Fool Me Once: Regulating “Fake News” and other Online Advertising

Abby Wood*  Ann M. Ravel†  Irina Dykhne‡

*University of Southern California, awood@law.usc.edu
†University of California, Berkeley School of Law, ann.ravel@gmail.com
‡University of Southern California Law School, irina.dykhne.2018@lawmail.usc.edu

This working paper is hosted by The Berkeley Electronic Press (bepress) and may not be commercially reproduced without the permission of the copyright holder.

http://law.bepress.com/usclwps-lss/261

Copyright ©2018 by the authors.
Fool Me Once: Regulating “Fake News” and other Online Advertising

Abby Wood, Ann M. Ravel, and Irina Dykhne

Abstract

A lack of transparency for online political advertising has long been a problem in American political campaigns. Disinformation attacks that American voters have experienced since the 2016 campaign have made the need for regulatory action more pressing.

Platforms desire self-regulation and have only recently come around to supporting transparency regulations. While government must not regulate the content of political speech, it can, and should, force transparency into the process. We propose several interventions aimed at transparency. Most importantly, campaign finance regulators should require platforms to store and make available ads run on their platforms, as well as the audience at whom the ad was targeted. Audience availability can be structured to avoid privacy concerns, and it meets an important speech value in the “marketplace of ideas” theory of the First Amendment, that of enabling counter speech. Our proposed regulations would capture any political advertising, including disinformation, that is promoted via paid distribution on social media, as well as all other online political advertising. Second, Congress should stop preventing regulatory agencies from closing existing loopholes around disclosure and disclaimers. Finally, government should require an opt-in for social media users to view narrowly-targeted ads or disputed content.
Fool Me Once: Regulating “Fake News” and other Online Advertising

Abby K. Wood, Ann M. Ravel, Irina Dykhne

April 18, 2018


Abstract

A lack of transparency for online political advertising has long been a problem in American political campaigns. Disinformation attacks that American voters have experienced since the 2016 campaign have made the need for regulatory action more pressing.

Platforms desire self-regulation and have only recently come around to supporting transparency regulations. While government must not regulate the content of political speech, it can, and should, force transparency into the process. We propose several interventions aimed at transparency. Most importantly, campaign finance regulators should require platforms to store and make available ads run on their platforms, as well as the audience at whom the ad was targeted. Audience availability can be structured to avoid privacy concerns, and it meets an important speech value in the “marketplace of ideas” theory of the First Amendment, that of enabling counter speech. Our proposed regulations would capture any political advertising, including disinformation, that is promoted via paid distribution on social media, as well as all other online political advertising. Second, Congress should stop preventing regulatory agencies from closing existing loopholes around disclosure and disclaimers. Finally, government should require an opt-in for social media users to view narrowly-targeted ads or disputed content.

1 Wood is Associate Professor of Law, Political Science, and Public Policy at University of Southern California (awood@law.usc.edu); Ravel is Lecturer in Law at Berkeley Law, and former Chair of the Federal Election Commission and California Fair Political Practices Commission; Dykhne is a J.D. candidate at the USC Gould School of Law. The paper has benefited from insights from Rebecca Brown, Chris Elmendorf, and Rick Hasen. Daniel Brovman, Samantha Hay, Justin Mello, Brandon Thompson, and Caroline Yoon provided fantastic research assistance. Teresa Delgado and Alex Manzanares joyfully created the time and space required to focus on the project. We also appreciate the following students for sharing their seminar papers from Wood’s Money in Politics class as we built the early drafts of this project: Oliver Wu, Sean Stratford-Jones, Mei Tuggle, Lauren Fishelman, Adrian Mahistede, Edward Prouty.
Introduction........................................................................................................................................3

1. Documenting and Framing the Problem..........................................................................................6
   A. Fake News is Political Advertising..........................................................................................7
   B. How Disinformation Can Weaken Democracy .........................................................................12

2. First Amendment, Political Speech, and Choice of Regulator ....................................................15
   A. Constitutional Framework for Campaign Advertising Regulation ........................................15
   B. Choice of Regulator..................................................................................................................21
      Industry Self-Regulation and Co-Regulation ........................................................................21
      Government Regulation...........................................................................................................24

3. Our Current, Insufficient, Regulatory Framework for Online Political Advertising ......................26

4. Constitutionally-Permissible Regulations to Address Disinformation Advertising ............................31
   A. Improve Transparency ...........................................................................................................33
      Require Platforms to Keep and Disclose all Political Communications and Audiences ..........35
      Close the Loophole for Disclaimers in Online Ads .................................................................44
      Eliminate Donor Anonymity for LLCs and 501(c) Organizations ........................................45
   B. “Nudge” and Educate Sharers and Viewers ...........................................................................45
   C. Considerations for Platform Efforts to Reduce Disinformation ............................................48
   D. A Note about Feasibility ..........................................................................................................49

5. Task Assignment and Action Across Multiple Jurisdictions ..........................................................50
   A. Federal Agency Competencies and Task Assignment ..............................................................50
   B. The Role of State and Local Government .............................................................................52

Conclusion...........................................................................................................................................53
INTRODUCTION

During the 2016 Presidential campaign, the average adult saw at least one “fake news” item on social media. The people distributing the articles had a variety of aims and operated from a variety of locations. Among the locations we know about, some were in Los Angeles, others in Macedonia, and yes, others were in Russia. The Angelenos aimed to make money and sow chaos. The Macedonians wanted to get rich. And the Russians aimed to weaken Hillary Clinton’s candidacy for president, foster division around fraught social issues, and make a spectacle out of the U.S. election. To these ends, the Russians mobilized trolls, bots, and so-called “useful idiots”, along with sophisticated ad tracking and micro-targeting techniques to strategically distribute and amplify propaganda. The attacks are ongoing.

Cheap distribution and easy user targeting on social media enable the rapid spread of disinformation. Disinformative content, like other online political advertising, is “micro-targeted” at narrow segments of the electorate, based on their narrow political views or biases. The targeting aims to polarize and fragment the electorate. Tracing the money behind this kind of messaging is next to impossible under the current regulations and Facebook’s current policies. Voters’ inability to “follow the money” has implications for our democracy, even in the absence of disinformation. And of course, an untraceable flood of disinformation prior to an election stands to undermine voters’ ability to choose the candidate that best aligns with their preferences.

Untraceable online political advertising undermines key democratic values, and the problem is exacerbated when the messaging contains

---

3 Undermining Democratic Institutions and Splintering NATO: Russian Disinformation Aims, Before the H. Comm. on Foreign Affairs, 115th Cong. 1, 27 (2017) (statement of Peter Doran, Executive Vice President, Center for European Policy Analysis).
4 See Russian Interference in the 2016 U.S. Elections, Before the S. Select Comm. on Intelligence, 115th Cong. 72-76 (2017) (statement of J. Alex Halderman, Professor of Comput. Sci. and Eng’g, Univ. of Michigan); Id. at 2, 20, 30.
6 Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel I, Before the S. Select Comm. on Intelligence, 115th Cong. 30-42 (2017) (statement of Clint Watts, Robert A. Fox Fellow, Foreign Policy Research Inst.).
disinformation. Scholars and analysts are writing about fake news and the failures of platforms to contain it. Some have focused on evaluating the impact of fake news on voter behavior and beliefs, or on political agenda setting. Others focus on legal fixes, such as direct platform regulation by restoring (or modifying) a statute that exempts platforms from liability arising from others’ speech on their platforms. Some offer media-based solutions. Others emphasize that platforms are the only entities who can, or should, correct the problem while staying within the existing First Amendment framework. Others are ready to re-interpret the First Amendment in light of the new imbalance between speakers and listeners. And some scholars have suggested that platforms should be regulated in a way that fits a pre-existing regulatory framework, such as the way we regulate media organizations or public utilities.

We add to this conversation that fake news and other online political advertising should be addressed with existing regulatory tools developed for older kinds of political advertising. Our argument begins with the simple observation that fake news is not “news”. It is political advertising. Like other kinds of political advertising, fake news seeks to persuade, mobilize, or suppress

---


voters and votes. And like other kinds of political advertising, it involves costs for production and distribution. Fake news is an especially confusing type of political advertising for two reasons. It is native, meaning that it poses as editorial or reporting content, and it is disinformative. Fake news is not the only format in which disinformation advertising occurs. Disinformation advertising is also distributed in the form of memes, videos, and images. The common theme among disinformation advertising is that it is false, it aims to affect people’s political opinions, and the advertiser pays to produce or distribute it.

The First Amendment provides clear limits on government’s ability to regulate politically-related messaging. The Constitution clearly allows for more government regulation than exists today for political speech on social media. The courts have repeatedly upheld both campaign finance disclaimers and disclosure of the funding behind political spending. At a minimum, disinformation advertising should be transparent.

Our campaign finance laws are riddled with gaps and loopholes, which exclude a large portion of online advertising from disclosure and disclaimer requirements. The lack of transparency for online ads facilitates violations of the ban on foreign spending in U.S. elections, and even where the source of the political communication is domestic, the public’s inability to “follow the money” may impact voters’ ability to make the right choice for them. Adding disinformation to the mix further damages the ability of voters to make the choice that best aligns with their preferences. While regulations to respond to this problem have been proposed, the agency tasked with regulation is not likely to enact anything in the near term.

The government should not rely upon the platforms to regulate themselves. While each platform is making proposals to increase transparency online, the fact remains that the lack of transparency originated with them, and for at least a decade, it appeared to serve their profit interests. Nevertheless, constitutional limits mean that only the platforms are able to implement some

---


16 Michael Gilbert’s work points out that there is a tradeoff between the loss of information from speech that may be “chilled” by disclosure and the loss of information where disclosure is unavailable. See Michael D. Gilbert, Campaign Finance Disclosure and the Information Tradeoff, 98 IOWA L. REV. 1847, 1858-61, 1866-69 (2013). Chilling and informational effects are difficult to measure. Our best estimates of chilling are that the effect is negligible. The information benefit from voters using heuristics is measurable and should outweigh any chilling effect, though no study has attempted to simultaneously measure both at the same time. See generally, Abby K. Wood, Campaign Finance Disclosure, ANN. REV. L. & SOC. SCI., forthcoming vol. 14 (on file with author).
potential fixes. If platforms are unable or unwilling to act in those areas, government cannot step in.

