, demonetization of bad actors, and fake accounts and bots; amplify authoritative content; and share data with researchers.[56] However, this agreement lacks measurable outcomes or enforcement mechanisms, falling prey to the usual pitfalls of self-regulation.[57]

Proposals:

22. Establish a global cybersecurity accord. Information warfare is a growing threat to democracy and international stability. Creating an international agreement to eschew online election interference in other countries would be a meaningful step towards protecting democracy. Ideally, this would include enforcement mechanisms.

23. Share information openly between allies. Government agencies, technology companies, and civil society actors around the world should share intelligence about manipulation operations freely across borders and aid in each other's transnational enforcement efforts.

24. Learn from policy models around the world. It is important to evaluate and learn from efforts to counter digital deception in other countries, while promoting responses based in democratic principles. Of course, policy models must be adapted to the local context; laws that might work in one country may be counterproductive in another, depending on governing structures, political dynamics, and differential uses of social media by populations. For example, disinformation spread on WhatsApp is a larger problem in other countries than in the U.S. and necessitates tailored responses.[58]

25. Promote democratic responses to digital deception abroad. Deceptive digital politics occurs across national boundaries and is being used to advance nationalistic and authoritarian agendas around the world. In the interest of promoting international stability, the U.S. should encourage other countries to respond to digital threats in ways that bolster democracy.

Research and Development

Technology companies must collaborate with civil society on research to detect threats, understand the political impacts of existing technologies, and design new digital technologies that better serve the public interest.

Academics and independent research groups have already contributed significantly to our understanding of deceptive digital politics; however, they are severely limited by what data the platforms choose to make available to them.

Facing greater public scrutiny, Facebook and Twitter have already taken small steps towards collaboration with researchers. Facebook has partnered with the Social Science Research Council, Social Science One, and philanthropic foundations on the Social Data Initiative, which shares privacy-protected data with researchers studying the role of social media in democracy and elections.[59] However, this initiative comes with a major caveat: data will only be made available for 2017 and later, preventing examination of the 2016 election.[60] As discussed above, Facebook's civil rights audit is a promising step, though greater transparency is needed with regard to its findings in order to ensure the company follows through. Meanwhile, as part of its goal to promote "healthy conversation," Twitter has partnered with researchers examining echo chambers and ties between online communities.[61] It is important to note that while the researchers' results remain independent, the platforms have heavy influence in setting the research agenda.

Civil society actors have also begun to develop frameworks for designing better technologies. From the Center for Humane Technology to the Institute for the Future's Ethical OS Toolkit (which Woolley helped develop), public interest technologists, social scientists, and advocacy groups are conceptualizing ways to build ethical considerations into the R&D process.[62]

Proposals:

26. Share data openly with third-party researchers. Technology companies should be required to provide researchers with access to platform data—of course, protecting user privacy— without placing limitations on the research agenda. Concerted efforts should be made to include researchers representing and studying impacts on marginalized groups.

27. Develop tools to detect disinformation and false accounts. While improving artificial intelligence won't be a magic bullet for solving deceptive digital politics, it is a necessary part of the solution. Technology companies possess expertise that government agencies lack when it comes to detecting digital threats. By sharing data with outside researchers, technology companies could likely greatly speed up the process of developing tools to assist with identifying deceptive political actors and content.

28. Consult with civil rights groups on an ongoing basis and incorporate findings into product development. Facebook's audit is a good starting point, but the results should be made public in the interest of transparency and accountability. Moreover, these groups' perspectives should be incorporated into product development processes rather than treated as a one-off public relations engagement.

29. Collaborate on ethical technology. Technology companies should engage with efforts such as the Center for Humane Technology and the Ethical OS in order to improve their design processes. New social media technologies should account for the ways they can be abused and should be designed to advance the public interest, not just companies' bottom lines.

Media and Civic Education

Most of the measures we have discussed so far seek to counter the threat of digital deception via efforts to target malicious actors and deceptive tactics. Another important piece of the puzzle is how to increase the resilience of the public in the face of digital attacks on political processes. This can be done by reinvigorating civic education and media literacy skills in the population, as well as by supporting credible media sources so that the press can work to amplify the truth in the face of disinformation.

Media organizations and civil society groups are already doing significant work to combat disinformation—via fact-checking initiatives, for example. However, they face major challenges in the social media environment, where the supposed democratization of information has made it easy to post and amplify incredible amounts of content and flattened the distinction between credible and deceptive information sources. Fact-checking is time consuming and checkers struggle to keep pace with the spread of disinformation. Facebook's partners, for example, take three days to process and down-rank false information once it is brought to their attention.[63] Moreover, it is unclear whether fact checks have the intended effect on audiences.