In this Article, we propose three transparency-related government regulations to increase transparency of political advertising and begin to address the problem of disinformation advertising. Our proposed regulations are all modest extensions of the way the federal government already regulates political advertising and are crucial for shedding light on the sources of political messaging online. Part I of this Article explains why disinformation advertising as it existed in 2016 – unregulated, from unknown sources, and aimed to fragment our politics – creates a problem for our democracy. In Part II, we explain the constitutional framework in which additional regulation would occur. We also explain the tradeoffs between regulation by government or regulation by platforms. In Part III, we discuss the loopholes in our existing regulatory system for political advertising online. The loopholes have enabled disinformation advertising to be distributed without regulation even when paid for by a foreign government. Part IV proposes several regulatory solutions that could reduce disinformation advertising, and short of reducing it, would make enforcement and following the money much easier. Our proposal for government regulation focuses on transparency. We also suggest guidelines for platform self-regulation to attack the problem. A brief review of regulations in several foreign jurisdictions, which concludes Part IV, demonstrates that social media platforms are already willing and able to comply with stricter regulation in other countries. Finally, in Part V, we consider task assignment within the federal bureaucracy, as well as actions taken at other levels of government. Federal inaction on the threat posed by Russian disinformation is not the whole story; cities and states are beginning to act to regulate platforms for city-wide elections.

1. DOCUMENTING AND FRAMING THE PROBLEM

“Fake news”, or fabricated news articles or blog posts that are intentionally false or misleading, have received a lot of attention since the 2016 general election. Fake news articles are distributed via social media to drive web traffic to websites.\(^\text{17}\)

We argue that the problem of “fake news” is better framed as a problem of native political advertising, and that the phenomenon benefits from lack of campaign finance transparency online. In this section, we describe the fake news phenomenon, tie fake news to campaign advertising in ways that allow for regulatory traction, and explain how disinformation presents challenges to democracy.

\(^\text{17}\) See Hunt & Gentzkow, supra note 2, at 213.
A. Fake News is Political Advertising

Fake news stories inundated social media networks during the 2016 election, sometimes generating millions of comments and reactions from users.18 Sophisticated disinformation is persuasive because it looks like credible journalism.19 But fake news is not “news.” It is native advertising and should be regulated as such. In the same way that commercial advertisers seek to persuade by projecting a particular image of a product, purveyors of political disinformation ads use fabricated information to persuade voters that a candidate is untrustworthy or unfit for office,20 or more generally to sow division among Americans.21 During the 2016 presidential election, many of these disinformation ads were strategically targeted at select groups to either encourage or suppress votes.22 Persuasion and targeting are the cornerstones of advertising. We therefore reject the label “fake news” and adopt “disinformation advertising.”

Plenty of disinformation advertising was produced in the United States. Indeed, a company called “DisInfoMedia”, which was the source of several fake news articles during the election, lists its address in suburban Los Angeles.23 But the public’s attention has been captured by fake news placed by foreign actors, especially Russians aiming to intervene in our election. Russia’s attack occurred (and continues) on social media platforms.24 Expert estimates of the number of shares on Facebook vary widely, from over 100 million to “into the billions”.25 These estimates include content ranging from fake news to generic

---

18 See generally, e.g., id. at 211-236; see also Silverman, supra note Error! Bookmark not defined.
20 See Entous et al., supra note 110.
22 See id. at ¶46.
25 Albright, supra note ; Burr statement, supra note .

ideological statements from foreign sources with no disinformative content. The fact is, lack of disclosure of online political spending means that no one captured the entire universe of political ads. The best evidence we have so far, from user-generated ad collection of 5 million ads by 10,000 Facebook users, suggests that 86% of the paid ads on Facebook in the last six weeks before the election were from suspicious groups (53.5%, of which 7.2% were later identified as Russian groups), astroturf movement groups (17.1%), and questionable news outlets (15.8%).

For a small fee, anyone can distribute content and generate impressions on social media. Using Facebook as an example, political ads, including disinformation ads, could be promoted, or boosted, for a fee, just like any other ad. Boosted ads appear higher on a user’s newsfeed. When boosting an ad, the creator selects which audience to target using filters like location, age, gender, or even interest. Some disinformation advertisers used Facebook’s “Custom Audiences” feature, which allows for much more sophisticated targeting than other methods, because it allows advertisers to place cookies on the browsers of those who click on their ads and then re-target people who clicked through. Russian meddlers used Custom Audiences to create websites and Facebook Pages with political sounding names that focused on socially divisive issues such as undocumented immigrants or African American activism. The operatives later

---


27 A group is coded as “suspicious” if its page was taken down by Facebook because it was linked to Russian ads or the Internet Research Agency, if its website “exists but shows little activity since Election Day and no information about the group exists elsewhere” or if its page is accessible, but there is no other information online about the group. The Russian groups were identified as such by Facebook and the House Intelligence Committee. Id. at 8.

28 The authors define these as groups that have not registered with the National Center for Charitable Statistics (NCCS), GuideStar, or the FEC.” Id.

29 These groups regularly produce “news, are “unaffiliated with any existing non-news groups such as a nonprofit”, “have little self-identification with a group” and “are often identified by a fact-check (e.g., PolitiFact, Factcheck.org, Snopes, Media Bias/Fact Check) or media watchdog organization (e.g., Media Matters for America) as a group generating false information (so called ‘fake news’)”.” Id.


re-targeted people who had visited their sites with further political messaging.\textsuperscript{33} The Trump campaign, itself, also used Custom Audience’s “diabolical little brother”, Lookalike Audiences, to target people that “look like” their custom audiences, based on their online habits.\textsuperscript{34} If the tools remain available to advertisers in future elections, it is likely that disinformation advertisers will use them in the future.

Russia also deploys tens of thousands of “sock puppets”, trolls, cyborgs, and bots to amplify and distribute their messages. Mass posting causes hashtags to trend, amplifying the bots’ messages.\textsuperscript{35} Social media users can easily build a large social media following using cheap third-party services to promote their Twitter or Facebook accounts.\textsuperscript{36} Helping distribute the propaganda are so-called “useful idiots”, American social media users who unwittingly support the Russian disinformation campaign by reacting to, commenting on, and sharing the sensational stories with their social media networks.\textsuperscript{37}

By now it should be clear that there is spending at many steps of this process, including whatever is spent in salaries and production cost to make the

\textsuperscript{33} Id. Facebook reported only one percent of the ads they turned over to Congress from the 2016 election used Custom Audiences. We do not know how many disinformation ads from other sources domestic or foreign, used it, and we do not know how common its use is now.


\textsuperscript{36} Ten thousand Twitter followers cost $39.89. Five hundred Facebook shares cost less than $25. See Buy Twitter Followers, SOZIALY, \url{https://www.sozialy.com/buy-twitter-followers/?gclid=EAIaIQobChMI956V9pfE1glVj4i-Ch1eNgf9EAAYASAAEgKwytD_BwE} (last visited Sept. 26, 2017); see also The Most Reliable Place to Buy Facebook Shares, Buy Real Marketing, \url{https://www.buyrealmktg.com/buy-facebook-shares} (last visited Sept. 26, 2017).

content in the first place. Once aggregate expenditures reach the threshold to trigger registration, the advertiser is subject to regulations like any other group regulated by the Federal Election Commission (“FEC”). While communications distributed on the Internet for free are generally exempt from FEC regulations, many political ads – including many disinformation ads – are placed into our newsfeeds for a fee and therefore subject to regulation under existing rules. We also know that some of the advertisers violated the ban on foreign expenditures in connection with a U.S. election, since they were paid for by foreign sources. In short, a lot of disinformation advertising is covered by our existing rules. The problem is retaining the content to enable enforcement, as we discuss in Part IV.

* * *

Media organizations are exempt from campaign finance regulations. Even if we are correct that “fake news” is better conceived of as advertising, is it also “news” that should be exempted from the rules? The FEC lacks a coherent regulatory approach to implementing the Federal Election Campaign Act’s (“FECA’s”) press (or “media”) exemption from campaign finance regulation. The exemption allows legitimate media sources to avoid registration with the FEC and compliance with campaign finance regulations. The Commission walks a tightrope in interpreting the exemption. If it defines “press” too broadly, the exemption will swallow the statute and allow all advertisers to claim exemptions as “press entities”. With an overly-narrow definition, the FEC would run afoul of the First Amendment by burdening the speech of the legitimate news media.

In determining whether an item should be subject to the press exemption, the FEC asks whether the entity is “a press entity”, and “whether [it] is acting in

38 See Statement of Vice Chair Ravel, FEC MUR 6729 (Checks and Balances), (Oct 24, 2014), p. 2, http://eqs.fec.gov/eqdocsMUR/14044363872.pdf. (“Since its inception, this effort to protect individual bloggers and online commentators has been stretched to cover slickly-produced ads aired solely on the Internet but paid for by the same organizations and the same large contributors as the actual ads aired on TV.”)
39 The Facebook Advisory Opinion has long been interpreted to allow an exemption from disclaimers under the “small items exemption”, though the FEC’s recent advisory opinion on the issue requires disclaimers for Facebook ads with express advocacy placed for a fee. FEC Advisory Op. 2017-12 (Take Back Action Fund), http://saos.fec.gov/aodocs/2017-12.pdf.
41 See, e.g., 52 U.S.C.A. § 30101(9)(B)(i) (exempting costs associated with producing news from the definition of “expenditure”); id. § 30101(4) (defining a “political committee” in terms of contributions collected and expenditures made); id. § 30120 (disclaimer requirements for political committees); id. § 30104 (disclosure requirements for political committees).
its legitimate press function." To determine whether a publication or organization is a press entity, the FEC asks “whether the entity in question regularly produces news stories, commentary and/or editorials.” When analyzing whether a press entity is acting “within its legitimate press function”, the FEC looks at (1) whether the entity’s materials are available to the general public, and (2) whether the materials are comparable in form to those ordinarily issued by the entity. The Commission does not analyze whether the materials are produced by trained journalists, whether the organization employs a fact checker or conducts fact checking functions, or any other typical indicia of a legitimate media organization. The test may be too lax: Because it does not consider indicia of traditional journalism when granting the exemption, the propaganda outlet of the Russian government, Russia Today, was deemed a “legitimate press entity” by the FEC.

Even under its minimal test, the FEC would not consider much of the disinformation on social media to be the product of a “press entity.” Take the Denver Guardian as an example. It existed only briefly before running a story about a murder-suicide committed by “an FBI agent believed to be responsible for the latest [DNC] email leaks”. Its registered address is actually a parking lot. The site had ads, Denver’s weather, and no more than two news stories during its entire existence. Similarly, Facebook Pages that disseminated content and memes, like the “Blacktivist” page, would not be considered press entities.

---

43 FEC Advisory Opinion 2016-01: Website’s distribution of news content to users qualifies for media exemption (2016); Reader’s Digest Ass’n v. FEC, 509 F. Supp. 1210, 1215 (S.D.N.Y. 1981).
46 The disinformation at issue is not “clickbait” headlines with spins on true (or mostly true) stories, like those from the partisan-leaning media. That speech, though biased, is protected. We are instead discussing complete political hoaxes like those that we saw in the 2016 election.
48 FBI Agent Suspected in Hillary Email Leaks Found Dead, summarized at https://www.snopes.com/fbi-agent-murder-suicide/.
49 Eric Lubbers, There is no such thing as the Denver Guardian, despite that Facebook post you saw, DENVER POST (Nov. 5, 2016), https://www.denverpost.com/2016/11/05/there-is-no-such-thing-as-the-denver-guardian/.
50 This is based on our research in the Internet Archive. http://web.archive.org/web/*http://denverguardian.com/
They were created in the months before the election and claimed to be activists, not journalists.

B. How Disinformation Can Weaken Democracy

Lack of transparency for online political advertising pre-exists the 2016 election, but the disinformation attacks have given the problem new urgency. Disinformation attacks threaten democracy, because:

Factual knowledge about politics is a critical component of citizenship, one that is essential if citizens are to discern their real interests and take effective advantage of the civic opportunities afforded them. . . . Knowledge is a keystone to other civic requisites. In the absence of adequate information neither passion nor reason is likely to lead to decisions that reflect the real interests of the public.\textsuperscript{51}

Disinformation advertising works like other kinds of propaganda.\textsuperscript{52} Here, the propaganda uses a fake media source to undermine trust in the media. The flood of false, hyperbolic, repetitive, and divisive information is difficult for its viewers to resist over time and can distort the information environment.\textsuperscript{53} Voters are left trying to select the candidate that is right for them, or to form opinions about policy, in the face of a “media firehose which has diluted trusted sources of information”.\textsuperscript{54} As Tim Wu explains, “[w]hen listeners have highly limited bandwidth to devote to any given issue, they will rarely dig deeply, and they are less likely to hear dissenting opinions. In such an environment, [information] flooding can be just as effective as more traditional forms of censorship.”\textsuperscript{55}

Scholars have argued that an informed electorate is a constitutional value and that we should recognize a canon of “effective accountability” which relies

\begin{footnotesize}
\begin{enumerate}
\item[54] Richard L. Hasen, \textit{Cheap Speech}, supra note 11.
\item[55] Wu, supra note \textbf{Error! Bookmark not defined.}, at 15.
\end{enumerate}
\end{footnotesize}
upon an informed electorate. Many voters are already poorly informed about the candidates and issues on the ballot, as well as more basic understandings of government structure and policies. Of course, uninformed voters are not unteachable: some studies show that providing voters with information increases voter competence, or their ability to vote in line with their preferences. More generally, voters have informational workarounds. They use heuristics, or informational shortcuts, to help them reach a decision. Uninformed voters can also take cues from elites they trust. If the heuristics they use, or the information coming from elites, are disinformative, voters are left worse off than if they had not paid attention in the first place. Corrections to disinformation do not help much, either. It is hard to “un-ring the bell” of misinformation – the effects of misinformation remain even after corrections are issued, and even when they are issued right away. Moreover, corrections can be misremembered and serve to further entrench the faulty information.

Disinformation campaigns share a targeting strategy with more run-of-the-mill political advertising on social media: microtargeting. Microtargeting small groups of voters with content that appeals to their pre-existing biases can...
deeper the democratic problem by subdividing the electorate, creating an endless number of potential cleavages among voters. As Elmendorf and Wood warn:

[I]t seems reasonable to fear that as broad, public appeals to the common good and national identity are supplanted by microtargeted appeals to the idiosyncratic beliefs, preferences, and prejudices of individual voters, voters will come to think of politics as less a common project than an occasion for expressing and affirming their narrow identities and interests. . . . Voters with out-of-the-mainstream and even abhorrent beliefs (such as overt racism) may find their beliefs legitimated and reinforced by micro-targeted messaging.62

Microtargeting stands to fragment the electorate into countless groups. When disinformation is microtargeted, each group has its own set of unreliable “facts” about our civic life. Moreover, because more extreme voters are more easily targeted for turnout or suppression, a vast, moderate, center is left out of the discussion of issues surrounding the election, undermining a key First Amendment value that campaigning enhances the “marketplace of ideas.”

Cass Sunstein proposes that a diversity of information and views are necessary to fix the problem of group polarization.63 But diversifying one’s information is harder than it seems, even if voters want to do so. Platform algorithms are designed to give users more of what they have liked in the past, creating so-called “filter bubbles”.64 The more frequently a social media user clicks on disinformation advertising or visits a hyperpartisan website, the more frequently similar content will be promoted on their Facebook newsfeeds or Internet search auto completions.65

In sum, disinformation hurts our democracy by undermining our faith in our institutions, weakening voter competence, and splintering the electorate. The nature of social media, with its affinity groups and algorithms, make it likely that disinformation will echo among one’s social media networks, and that countervailing information will not reach the user. The lack of transparency in online political advertising has long been a problem, and the recent disinformation attacks have made shedding light on online political advertising more urgent.

64 See Bakshy et. al, supra note Error! Bookmark not defined., at 1131.
65 See Silverman, supra note Error! Bookmark not defined.
2. FIRST AMENDMENT, POLITICAL SPEECH, AND CHOICE OF REGULATOR

Political opinions and information posted online are indisputably political speech, protected by the First Amendment. Activities that are less obviously “speech” have been constitutionalized by courts responding to deregulation activists using the First Amendment as a deregulatory tool. This includes political expenditures. The “constitutionalization” of campaign finance has implications for the scope of government involvement in regulating online political advertising, including disinformation advertising. Where our democracy and political discourse require intervention to ban or restrict speakers or their speech, government cannot intervene outside of a narrow set of circumstances. Government regulation of online political advertising, including disinformation advertising, is on firmest constitutional ground when it requires disclosure of who is speaking to whom, when, and about what. The remaining responsibility for reducing disinformation on social media undoubtedly falls to the social media platforms. Here’s the rub: however much the platforms claim they want to self-regulate, their short term profit motives suggest they would be, at best, an unreliable and inconsistent regulator.

Here, we explain the current state of play in First Amendment jurisprudence and discuss the merits of platform self-regulation and government regulation.

A. Constitutional Framework for Campaign Advertising Regulation

First Amendment protections for political speech are strong in the United States, enhanced by conservative-libertarian rhetoric among First Amendment scholars. The courts apply strict scrutiny to content regulation of political speech. Several legislative attempts to regulate the content, amount, or source of political speech have met their demise under this standard. In order to survive strict scrutiny, the government must show that the regulation is necessary to serve a compelling state interest and is narrowly drawn to achieve that end. Preserving fair and honest elections and preventing foreign influence in our elections are

---

67 See, R.A.V. v. City of St. Paul, 505 U.S. 377, 382 (1992) (“The First Amendment generally prevents government from proscribing speech, or even expressive conduct, because of disapproval of the ideas expressed. Content-based regulations are presumptively invalid.”) (internal citation omitted); see also 281 Care Comm, supra note 69.
compelling government interests.\textsuperscript{69} The court has not elevated the government interest in preventing fraud on the electorate to the status of “compelling interest”, but it has said that the interest “carries special weight during election campaigns when false statements, if credited, may have serious adverse consequences for the public at large.”\textsuperscript{70} There is no federal precedent directly on point as to whether government can regulate fraudulent political speech with a narrowly tailored law.\textsuperscript{71} A narrowly-tailored prohibition on fraudulent online political speech could survive constitutional scrutiny where prior prohibitions on fraudulent speech have failed. In the cases it has faced so far, the court has said that the answer to false speech is not a blanket rule either allowing or prohibiting censorship. Rather, the answer to false speech is counter-speech.\textsuperscript{72}

Where the government regulation falls short of a ban or a limit, as is the case with campaign finance disclosure and disclaimer regulations, it is subject to exacting scrutiny. To survive exacting scrutiny, the government must identify an overriding\textsuperscript{73} or sufficiently important\textsuperscript{74} government interest, which is


\textsuperscript{70} McIntyre, supra note Error! Bookmark not defined., at 349.

\textsuperscript{71} We do not need to regulate fraudulent political speech for our proposed regulations; we merely note that the question is an open one. The 8th Circuit struck down a regulation as being overbroad, and it specifically declined to decide whether preventing fraud on the electorate is a compelling government interest. See 281 Care Comm. v. Arneson, 638 F.3d. 621 (8th Cir. 2011), cert denied 133 S. Ct. 61 (2012) (“Today we need not determine whether, on these facts, preserving fair and honest elections and preventing fraud on the electorate comprise a compelling state interest because the narrow tailoring that must juxtapose that interest is absent here.”). U.S. v. Alvarez, 567 U.S. 709 (2012), is often cited for the proposition that government cannot regulate fraudulent political speech. In Alvarez, the speech at issue was Alvarez’s misrepresentation that he had won the Congressional Medal of Honor. It was not campaign related speech. If Alvarez’s fraudulent speech was deemed protected by the Supreme Court, it is possible that fraudulent speech that is more directly political, like disinformation advertising about campaign-related issues, would also be protected, but the result is not inevitable. The degree of harm, which here is very high, is a crucial consideration in the inquiry. See Rebecca Brown, The Harm Principle and Free Speech, 89 S Cal L Rev 953 (2016).