The public, meanwhile, struggle to understand the extent to which social media has affected the distribution of information or to distinguish between reliable and unreliable sources. People readily seek out information that confirms their biases; in fact research suggests that many may view the consumption of partisan news as a form of political expression.[64] Media literacy and civic education can combat the biases that predispose people to fall prey to digital deception.

Proposals:

30. Multisector media literacy initiatives. The government should work with tech companies, media outlets, and other civil society groups on a large-scale public education campaign about disinformation and critical reading skills.

31. Build media literacy and civics into public education. Public schools should incorporate democratic principles and media evaluation skills into their curricula to ensure that the next generation of voters is less susceptible to deceptive digital tactics.

32. Support local newsrooms. Funders, technology companies, and the rest of civil society need to rally around local reporting. We need to rebuild the infrastructure of credible journalism as a counterweight to disinformation.

Competition

A final area that merits consideration is policies to promote competition and reduce the market dominance of companies such as Facebook and Alphabet. This could help alleviate the harms of deceptive digital politics by reducing the reach of platforms, forcing them to reevaluate their business models, and making them more likely to comply with regulation.

Proponents of antitrust legislation argue that technology companies have grown too big to hold accountable and are engaged in anti-competitive behavior that gives them disproportionate reach and influence.[65] Facebook, for one, has captured a major portion of the social media market with its acquisitions of Instagram and WhatsApp. Google, meanwhile, was fined $5 billion by the EU in July 2018 for tying its search engine and Chrome to Android devices.[66] This amount doesn't meaningfully impact Google's profits—but if companies were to be policed more heavily by market regulators in the U.S. and around the world, they might be more amenable to reevaluating their business models.

Measures to increase competition for online platforms won't eliminate digital deception, however. Opportunistic actors can simply move to new platforms. Facebook provides influence operatives with enormous reach (two billion users) at low cost, combined with the functionality to narrowly target specific groups. However these actors already engage in cross-platform operations. The ecosystem of digital deception extends from gaming platforms like Discord to 4Chan and 8Chan to Tumblr, Pinterest, and LinkedIn. Introducing competitive pressures might reduce the reach of any single platform, but the barriers to operating on more and newer platforms will likely remain low enough that online political manipulation will continue apace.

Proposals:

33. Review mergers and acquisitions more stringently. Facebook and Alphabet have achieved market dominance by acquiring new businesses and potential rivals. The FTC should review all past and future mergers and acquisitions by these companies with a more stringent standard than the present one (which is based on costs to consumers—a standard that is largely irrelevant in the face of these companies' "free" products).[67]

34. Investigate and enforce penalties for anti-competitive behavior by technology companies. Those competitors that the technology titans don't acquire, they seek to drive out of business using their existing market dominance. The FTC must bring greater accountability to the technology sector and penalize bad behavior by companies to demonstrate that they can no longer act against the public interest with impunity.

CONCLUSION

Our democracy is being threatened by deceptive digital politics—and though the problem has been widely known since the 2016 election, we have yet to act to safeguard our political processes. Leaving technology companies to their own devices has failed to protect the public interest, while the problem itself is being used to feed nationalistic and authoritarian propaganda narratives in the U.S. and around the world. It is imperative that government, civil society, and technology companies come together to respond to these complex problems via policy interventions that are grounded in democratic principles.

In this paper, we have offered numerous proposals for combatting digital deception in politics, grounded in the principles of transparency, accountability, standards, coordination, adaptability, and inclusivity. While wide-ranging, these proposals are not comprehensive, and each merits further consideration to ensure that it truly serves the public interest. We hope that this can serve as a productive starting point for a rapid deliberation process that results in meaningful policy change in time for the 2020 elections.

References

[1]Stubbs, J., & Bing, C. (2018, August 28). Exclusive: Iran-based political influence operation - bigger, persistent, global. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-iran-facebook-exclusive/exclusive-iran-based-political-influence-operation-bigger-persistent-global-idUSKCN1LD2R9

[2]Nimmo, B. (2018, August 16). #TrollTracker: Russian Traces in Facebook Takedown. Retrieved January 17, 2019, from https://medium.com/dfrlab/trolltracker-russian-traces-in-facebook-takedown-767aac0a3483

[3]Ghosh, D., & Scott, B. (2018a). *Digital Deceit: The Technologies Behind Precision Propaganda on the Internet*. New America. Retrieved from https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/

[4]Woolley, S. C., & Howard, P. N. (2018). Introduction: Computational Propaganda Worldwide. In S. C. Woolley & P. N. Howard (Eds.), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (pp. 3–18). Oxford, New York: Oxford University Press.