\textsuperscript{72} Alvarez, supra note Error! Bookmark not defined., at 718, 726 (“Some false speech may be prohibited even if analogous true speech could not be. This opinion does not imply that any of these targeted prohibitions are somehow vulnerable. But it also rejects the notion that false speech should be in a general category that is presumptively unprotected.”)(“ The remedy for speech that is false is speech that is true.”). Of course, with regard to some efforts to reduce false speech, if the platforms do not act, government cannot step in. For example, the government may be able to require that platforms use neutral fact checkers, but it probably could not perform the fact-checking function itself or specify which fact checkers the platforms should use.


\textsuperscript{74} Citizens United, supra note Error! Bookmark not defined., at 339.
substantially related, or even narrowly tailored to meet it. The primary government interest supported by the disclosure regulations the court upheld *Citizens United*, *McConnell*, and *Buckley* is the “informational benefit”, which is about improving voter competence, by “[e]nabling the electorate to make informed decisions and give proper weight to different speakers and messages”. The *Buckley* court also mentioned disclosure’s aid in enforcing campaign finance laws as a government interest. Our transparency-related proposals should survive exacting scrutiny.

The right to free speech can bump up against the government interest in integrity of elections, which may provide an opening for government regulators. Government can regulate foreign-sponsored express advocacy, contributions, and expenditures, whether or not they contain disinformation. In the Bluman case, the Supreme Court has voiced strong views that the government has a compelling interest in limiting direct campaign contributions by foreign nationals, but the language is somewhat uncertain about other involvement of

---

75 *Buckley*, supra note 56 at 64.
76 McIntyre v. Ohio Elections Comm’n, supra note *Error! Bookmark not defined.*, at 347.
78 The cases also involved discussion of other interests, such as the government’s interest in preventing corruption or its appearance, and the government’s interest in enabling enforcement of the campaign finance laws. *Citizens United*, supra note 56 at 364, *McConnell*, supra note 56 at 201; *Buckley*, supra note 56 at 64.
79 One of us also has argued elsewhere that courts should recognize the government's interest in securing the data necessary to evaluate its own campaign finance policies as a justification for disclosure policies. Without knowing who is contributing and spending in campaigns, the government cannot know the distributional effects of policy changes. *See* Douglas M. Spencer & Abby K. Wood, *Citizens United*, *States Divided: An Empirical Analysis of Independent Political Spending*, 89 Ind. L.J. 315, 330 (2014).
foreign nationals.\textsuperscript{81} Speech around elections is fairly closely regulated.\textsuperscript{82} In many parts of the country, polling places require a physical setback for political activities, with campaign signs, protests, and clothing that advocates for a candidate or initiative banned near polling places.\textsuperscript{83} Protecting the integrity of the election is an “obviously” and “indisputably” compelling state interest, which has justified restrictions on our right to political speech in physical proximity to an election place.\textsuperscript{84} Similarly, temporal proximity to elections is important, especially in the disclosure and disclaimer context. Disclosures are required more frequently as elections approach, and the “electioneering window” opens, and the list of categories of political advertisements that require disclaimers expands.\textsuperscript{85} Even under the existing jurisprudence, there may be leeway for government to force more stringent regulations on platforms as elections approach.

While we have less guidance on other potential government actions we propose, we believe that the courts should uphold government efforts to educate voters and social media users about disinformation and fact-checking. Similarly, we believe the courts would uphold a regulation requiring platforms to provide an opt-in or opt-out system allowing social media users to control whether they view content previously flagged as false.\textsuperscript{86}

\* \* \*

Under the existing jurisprudential framework, government’s main involvement to combat disinformation advertising will be related to transparency. But it may be time to re-visit the foundations of our First Amendment jurisprudence. The cases fleshing out First Amendment protection of political speech are a relatively late addition to our constitutional

\textsuperscript{81} The prohibition upheld in Bluman was interpreted to exclude issue advocacy by foreign nationals. Bluman, supra note 80 at 284.


\textsuperscript{84} See Burson v. Freeman, 504 U.S. 191, 199 (1992). By the time this Article is in print, the Supreme Court may have decided a Minnesota case challenging Burson. Minn. Voters All. v. Mansky, supra note Error! Bookmark not defined..


\textsuperscript{86} For more on the constitutionality of an opt-in or opt-out requirement, see Elmendorf & Wood, supra note 62 at 40 (“Also pertinent is Sorrell v. IMS Health, Inc., which invalidated a consent-to-use-of-personal-data requirement that disfavored particular speakers and types of speech. The consent requirements we propose would be viewpoint neutral, but they would disfavor a kind of speech (micro-targeted political advertising), and they advance only a limited privacy interest.”)
jurisprudence, and like all law, they were created in a specific historical context. The jurisprudence developed at a time when listeners were plentiful and speech less so. Recent Supreme Court majorities have interpreted the Amendment to protect speakers, not listeners. Our transparency proposals fit the existing framework comfortably. But should government be able to do more to protect listeners from the “flood” of disinformation advertising before elections?

The Internet platforms themselves lack a coherent theory of the First Amendment. Platforms are not merely a venue for debates in the “marketplace of ideas”, in which truth can eventually win out. The truth stands little chance against the volume of disinformation advertising and other false political messaging that flooded the “marketplace” in the weeks leading up to the 2016 election. Nor are the platforms exclusively supportive of speakers’ personal autonomy to say whatever they want, another theory of the First Amendment. Terms of service of even the most libertarian platforms forbid behavior that is offensive, but not illegal. Platform users are speakers and listeners; and platforms should want to balance their interests, but only speakers pay them. The platforms also have not taken a collectivist, or deliberation-enhancing approach to speech on their platforms, under a theory that the First Amendment should promote political engagement and public discourse. At best, they have adopted an inconsistent amalgam of these ideas.

As Volokh explains, with the advent of “cheap speech” online, intermediaries are weakened. Speakers, freed from editorial gatekeeping, have

---

87 Tim Wu, Is the First Amendment Obsolete?, Emerging Threats: The Knight First Amendment Institute at Columbia University (Sept. 2017), https://knightcolumbia.org/sites/default/files/content/Emerging%20Threats%20Tim%20Wu%20on%20the%20First%20Amendment%20Obsolete.pdf (“As scholars and historians know well, but the public is sometimes surprised to learn, the First Amendment sat dormant for much of American history… As the story goes, the First Amendment remained inert well into the 1920s.”)


89 False information reaches more people than true information, and it spreads faster. Political disinformation spreads even faster than other kinds of false news. See Soroush Vosoughi, Deb Roy, and Sinan Aral, The spread of false and true news online, 359 Science 1146, 11467-1151 (2018).


91 Syed, supra note 88, at 342-345.

become less trustworthy. Listeners are better able to select speakers that affirm, rather than challenge, their ideologies; and political advertisers are better able to target them “to make arguments to small groups that they would rather not make to the public at large.”

Tim Wu argues that First Amendment jurisprudence should adapt to our current conditions, in which speakers are plentiful and listeners receive so much messaging that it is harder for speakers to “break through” than ever. In the age of cheap speech, the flood of disinformation advertising distributed by bots works to dilute human political speech, biasing the playing field in favor of machine-generated echoes of highly amplified, reckless, or even malevolent, speakers. Policing non-human speakers would help to promote a “robust speech environment surrounding matters of public concern.”

This collectivist-oriented shift would allow for government to at least backstop the platforms in their efforts to root out disinformation advertising.

Like Hasen, we see that a headwind may be building against government regulation requiring transparency of online political advertisements, even where the regulation would stop disinformation. Nevertheless, prior libertarian efforts to build a case of “substantial overbreadth” did not have the facts that we now have, since the 2016 election. Regulators can now show demonstrable damage, intent by meddlers (both foreign and domestic) to mislead and to affect elections; and involvement by two entities with little to no First Amendment protection: foreigners and non-humans.

93 Id.
94 Wu, supra note 87.
95 Id. Wu also says that the “captive audience” doctrine might be extended into the social media realm to provide a rationale for new regulation to protect listeners. The opt-in / opt-out provisions we discuss in Part IV aim at not having a captive audience for disinformation. The existence of the opt-in / opt-out provision would therefore slightly weaken the government’s case in defending its regulation, to the extent that the “captive audience” line of cases would be seen to apply to disinformation advertising. Nevertheless, we think the benefit offered to voters from regularly being reminded they can opt in or out of seeing disputed content far outweighs the risk that a court might use the provision against the state in defending regulations.
96 Hasen, Cheap Speech, supra note 11, at 19-23.
97 Not only was the flood of disinformation damaging in itself, but disinformation caused real-world damages as well. One serious event was the so-called “Pizzagate” scandal, in which disinformation advertising spread a rumor that a pizza shop had a Clinton-run pedophilia ring in it. The shop’s business was hurt and its owners were harassed for months.
98 These are serious harms. See generally Brown, supra note 71. Bots are essentially code, and whether code is speech is not yet clear (see Neil Richards, Apple’s “Code = Speech” Mistake, MIT Technology Review (2016), https://www.technologyreview.com/s/600916/apples-code-speech-mistake/ (arguing that the Government can and should regulate bots, as distinct from
B. Choice of Regulator

Negative market externalities justify regulation. We usually think of market externalities as related to negative effects on our environment or public health born of market activity – say, from air pollution. Here, the market activity is platforms chasing profits without exercising any gatekeeping or transparency responsibilities, and the externality is a cost born by social media users in their roles as voters and participants in civic life. The platforms have so far not internalized the cost that their ad placement systems impose.

Here we discuss the relative merits of industry self-regulation and government regulation, each within their own constitutionally permissible spheres of action.

Industry Self-Regulation and Co-Regulation

It is not a forgone conclusion that government must be the main regulator to address the disinformation advertising problem. Platforms have long resisted government regulation. Nate Persily has argued that “the principal regulator of political communication will not be a government agency but rather the internet portals themselves.” 99 The platforms are certainly well-situated to use the technological tools at their disposal to minimize the amount of disinformation advertising that reaches their users. Facebook and Twitter were the locations of most of the “attacks” in the 2016 election, and so we focus on them here. After dragging their heels, 100 both companies have taken halting steps to prevent future attacks, 101 actions that are also aimed at heading off government regulation. The platforms have also continued to experience disinformation attacks.

The platforms suffer from conflicts of interest and political vulnerabilities that push them away from strong action to combat the problem. Platforms make money from advertising, including disinformation advertising. The more ads they sell, the more content that is promoted on their platforms, the

---


100 Persily, supra note 99.

101 See infra, Part Error! Reference source not found.
scarcer the space for ads, and the more they can charge per ad. The more users
that click through on any pay-per-click ad, the higher the platforms’ ad
revenues. Disinformation advertising headlines are refined to attract the most
clicks, accruing money for the platforms in the process. The presence of bots and
other non-human accounts inflates the number of users on the platforms,
increasing the amount they can charge to sell ads to all users, not just to foreign
interlopers in our democracy. While bots and disinformation advertising can
degrade the user experience and damage long-term revenues of the platforms,
their short-term bottom line increases because of advertising and inflated user
counts.

Platforms are also politically vulnerable. After Mark Zuckerberg initially
announced the self-regulatory measures Facebook plans to take, within a week,
he had softened his stance and begun to “both sides” the issue, saying “[b]oth
sides are upset about ideas and content they don’t like.” Professor Zeynep
Tufekci, who researches online disinformation and authoritarianism, was quick
to point out that his reaction reflected a common fear of social media companies:
that they be depicted as “anti-conservative.” In other words, the social media
companies will feel pressured to over-correct: Even though the disinformation
advertising that currently circulates online is overwhelmingly anti-liberal or pro-
conservative, the political vulnerability of the platforms means that they will
under-address the problem. Their political vulnerability leads them to be an
unreliable self-regulator.

To the extent that the platforms do self-regulate – and in some aspects of
fake news, the platforms are the only constitutionally permitted regulator – they
are still far from the typical model of industry self-regulation or co-regulation.
Industry self-regulation requires an industry-level organization that regulates its
members by setting rules and standards about how they should conduct their
business. Industry self-regulation is almost never “pure” self-regulation but
involves a nexus to a government regulator. It is better conceived of as co-
regulation in many instances, with government agencies providing legal

---

102 See Facebook Business, Creating Ads, Is there a minimum cost per click (CPC) bid?,
FACEBOOK, https://www.facebook.com/business/help/176506602405065 (last accessed October
5, 2017).
103 Zeynep Tufekci, Opinion, Zuckerberg’s Preposterous Defense of Facebook, N.Y. TIMES,
104 Id. See also Nicholas Thompson & Fred Vogelstein, Inside the Two Years that Shook
Facebook – and the World, WIRED (Feb. 12, 2018), https://www.wired.com/story/inside-
facebook-mark-zuckerberg-2-years-of-hell/
105 Lisa L. Sharma, et. al, The Food Industry and Self-Regulation: Standards to Promote Success
and to Avoid Public Health Failures. 100.2 AM. J. OF PUB. HEALTH 240 (2010), (citing Neil
Gunningham & Joseph Rees, Industry Self-Regulation: An Institutional Perspective. 19 L. POL’Y
363 (1997)).
backstops and imposition of civil or criminal penalties.\textsuperscript{106} Co-regulation stands the best chance of success when certain conditions exist. Most importantly, the industry actors must be committed to the purpose of the regulation. Private regulators set up in a co-regulatory framework require the state to provide “clear missions, and then maintain a close watch” over the private regulators.\textsuperscript{107} The government must also be able to extract information from industry – here, the platforms – as to how the self-regulation efforts are succeeding. The state also requires both “expertise and capacity to assess the performance of nongovernmental regulators; and those nongovernmental regulators must face a credible threat that their public overseers will assume regulatory jurisdiction if they do not meet their obligations.”\textsuperscript{108}

An analogy to co-regulation by an industry group closely related to the issue at hand my help to illustrate what industry self-regulation looks like when it has the backing of government regulators. The Digital Advertising Alliance runs an opt-out program from advertisements based on cookie-tracking.\textsuperscript{109} The industry enforcement process consists of confidential review of complaints by a committee, followed by a board-level censure, membership suspension or expulsion, referral to the Federal Trade Commission (“FTC”) or law enforcement, and publicity for non-compliance.\textsuperscript{110} By comparison, the platforms’ initial offerings to address the problem of disinformation advertising are paltry. It took Facebook over a year to even suggest it would be reaching out to other companies to “share information on bad actors and make sure they stay off all platforms.”\textsuperscript{111} We are a long way from effective and comprehensive industry self-regulation or co-regulation.

\begin{footnotesize}
\textsuperscript{106} Gunningham & Rees, \textit{supra} note 105.
\textsuperscript{108} Id.
\end{footnotesize}
Government Regulation

Government regulation is coordination-facilitating and symbolically important. It facilitates coordination between industry members in mundane, but important, ways. For example, government can require uniform information to be collected and provided in a uniform format. Standardized reporting allows the public, watchdog groups, journalists, and scholars to compare across platforms and over time in their analysis of data. Moreover, shared information across platforms would be useful for platforms wanting to ban identifiable bad-actors who use the same accounts to buy, place, and promote ads. Government regulations also facilitate coordination through disclosure and audits to ensure compliance.

Government action in the realm of online political advertising is also symbolically important. In areas of national security and elections, signaling matters. The fact that our government has been so quiet in the face of disinformation advertising, in particular, sends a signal to the attackers and to the public. The attackers – domestic and foreign – receive the message that no one is policing our campaigns, and they can continue to spread disinformation, sow division, and profit with impunity. The public receives the message that the government does not take the problem seriously enough to act.

Government regulation also matters because law has expressive value. Law itself has special gravity, and adopting a policy into law signals the importance of the policy to the government. Codifying a policy can affect citizen expectations and behavior. It also signals that all members of a regulated industry must play by the same rules, an important rule-of-law value. In deciding on a regulatory approach, policymakers should keep in mind that policy choices do not just bring about certain immediate material consequences; they also will be understood, at times, to be important for what they reflect about various value commitments – about which values take priority over others, or how various values are best understood. Both the material consequences and the expressive consequences of policy choices are appropriate concerns for policymakers.


114 Pildes and Sunstein, supra note 112.
Therefore, even in areas of regulation where the industry could self-regulate (or co-regulate with government), sometimes the government should still act to signal its seriousness in protecting important values.

Government is constitutionally prohibited from anything resembling censorship, and moreover, the platforms are in a better position to experiment with interventions that shift the incentives of producers and consumers of fake news. Nevertheless, where, as here, the platforms’ incentives and the public’s social welfare are misaligned in a way that would prevent the platforms from self-regulating (or prevent them from credibly committing to a self-regulation scheme), government should do what it can within constitutional limits, to help re-align actors’ incentives.

All of this political disinformation flooded into social media at a time when the FEC lacked an effective framework for regulating any political advertising online, regardless of content. When political advertising occurs on television, cable, satellite, and radio, government disclosure requirements are comprehensive, and compliance is high. Due to gaps in the regulatory regime and clever lawyering by political attorneys, the same advertisement that would be subject to disclaimer and other transparency requirements on television can go without them if it instead appears online. We explain these gaps in Part 3.
3. OUR CURRENT, INSUFFICIENT, REGULATORY FRAMEWORK FOR ONLINE POLITICAL ADVERTISING

In the years leading up to the 2016 election, voters heard about the inadequacy of the federal campaign finance regulatory framework to handle the coming flood of money and advertising, both online and off. Insiders, such as former FEC lawyers quoted in the media, called campaign finance in the United States “the Wild West” and reported that “[c]andidates and political groups are increasingly willing to push the limits . . . and the F.E.C.’s inaction means that there’s very little threat of getting caught.” All of the regulatory and institutional weaknesses that drove this kind of reporting are even more extreme in the narrow regulatory regime we consider here – that of online advertising.

Online political advertising differs from older forms of political advertising in important ways and deserves a regulatory framework that accounts for the differences. Online political advertising is more likely to be “native” advertising, more likely to contain disinformation, more likely to be untraceable (preventing counter-speech), and much cheaper. In this Part, we describe the regulatory framework and its gaps.

“Public communications” and ad retention. Most FEC transparency requirements attach to “public communications”. Public communications include messages displayed on broadcast television, in print, on billboards, etc. It also includes all committee websites and emails whenever a committee sends more than 500 “substantially similar” messages. Importantly, the current definition excludes Internet ads “except for communications placed for a fee on another person’s or entity’s website”.

In order to aid enforcement on broadcast, cable, satellite, and radio ads, the Federal Communications Commission (“FCC”) requires reporting of the financial details of the transaction as well as the station, time, and programming during which the ad ran. The ads themselves, while not required to be retained by broadcasters, are captured by the public in all the ways the public records live programming. There is currently no requirement at the federal level that online political ads or the data around their placement be retained, making enforcement virtually impossible.

Disclaimers. The law requires disclaimers for many kinds of political advertisements. They say “Paid for by the XYZ State Party Committee and authorized by the Sheridan for Congress Committee”, or “Paid for by the QRS Committee (www.QRScommittee.org) and not authorized by any candidate or candidate’s committee.” On broadcast, cable, and satellite political messages, the FEC requires disclaimers on all public communications (1) made by a political committee (2) that expressly advocate for the election or defeat of a “clearly identified” candidate (3) that solicit contributions. They are also required on (4) electioneering communications, which are publicly distributed communications that refer to a “clearly identified candidate for Federal office” and are distributed 60 days or fewer before a general election 30 days or fewer before a primary (electioneering communications). In translating these four disclaimer triggers to Internet communications, regulatory coverage decreases substantially. The first three triggers, for political committees, express advocacy, and solicitations, apply only where the communication is “placed for a fee.” The fourth, electioneering communications, is completely inapplicable, because electioneering communications are defined to exclude political messaging on the Internet.

As noted in Part 1, in the weeks leading up to the election, well within the electioneering communications window, disinformation ads explicitly naming presidential candidates generated more attention than news articles from leading national newspapers. Among the disinformation ads that did not expressly advocate for the election or defeat of a candidate, many still mentioned candidates by name or showed their images. Were they on broadcast, satellite, or cable, our regulations would have required disclaimers as electioneering communications.