[5]Brandeis, L. D. (1914). *Other People's Money: And how the Bankers Use it* (p.92). New York, NY: F.A. Stokes.

[6]Buckley v. Valeo, No. 75–436 (U.S. January 30, 1976).

[7]Frier, S., & Sebenius, A. (2018, September 4). Who's in Charge of Protecting Social Media from Election Interference? *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2018-09-04/who-s-in-charge-of-protecting-social-media-from-election-interference

[8]Collier, K. (2018, August 23). Tech Companies Are Gathering For A Secret Meeting To Prepare A 2018 Election Strategy. *BuzzFeed News*. Retrieved from https://www.buzzfeednews.com/article/kevincollier/tech-companies-are-gathering-for-a-secret-meeting-to

[9]Lapowsky, I. (2018, August 22). Tech Giants Are Becoming Defenders of Democracy. Now What? *Wired*. Retrieved from https://www.wired.com/story/microsoft-facebook-tech-giants-defending-democracy/

[10]Woolley, S. C., & Howard, P. N. (2018). Introduction: Computational Propaganda Worldwide. In S. C. Woolley & P. N. Howard (Eds.), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (pp. 3–18). Oxford, New York: Oxford University Press.

[11]Bennett Moses, L. (2007). Recurring Dilemmas: The Law's Race to Keep Up With Technological Change. *Journal of Law, Technology, & Policy*, *2007*(21), 239–285. https://doi.org/10.2139/ssrn.979861

[12]Groll, E. (2018, April 10). Zuckerberg: We're in an 'Arms Race' With Russia, but AI Will Save Us. Retrieved January 17, 2019, from https://foreignpolicy.com/2018/04/10/zuckerberg-facebook-were-in-an-arms-race-with-russia-but-ai-artificial-intelligence-will-save-us/

[13]Gleicher, N., & Stamos, A. (2018, July 31). Removing Bad Actors on Facebook. Retrieved January 17, 2019, from https://newsroom.fb.com/news/2018/07/removing-bad-actors-on-facebook/

[14]DiResta, R., Shaffer, K., Ruppel, B., Matney, R., Fox, R., Albright, J., … Sullivan, D. (2018, December 17). *The Tactics & Tropes of the Internet Research Agency*. New Knowledge. Retrieved from https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf

[15]Fischer, S. (2018, May 2). Exclusive: Facebook commits to civil rights audit, political bias review. Retrieved January 17, 2019, from https://www.axios.com/scoop-facebook-committing-to-internal-pobias-audit-1525187977-160aaa3a-3d10-4b28-a4bb-b81947bd03e4.html

[16]Funke, D. (2018, August 15). Americans don't think the platforms are doing enough to fight fake news. Retrieved January 17, 2019, from https://www.poynter.org/fact-checking/2018/americans-dont-think-the-platforms-are-doing-enough-to-fight-fake-news/

[17]Frenkel, S., Confessore, N., Kang, C., Rosenberg, M., & Nicas, J. (2018, November 30). Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis. *The New York Times*. Retrieved from https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html

[18]Stolzoff, S. (2018, November 16). The problem with social media has never been about bots. It's always been about business models. Retrieved January 17, 2019, from https://qz.com/1449402/how-to-solve-social-medias-bot-problem/

[19]Morozov, E. (2014). *To Save Everything, Click Here: The Folly of Technological Solutionism* (Reprint edition). New York, NY: PublicAffairs.

[20]Harwell, D. (2018, April 11). AI will solve Facebook's most vexing problems, Mark Zuckerberg says. Just don't ask when or how. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/ai-will-solve-facebooks-most-vexing-problems-mark-zuckerberg-says-just-dont-ask-when-or-how/?

[21]Vincent, J. (2018, April 5). Why AI isn't going to solve Facebook's fake news problem. Retrieved January 17, 2019, from https://www.theverge.com/2018/4/5/17202886/facebook-fake-news-moderation-ai-challenges

[22]Shahbaz, A. (2018). *Freedom on the Net 2018*. Freedom House. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2018

[23]Federal Election Commission. (2018). Internet Communication Disclaimers and Definition of '"Public Communication."' *Federal Register*, *83*(58), 12864–12881.

[24]Honest Ads Act, S. 1989, 115th Cong. (2017).