---

120 11 C.F.R. 100.26 (2017) (“Public communication means a communication by means of any broadcast, cable, or satellite communication, newspaper, magazine, outdoor advertising facility, mass mailing, or telephone bank to the general public, or any other form of general public political advertising. The term general public political advertising shall not include communications over the Internet, except for communications placed for a fee on another person's Web site.”); 11 C.F.R. 110.11(a) (2017) (defining the scope of disclaimer requirements as limited to public communications as defined in 11 C.F.R. 110.26 (2017) and electioneering communications – which are defined in 11 C.F.R. 100.29(c)(1) (2017) to exclude communications over the Internet).
121 11 C.F.R. § 100.29(a), (a)(1)-(2) (2017).
communications. They were placed online, and so we do not know who paid for them.\footnote{122}{See 11 C.F.R. § 100.29(c) (2017).}

In sum, a paid ad distributed via social media (on the Internet) must carry disclaimers like any other public communication if it advocates for the election or defeat of a clearly identified candidate. However, anything posted for free, like a blog post, a Tweet, or even disinformation that one generates personally from their personal profile or page, requires no disclaimer, even if it mentions a candidate by name right before the election, and even if it is amplified by a paid “bot army” or purchased “shares” on Facebook.

Many communications placed online for a fee – which would otherwise require disclaimers – have not had them. Presumably, the advertiser would claim an exemption under the “small items” or “impracticable” exceptions to disclaimer requirements.\footnote{123}{11 C.F.R. § 110.11(f)(1)(i)-(ii) (2017).} The small items exception applies to communications on physical items, such as bumper stickers, buttons, and pens, which were considered too small to bear a disclaimer.\footnote{124}{See 11 C.F.R. § 110.11(f)(1)(i) (2017).} The impracticable exception applies to communications in skywriting, water towers, and clothing, where it would be too difficult to include a disclaimer.\footnote{125}{See 11 C.F.R. § 110.11(f)(1)(ii) (2017).}

Because of landing pages on click-through political advertisements, it has never truly been impracticable for an advertiser to provide a disclaimer. They could always have provide one at the landing page. That fact did not stop platforms from asking the FEC whether the exceptions apply to character-limited ads on their platforms. In 2011 the FEC could not decide whether Facebook ads with less than 200 characters of text could qualify under either exception,\footnote{126}{FEC Advisory Op. Request 2011-09 (Apr. 26, 2011), http://saos.fec.gov/aodocs/1174825.pdf; Certification of Vote for FEC Advisory Op. 2011-09 (June 15, 2011), http://saos.fec.gov/aodocs/1176290.pdf; FEC Agenda Document No. 11-32 (June 15, 2011), http://saos.fec.gov/aodocs/1176195.pdf.} a 3-3 vote that was long interpreted as an exemption.\footnote{127}{Google’s AO request did propose a disclaimer on a landing page. FEC Advisory Op. Request 2010-19 (Aug. 5, 2010), http://saos.fec.gov/saos/searchao?AONUMBER=2010-19.} The commission has recently clarified that a disclaimer is required, but they could not agree on the rationale.\footnote{128}{FEC Advisory Op. 2017-12, \textit{supra} note 39.}
The FEC has also recently failed to decide whether nonconnected political committees\footnote{129}{Nonconnected committees are a class of committees that includes Leadership PACs and SuperPACs. \textit{Types of Nonconnected PACs}, \textit{Fed. Election Comm’n}, https://www.fec.gov/help-candidates-and-committees/registering-pac/types-nonconnected-pacs/ (last visited Oct. 2, 2017).} may use Twitter without placing a disclaimer on their Twitter
This opinion gives the green light to groups that want to hide behind Twitter handles and not reveal even the group’s website or physical address.

**Disclosure.** In addition to gaps in our disclaimer requirements, our disclosure rules are also fraught with holes and exceptions that have led to untraceable money pumping through our elections. Campaigns, party committees, and PACs must all submit regular reports to the FEC, disclosing their contributions and expenditures. However, since *Citizens United* over half a billion dollars has flowed through 501(c) tax-exempt non-profits, which are typically organized as 501(c)(4) or 501(c)(6) "social welfare" organizations, to make independent expenditures or support groups who do. These “dark money” groups are not required to publicly disclose their donors. Funds can be donated to 501(c)'s by individuals, corporations (including LLCs), unions, and anyone seeking anonymity – including foreign sources. (Foreign spending “in connection with an election” is illegal but would be easy to do via these avenues, as we discuss below.)

The groups do disclose their contributions to the IRS. But with an audit rate of 1% for tax-exempt non-profits, the IRS is unlikely to investigate the sources behind donations to so-called “dark money” organizations, even where...
they use their resources to spread disinformation.\textsuperscript{136} Congress has prohibited the Securities and Exchange Commission and from using appropriated funds to draft or implement rules requiring the corporations it regulates to disclosure political spending.\textsuperscript{137}

\textit{Foreign influence.} Some political disinformation ads may also violate the FEC’s ban on spending by foreign nationals “in connection with any federal, state, or local election in the United States” and making any disbursement for an electioneering communication.\textsuperscript{138} The restriction was upheld in \textit{Bluman v. Federal Election Commission}\.\textsuperscript{139} At least some disinformation ads violate the ban on foreign spending for independent expenditures. Independent expenditures advocate for the election or defeat of a “clearly identified candidate” in express terms.\textsuperscript{140}

Of course, some disinformation ads are merely “issue ads”. They seek to influence voters by shifting public perception but do not advocate for the election or defeat of any particular candidate or even mention a candidate. Under our current regulatory framework, a hostile foreign government can potentially disseminate divisive information about fraught social issues or spread disinformation about a candidate without violating American campaign finance law, even if they are placed right before the election.\textsuperscript{141}

To summarize: because of outdated loopholes, we face the reality that disinformation advertisements, which often mention or display candidates and would be considered electioneering communications if placed elsewhere, are distributed online with no regulation, no disclaimers, little disclosure, and sometimes using foreign money. Online advertising has become exponentially more important for political campaigns since the FEC adopted its outdated regulations in 2006, and it will become the most important way for politicians to

\textsuperscript{137} Consolidated Appropriations Act, H.R. 244, § 635 115\textsuperscript{th} Cong. (2017). A similar prohibition exists for IRS.
\textsuperscript{138} 11 C.F.R. §110.20(f) and 11 C.F.R. §110.20(e) (2017)
\textsuperscript{140} 11 C.F.R. § 100.16 (2017).
communicate with voters in the very near future. Excluding a large portion of online advertising from disclosure and disclaimer regulations is both problematic and unsustainable.

4.  **CONSTITUTIONALLY-PERMISSIBLE REGULATIONS TO ADDRESS DISINFORMATION ADVERTISING**

We now turn to our proposals. Our primary focus is on transparency, education, and “nudges” that government can constitutionally implement. The reforms we propose would reach any advertising that is placed for a fee or placed for free and promoted or produced for a fee, whether disinformative or not. Viral disinformation without paid shares or re-tweets, memes made by individuals at home for free and posted to personal social media sites, and similar low-cost and low-volume activity, would not be subject to the regulations we propose.

We recognize that defining which advertisements deserve regulation is a persistent and sticky problem in campaign finance regulation. Our definition has two main components: cost and intent to influence peoples’ votes. Political ads cost money to produce, post or dissemiante, including payments for microtargeting and any off-platform payments to “bot farms”, paid “likes” and “shares” for distribution. Political ads also aim to influence the election. Evidence that an ad aims to influence the election, rather than merely discuss “issues” is particularly thorny category. The current line between an ad aiming to influence the election and one merely discussing “issues” includes “express advocacy” or, within a certain window before the election, reference to a clearly identified candidate. This line is hard to police, and it also may be meaningless in the online setting, in which an ad can persist over time.

An example may help to illustrate the definitional challenge. Suppose that a group called “Liberals Against Forced Motherhood” has spent more than the minimum threshold on political advertising and is registered with the FEC. Consider three scenarios.

1. Suppose the group posts a meme online and pays Facebook to promote it in the newsfeeds of its followers. The text of the meme says “Hands off our birth control!” With no other words or imagery, this would be considered an issue ad under the current rules, no matter when it runs, and it would not require a disclaimer.

---

2. Now suppose the group posts the meme and pays Facebook to promote it in the newsfeeds of its followers, and the text of the meme overlays a photograph of a Republican presidential candidate. Under the current rules, that advertisement would not be subject to disclaimer requirements unless it ran right before the election, during the “electioneering communications” window, because the photograph shows a “clearly identified candidate”. Of course, given the nature of social media, it can be posted well before the “electioneering communications” window opens, and members of the group can continue sharing and circulating it, disclaimer-free, right before the election.

3. Finally, suppose the group posts a meme online and pays Facebook to promote it in the newsfeeds of its followers, and the text of the meme says “Hands off our birth control! Vote against Candidate X!” Under the current rules, this meme will require a disclaimer no matter when it is posted, because it contains “express advocacy”.

Now change the facts. What if the meme is posted “for free” on the group’s Facebook page, and fake Facebook users have been paid, off-platform, to share it? The group does not pay Facebook for promotion, but the ad circulates, nevertheless. The current rules have been interpreted in a way that would not require disclaimers on any of them, but we believe this interpretation, made in the days before bots and fake “shares” should be updated to account for our new reality.

Finally, consider one more distributional change. Suppose now that, instead of paying Facebook to promote only to page subscribers, the group pays Facebook to promote the ad to anyone who “looks like” their subscribers and any women who are between the ages of 18-45, who have a college education, who are white, who “like” Planned Parenthood, and who live in swing states? Does this kind of micro-targeting turn the issue ad in the first scenario into a political ad? We think it does – particularly the “swing state” targeting. Even if disclaimers should not be required, the ad itself should be retained so that targeted users can know who is attempting to persuade them.

These are difficult questions that we grapple with more below. When most ads were limited in time and larger groups of the electorate were targeted, it was understandable that there was a limitation on electioneering ads in order to permit true issue related speech. In light of the realities and challenges of political advertising online, issue speech has become so politicized and so microtargeted that we need to have a national conversation on where to draw the line.

Our proposal follows. It is modest, it is constitutional, and it will not solve the problem of online disinformation. It is, however, a necessary and important step in the right direction. After discussing our proposal, we briefly provide self-regulatory considerations for platforms wanting to take real steps to reduce the quantity of disinformation advertising on their platforms.
A. Improve Transparency

Without transparency, we cannot “follow the money” behind political advertising we see online. Most relevant to the world of disinformation advertising, we cannot know how much of the messaging we see online is foreign-funded or distributed. It took almost a year for Facebook to make public some of the foreign-funded ads it displayed to its users. If online advertising, including disinformation advertising, were subject to transparency regulations, we would have seen them in real time.

In order to subject online political advertising to disclaimer and disclosure requirements, the groups producing large amounts of it should be required to register with election administrators, just as they do when they make political expenditures offline. Because advertising on social media is so inexpensive, regulators should carefully consider the appropriate threshold of aggregate spending to trigger a group to register with regulators.\textsuperscript{143}

As the Supreme Court has repeatedly acknowledged since \textit{Buckley v. Valeo}, accurate and timely disclosures serve an important informational role in our democracy. As the \textit{Buckley} court said,

\begin{quote}
...[D]isclosure provides the electorate with information as to where political campaign money comes from and how it is spent by the candidate in order to aid the voters in evaluating those who seek federal office. It allows voters to place each candidate in the political spectrum more precisely than is often possible solely on the basis of party labels and campaign speeches. The sources of a candidate's financial support also alert the voter to the interests to which a candidate is most likely to be responsive, and thus facilitate predictions of future performance in office.\textsuperscript{144}
\end{quote}

\textsuperscript{143} We discussed the media exemption in Part 2, \textit{supra}, but we reiterate here that Facebook Pages and fake newspapers like the nonexistent “Denver Guardian” do not qualify for the media exemption.

\textsuperscript{144} Buckley, \textit{supra} note 56 at 66-67. While some of its opinions upholding disclosure have turned on the anti-corruption rationale, the court has remained convinced of the informational benefits of disclosure in the intervening 40 years. \textit{See, e.g.,} the majority opinion in \textit{Citizens United}, which emphasizes that the information provided by disclosure is even more powerful in the age of the Internet, “because modern technology makes disclosures rapid and informative,” and that “this transparency enables the electorate to make informed decisions and give proper weight to different speakers and messages.” \textit{Citizens United, supra} note 56 at 364.
Political scientists have shown that campaign finance transparency affects voter opinion. Adam Bonica has shown that campaign finance contributions are as strong of a predictor of legislative behavior – as informative, in other words – as incumbent legislators’ prior votes. We also know that voters demand disclosure and learn from a group or candidate’s decision to not disclose.

Scholars and activists have written about ways to enhance the effectiveness of donor disclosure to the public, from formatting changes, to including names of the top donors in disclaimers, to closing the Internet and corporate independent expenditure disclaimer and disclosure loopholes. Legal scholars have pushed for more elaborate disclaimers. Levitt proposes that disclaimers resemble the Nutrition Facts label on packaged food. The State of Montana adopted a disclaimer that included information about whether the ad sponsor chose to disclose its donors or not.

As more political advertising moves online, without regulatory changes, the likelihood that voters see untraceable ads increases. A regulation adopting disclosure and disclaimer rules for online advertisements are a step in the right direction. We also propose a repository to facilitate real-time transparency of all

147 See generally, Wood, Show Me the Money, supra note Error! Bookmark not defined. We acknowledge again Gilbert’s theory that disclosure can cause loss of information due to the chilling effect that the court assumes exists (but which scholars have found scant evidence of). Gilbert, supra note 16.
150 Levitt, supra note 148. This was adopted by the City of San Francisco. See City and County of San Francisco Ethics Comm’n, Before you Vote, Read the Label https://sfethics.org/disclosures/campaign-finance-disclosure/campaign-finance-disclosure-november-3-2015-election-dashboards/san-francisco-democracy-facts-lab-el-november-4-2014-election.
online political ads as well as ex post enforcement of violations of campaign finance rules.

In this section, we discuss three transparency-related regulatory changes for online political advertising.

Require Platforms to Keep and Disclose all Political Communications and Audiences

Government should require political advertisers on large social medial platforms to save and post every version of every political communication placed online, whether video, print, or image, and whether placed “for a fee” or not. The communications should be placed on a dedicated and easy-to-locate page on the campaign’s or group’s website or user page on the platform, as well as on a dedicated page created by the platform. The communications should be stored in their entirety, and they should be posted along with a uniform set of data stored in a uniform format for easy analysis and comparison across campaigns and over time. The FEC should also retain this data, for longer term storage, and to ensure that it exists even when platforms change or cease to operate.

In addition to the communication itself, the online advertising repository should contain the following data: when the communications ran, how much they cost to place and promote, candidates to which the communications refer, contested seat / issues mentioned, targeting criteria used, number of people targeted, and a platform-provided Audience identifier (“Audience ID”). For example, if a communication was aimed at women Facebook has identified as Democrats (from their profile pages), who “like” the show “Blackish” and also “like” Black Lives Matter, that information should be disclosed with the communication. Similarly, if the advertiser used outside consultants or internal data to generate a list of names, including through Custom or Lookalike Audiences on Facebook or similar services on other platforms, the advertiser must provide an Audience ID that will enable groups to engage in “counter speech” to the same audience. The Audience ID will be linked within the platform to a list of user names, but the platform should not disclose the audience names to anyone but the FEC.

The repository is an improved version of the Political File for television commercials.152 The Political File contains information about the ads, but not the

152 The FCC’s website describes the political file content of the Public File as follows.

- Political file (as required by [47 C.F.R.] 73.3526(e)(6), 73.3527(e)(5) ([2017])) (retain for two years). This file must contain all requests for specific schedules of advertising time by candidates and certain issue advertisers, as well as the final dispositions or “deals” agreed to by the broadcaster and the advertiser in response to any requests. It is
ads themselves. Crucially, the Political File contains targeting information, because the broadcaster or cable/satellite network (embedded in a market) and time of day the ad run are both disclosed. However, the design of the Political File is outdated. It is organized by station and is therefore cumbersome to navigate manually to get a picture of advertising for a statewide or national race over space and time. The FCC offers an API for researchers to download the information contained in it, but much of the information is stored in PDF documents and hand-written, making it difficult to glean systematic data quickly. The political advertising repository we propose will better serve our current technological abilities and democratic needs.

Of course, political advertisers will protest that this disclosure burdens their speech by requiring that they disclose their microtargeting strategies. The objection is absurd. When a campaign runs a television ad during the 8:30 PM airing of “Blackish” on the ABC affiliate in the St. Louis market – all of which is information that is disclosed in the Political File – the campaign’s targeting strategy is revealed. Online targeting can be “narrower”, in that the communications can be targeted to a smaller group of people, but just because the targeting strategies are more precise online does not grant the speakers more protection under the First Amendment. The size of the audience does not predict whether or not targeting criteria should be disclosed. If anything, communications targeting a narrower audience may be more damaging to civic values, because they are aimed at suppressing or mobilizing voters, rather than

not necessary to retain any of the materials relating to the negotiation between the parties to reach the disposition. Finally, the file must include the reconciliation of the deal such as a description of when advertising actually aired, advertising preempted, and the timing of any make-goods of preempted time, as well as credits or rebates provided the advertiser. The request and disposition must be placed in the file as soon as possible, which the Commission has determined is immediately absent extraordinary circumstances. The reconciliation information need not be placed in the file immediately but the broadcaster must identify a person or persons at the station capable of informing an advertiser of the details of any reconciliation information.

The Political File requirements for cable (47 C.F.R. 76.1701(d) (2017)) and satellite (47 C.F.R. 25.701(d) (2017)) track the language for broadcast with some differences that are not material here, with one interesting exception. The Political File for cable must retain a list of the “the chief executive officers or members of the executive committee or board of directors”, as applicable, of any entity that has paid for or furnished television broadcast programming that is “political matter or matter involving the discussion of a controversial issue of public importance.” (47 C.F.R. 76.1701(d) (2017))

making broad persuasive appeals. Narrow targeting may therefore deserve less, rather than more, constitutional protection. Finally, posting targeting criteria and Audience IDs for online ads facilitates counter speech in the same way that disclosure of the date, time, station, and program in which a television ad runs facilitates counter speech to the same audience.\footnote{Wood, Ravel, and Dykhne, supra note \textit{Error! Bookmark not defined.}, at 726 ("The remedy for speech that is false is speech that is true.").}\footnote{Alvarez, supra note \textit{Error! Bookmark not defined.}, at 726 ("The remedy for speech that is false is speech that is true.").} Arizona Free Enterprise Club v. Bennett, 564 U.S. 721, 726 (2011) contains dicta implying that facilitating more speech is not a valid regulatory objective under the First Amendment ("Leveling the playing field" can sound like a good thing. But in a democracy, campaigning for office is not a game. It is a critically important form of speech."). In that case, a public financing scheme provided additional funds to candidates facing attacks by outside spenders. Here, the regulation we propose (and the existing FCC Political File) does not fund speech, it merely reveals the audience to whom an opponent or opposing group spoke. We therefore believe that the more precise Alvarez case about false speech would be more persuasive to the court than Arizona Free Enterprise.\footnote{Antonio Garcia Martinez, who “helped create Facebook’s ad machine,” is skeptical that a repository of every ad run would be informative to viewers. “Per [Zuckerberg’s] video [announcing new transparency policies], Facebook pages will now show each and every post, including dark ones (!), that they’ve published in whatever form, either organic or paid. It’s not entirely clear if Zuckerberg intends this for any type of ad or just those from political campaigns, but it’s mindboggling either way. Given how Facebook currently works, it would mean that a visitor to a candidate’s page—the Trump campaign, for instance, once ran 175,000 variations on its ads in a single day—would see an almost endless series of similar content.” Antonio Garcia Martinez, \textit{I Helped Create Facebook’s Ad Machine. Here’s How I’d Fix it}, \textit{WIRED} (Sept. 22, 2017), https://www.wired.com/story/i-helped-create-facebooks-ad-machine-heres-how-id-fix-it.} We disagree. In the age of big data, smart data journalists and campaigns can distill key information from the repository, even if it does seem initially to contain “an almost endless series of similar
It is also important that reporting be coordinated across all online platforms. Platforms and political advertisers must use a uniform reporting format for all advertisers and distributors to report their activity. Gone are the days of handwritten and scanned forms, like we see in the Political File. Platforms can offer repository reporting and storage as a service to ad buyers and distributors, and reporting can happen as soon as the ad begins to appear in users’ feeds. Regulators, researchers, civil society watchdogs, and data journalists can analyze the data, take action based on it, and report to the public the current state of affairs in online political advertising. And yes, opposing campaigns can run countermessaging based on it, just as they can with disclosures to the Political File for television.