[25]Picchi, A. (2018, April 11). Facebook: What is the Honest Ads Act? *CBS News*. Retrieved from https://www.cbsnews.com/news/facebook-hearings-what-is-the-honest-ads-act/

[26]Ad Archive. (n.d.). Retrieved January 17, 2019, from https://www.facebook.com/ads/archive/?active_status=all&ad_type=political_and_issue_ads&country=US

[27]Gadde, V., & Falck, B. (2018, May 24). Increasing Transparency for Political Campaigning Ads on Twitter. Retrieved January 17, 2019, from https://blog.twitter.com/en_us/topics/company/2018/Increasing-Transparency-for-Political-Campaigning-Ads-on-Twitter.html

[28]Walker, K. (2018, May 4). Supporting election integrity through greater advertising transparency. Retrieved January 17, 2019, from https://www.blog.google/outreach-initiatives/public-policy/supporting-election-integrity-through-greater-advertising-transparency/

[29]Ghosh, S. (2018, October 31). Facebook approved political ads "paid for" by Cambridge Analytica - Business Insider. *Business Insider*. Retrieved from https://www.businessinsider.com/facebook-approved-political-ads-paid-for-by-cambridge-analytica-2018-10

[30]Turton, W. (2018, October 25). Facebook's political ad tool let us buy ads "paid for" by Mike Pence and ISIS. *Vice News*. Retrieved from https://news.vice.com/en_us/article/wj9mny/facebooks-political-ad-tool-let-us-buy-ads-paid-for-by-mike-pence-and-isis

[31]Singer, N. (2018, September 2). Tech Giants Now Share Details on Political Ads. What Does That Mean For You? *The New York Times*. Retrieved from https://www.nytimes.com/2018/09/02/technology/03adarchive.html

[32]Guynn, J. (2018, October 17). Facebook takes down ads mentioning African-Americans and Hispanics, calling them political. *USA TODAY*. Retrieved from https://www.usatoday.com/story/news/2018/10/17/facebook-labels-african-american-hispanic-mexican-ads-political/1608841002/

[33]Nix, N. (2018, August 6). Russian Meddling Prompts States to Impose Online Ad Rules. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2018-08-06/russian-meddling-prompts-states-to-set-online-political-ad-rules

[34]Sanders, E. (2019, January 2). As 2019 Begins, So Does Facebook's Ban on Local Political Ads in Washington State. *The Stranger*. Retrieved from https://www.thestranger.com/slog/2019/01/02/37628091/as-2019-begins-so-does-facebooks-ban-on-local-political-ads-in-washington-state

[35]Sridharan, H., & Ravel, A. M. (2017). *Illuminating Dark Digital Politics: Campaign Finance Disclosure for the 21st Century* (p. 14). MapLight. Retrieved from https://s3-us-west-2.amazonaws.com/maplight.org/wp-content/uploads/20171017200640/Illuminating-Dark-Digital-Politics.pdf

[36]Chapter 9 - Committee Report - Form 460. (2018). In *Campaign Disclosure Manual 1 - Information for State Candidates, Their Controlled Committees, and Primarily Formed Committees for State Candidates* (pp. 9.1-9.52). California Fair Political Practices Commission. Retrieved from http://www.fppc.ca.gov/content/dam/fppc/NS-Documents/TAD/Campaign%20Manuals/Manual_1/Manual-1-Chapter-9-Form-460.pdf

[37]Nadler, A., Crain, M., & Donovan, J. (2018, October 17). *Weaponizing the Digital Influence Machine*. Data & Society. Retrieved from https://datasociety.net/output/weaponizing-the-digital-influence-machine/

[38]Howard, A. (2018, August 22). US election campaign technology from 2008 to 2018, and beyond. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/611823/us-election-campaign-technology-from-2008-to-2018-and-beyond/

[39]The White House. (n.d.). *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf

[40]Kerry, C. F. (2018). *Why protecting privacy is a losing game today – and how to change the game*. Brookings Institute. Retrieved from https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/

[41]Lawler, R. (2018, April 10). Senators introduce bill creating a "privacy bill of rights." *Engadget*. Retrieved from https://www.engadget.com/2018/04/10/senators-introduce-bill-creating-a-privacy-bill-of-rights/

[42]Ghosh, D. (2018, July 11). What You Need to Know About California's New Data Privacy Law. *Harvard Business Review*. Retrieved from https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law

[43]Feinstein Bill Would Regulate Social Media Bots Designed to Influence U.S. Elections |. (2018, June 25). Retrieved January 18, 2019, from https://www.judiciary.senate.gov/press/dem/releases/feinstein-bill-would-regulate-social-media-bots-designed-to-influence-us-elections

[44]Musil, S. (2018, October 1). California bans bots secretly trying to sway elections. *CNET*. Retrieved from https://www.cnet.com/news/california-bans-bots-secretly-trying-to-sway-elections/

[45]Reynolds, T., Bassante, D., Chakrabarti, S., Lyons, T., Gleicher, N., & Leathern, R. (2018, July 24). Q&A on Election Integrity | Facebook Newsroom. Retrieved January 18, 2019, from https://newsroom.fb.com/news/2018/07/qa-on-election-intergrity/

[46]Timberg, C., & Dwoskin, E. (2018, July 6). Twitter is sweeping out fake accounts like never before, putting user growth at risk. *The Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/?

[47]Howard, P. N., Woolley, S., & Calo, R. (2018). Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics*, *15*(2), 81–93. https://doi.org/10.1080/19331681.2018.1448735

[48]Communications Decency Act, 47 U.S.C. § 230 (1996).

[49]Hwang, T. (2017). *Dealing with Disinformation: Evaluating the Case for CDA 230 Amendment* (SSRN Scholarly Paper No. ID 3089442). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=3089442

[50]Lapowsky, I. (2018, August 22). Tech Giants Are Becoming Defenders of Democracy. Now What? *Wired*. Retrieved from https://www.wired.com/story/microsoft-facebook-tech-giants-defending-democracy/

[51]Cordell, C. (2018, June 11). Attempt to reinstate the congressional technology office falls flat in House. *FedScoop*. Retrieved from https://www.fedscoop.com/house-office-of-technology-assessment-fails/

[52]AI in Government Act of 2018, S. 3502, 115th Cong. (2018).

[53]Barrett, B. (2018, May 15). White House Cuts Critical Cybersecurity Role as Threats Loom. *Wired*. Retrieved from https://www.wired.com/story/white-house-cybersecurity-coordinator/

[54]Funke, D. (2019, January 8). A guide to anti-misinformation actions around the world. Retrieved February 7, 2019, from https://www.poynter.org/fact-checking/2019/a-guide-to-anti-misinformation-actions-around-the-world/

[55]Satariano, A. (2018, May 24). G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog. *The New York Times*. Retrieved from https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html

[56]Code of Practice on Disinformation. (2018, September 26). *Digital Single Market - European Commission*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

[57]Lomas, N. (2018, September 26). Tech and ad giants sign up to Europe's first weak bite at 'fake news.' Retrieved February 7, 2019, from http://social.techcrunch.com/2018/09/26/tech-and-ad-giants-sign-up-to-europes-first-weak-bite-at-fake-news/

[58]Bradshaw, S., & Howard, P. N. (2018). *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*. Oxford Internet Institute. Retrieved from https://comprop.oii.ox.ac.uk/research/cybertroops2018/

[59]King, G., & Persily, N. (2019). *A New Model for Industry-Academic Partnerships*. Working Paper. Retrieved from https://gking.harvard.edu/partnerships

[60]Ingram, D. (2018, August 18). Facebook opens up to researchers — but not about 2016 election. *NBC News*. Retrieved from https://www.nbcnews.com/tech/tech-news/facebook-opens-researchers-not-about-2016-election-n901651

[61]Gadde, V., & Gasca, D. (2018, July 30). Measuring healthy conversation. Retrieved February 7, 2019, from https://blog.twitter.com/en_us/topics/company/2018/measuring_healthy_conversation.html

[62]McGonigal, J., & Woolley, S. (2018, August 7). Ethical OS Toolkit. Retrieved February 7, 2019, from https://ethicalos.org/

[63]Funke, D., & Mantzarlis, A. (2018, December 14). We asked 19 fact-checkers what they think of their partnership with Facebook. Here's what they told us. Retrieved February 7, 2019, from https://www.poynter.org/fact-checking/2018/we-asked-19-fact-checkers-what-they-think-of-their-partnership-with-facebook-heres-what-they-told-us/

[64]Owen, L. H. (2018, December 7). Few people are actually trapped in filter bubbles. Why do they like to say that they are? Retrieved February 7, 2019, from http://www.niemanlab.org/2018/12/few-people-are-actually-trapped-in-filter-bubbles-why-do-they-like-to-say-that-they-are/

[65]Ghosh, D., & Scott, B. (2018b). *Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet*. New America. Retrieved from https://www.newamerica.org/public-interest-technology/reports/digital-deceit-ii/

[66]Warren, T. (2018, July 18). Google fined a record $5 billion by the EU for Android antitrust violations. Retrieved February 7, 2019, from https://www.theverge.com/2018/7/18/17580694/google-android-eu-fine-antitrust

[67]Ghosh, D., & Scott, B. (2018b). *Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet*. New America. Retrieved from https://www.newamerica.org/public-interest-technology/reports/digital-deceit-ii/