Facebook’s proposals so far are insufficient to achieve the level of transparency our democracy requires and will not facilitate enforcement of substantive campaign finance rules. Facebook claims it will require disclosure of “which page paid for an ad, but we will also make it so you can visit an advertiser’s page and see the ads they’re currently running to any audience on Facebook.” As we have argued elsewhere, their design falls short of the repository discussed here in several ways. First, it only requires that advertisers display the ads they are currently running. In the age of disappearing ads, the truly divisive ads can run for limited periods and escape detection. Second, there are so many outside groups now, each with their own Pages on Facebook that monitoring advertisers in real time would be almost impossible, even if each campaign wants to monitor just the groups advertising against it. Take, for example, the candidacy of Republican Ted Cruz in 2016. He was supported by his own campaign, six Super PACs, and probably also several other outside groups who supported multiple candidates. He also benefitted when outside groups opposed the 16 other candidates in his crowded field. Under Zuckerberg’s formulation, to get a picture just of advertising “currently” benefitting Ted Cruz, one would have to scroll through more than a dozen or more Pages. In a centralized repository, a user could filter results to view all ads mentioning Ted Cruz or any of his opponents, or any particular issues he cares about.

The Honest Ads Act of 2017 contains a rough description of a set of transparency requirements that would apply to any person or group spending more than $500 (aggregate) to make electioneering communications online and

---

would require that the platform maintain a public file. The current draft of the bill is vague on whether the system is disaggregated, like the FCC’s Political File, where users must search station-by-station and year by year. If the current proposal’s design is also disaggregated, then members of the public wanting to view the ads would be stymied by having to search advertiser-by-advertiser to find the ads they seek. This early design can be improved. First, disclosure should be standardized across platforms. Second, the $500 aggregate spending trigger is probably at the upper limit of what will be effective. It may be politically pragmatic to include a spending trigger, but the Constitution does not require one, and the Political File does not have one. Five hundred dollars is well below the campaign contribution limit and the registration thresholds with the FEC, but it has enormous advertising reach on Facebook. A numerical example illustrates. Imagine a Super PAC called Vermonters for Bernie. Vermont has around 500,000 voting-aged residents. Suppose that 400,000 of them are on Facebook. For less than $4,000 and the current cost-per-impression price of less than a penny, the group could show all voting-age residents of Vermont the ad. Of course, a group would only target voters that it knew it wanted to turn out to vote or that it knew it wanted to suppress – in other words, a much smaller number than the 400,000 or so registered voters on Facebook. For $250, an ad will have 25,000 “impressions”, appearing in the newsfeeds of 25,000 people. Considering the last election came down to fewer than 80,000 voters in three states, we believe the threshold triggering regulation should be fairly low. The platforms can also advise the advertisers of their obligation to register with and report to the FEC once they hit a certain threshold, to avoid a situation in which unsophisticated actors are swept up in the regulatory regime for very small expenditures.

A side benefit of the repository – and a crucially important one, from the standpoint of democracy – is that these transparency requirements will reduce

160 Cost per click is higher, around 22-30 cents per click over the time we’ve written this article. However, many disinfection ads clicked through to non-functioning landing pages, meaning that they may be placed for impressions, rather than clicks. Enough repetition in one’s newsfeeds from outlandish headlines with provocative pictures may be enough to suppress one’s enthusiasm for a candidate or conversely to mobilize her opponents.
161 Garcia Martinez thinks that the size of the Russian ad buy of $100,000 is “peanuts” and “didn’t influence the election’s outcome”. The peanuts may be in comparison to Facebook’s ad revenues, in which case we agree. No study has yet shown the effect of Russian ads or disinformation ads on social media for getting out the vote or suppressing the vote, so his conclusion that it did not affect the election is untested. Garcia Martinez, supra note 155.
the incentives to produce not only disinformation advertising but any divisive advertising microtargeted at small subsets of the population. Microtargeting is not, in itself, bad. But, as one of us has argued elsewhere, modern day campaigns are best able to target extreme voters. Microtargeting skews the demographics of the voting population away from the district itself and contributes to elite political ignorance.\textsuperscript{162} As individual microtargeting possibilities increase, campaigns and groups will want to give slightly different messages to different people. Indeed, one particular ad buy containing disinformation advertising (and paid for by Russians) was aimed in exactly this way, targeted at people who had expressed interest in “LGBT community, black social issues, the Second Amendment, and Immigration.”\textsuperscript{163} If advertisers are required to post every version of every ad on the same site, voters – via their informational intermediaries in the media – can detect when a group is trying to “divide and conquer” parts of the electorate. Opposition researchers can use their opponents’ divisive strategies against them. Smart data analysts can create tools that voters can use to see what their newsfeed would look like with a different configuration of “likes” and information. A user who sees ads in favor of guns, against abortion, and in support of Republican candidates could use the tool to see how her feed would look if she lived in a different zip code, “liked” Planned Parenthood and Everytown, or identified herself as a Democrat on her profile. Knowing the kind of advertising (and disinformation) our fellow voters receive can help aid deliberation in democracy.\textsuperscript{164}

a) Triggering Conditions

What online messages should be subject to these new transparency rules? Three, non-exclusive options are possible: first, the traditional bright line rule of candidate or ballot initiative mentions; second, a more-easily automated rule of identifying political content by targeting; and third, classifying the advertisers as political or not, gating their access to the platforms for advertising buys, and requiring repository storage of everything they run. We think all three can be deployed together, where any ad that fits any of the three rules would be included in the repository.\textsuperscript{165} Inclusion in the repository does not mean that disclaimers

\textsuperscript{162} See Elmendorf & Wood, supra note 62, at 33; Ryan D. Enos & Eitan D. Hersh, Campaign Perceptions of Electoral Closeness: Uncertainty, Fear and Over-Confidence, BRITISH J. OF POL. SCI. (2015).

\textsuperscript{163} Carol D. Leonning et. al, supra note \textit{Error! Bookmark not defined.}.

\textsuperscript{164} Most voters will not explore the repository themselves, of course. Just like with FEC filings, and political polling, they will receive the information as it is filtered through the media, as data journalists make browser plug ins, and as clever activists attempt to “gamify” learning about campaign advertising.

\textsuperscript{165} Including ads “swept up” by political targeting categories or by type of advertiser in the repository means that more than mere “electioneering communications” will be included in the repository. We do not see a “constitutional overbreadth” challenge to this as viable, in part
and disclosure are required. That is a separate determination to be made based on a loophole-free version of our existing regulations and described more fully in Part IV(C).

(1) References to candidates or ballot propositions

The cleanest regulatory line tracks the current regulatory requirements for disclaimers in other contexts: ask whether the ad advocates for the election or defeat of a clearly identified candidate or ballot initiative, or whether the ad mentions or shows a candidate or proposition and airs within a certain specified time before the election. We believe an ad belongs in the repository if it mentions or shows a candidate or issue any time after a candidate declares her candidacy or the issue is approved on the ballot. Given that disinformation advertising preceded the 2016 election by more than a year, we believe this temporal expansion for electioneering communications made online is wise.166

Facebook already monitors ads for content in order to minimize the amount of content that violates its terms of service.167 It prohibits or restricts advertising for tobacco, drugs (illegal or prescription), weapons, adult content, “sensational content” (“ads must not contain shocking, sensational, disrespectful, or excessively violent content”), misleading or false content, and many other categories that the platform already tries to identify and reject before it goes live as an advertisement. The advertising review process is entirely automated, though the platform has said it plans to include more humans in advertising review. Either way, reviewing ads for mentions of candidates is completely possible. When the ad mentions or displays a candidate, the ad should go to the repository.168

because the political file for broadcast and radio advertising implemented by the FCC already includes so-called “issue ads”, which do not reference a candidate in the way that electioneering communications do. Issue ads do not require disclaimers, yet important details about them are made public in the Political File. If regulators or legislators were concerned with a possible overbreadth challenge succeeding, they could make only ads identified under (1), reference to candidates or ballot issues, public. Ads identified by targeting criteria (2) or advertiser (3) could be provided to the regulator to check for potential violations of campaign finance laws. Counter speech would be impossible under this scenario.

166 We are not alone. See, e.g., Kennedy and Tausanovitch, supra note 131.
167 “During the ad review process, we'll check your ad's images, text, targeting, and positioning, in addition to the content on your ad's landing page. Your ad may not be approved if the landing page content isn't fully functional, doesn't match the product/service promoted in your ad or doesn't fully comply with our Advertising Policies.” Facebook Advertising Policies, FACEBOOK, https://www.facebook.com/policies/ads/ (last visited Oct. 2, 2017).
168 One aspect of this will be difficult to administer: Facebook will need a complete list of all candidates running for office anywhere in the country. It can work with federal, state, and local
As a back-up method, the platforms should require advertisers to indicate whether the ad mentions a candidate. The platforms can attach penalties (refuse to sell ad space, raise prices, temporarily suspend accounts, report to government regulators) on advertisers who lie on these forms. A system that is based on ad content will require spot checks and a way for advertisers to object to their inclusion in the repository as well as for viewers to report whether an ad that should contain a disclaimer actually does.

(2) Political targeting categories

Another triggering criteria is easier to automate by social media companies. We can require ad disclaimers and inclusion in the repository when an ad is targeted at explicitly political groups or contains “suspect classes”. Targeting categories might include political parties; “likes” or “follows” of political parties, candidates, issues, or groups that have parties, candidates or issues in the group’s name (like “Texans for Hillary” or “Minnesotans against abortion”); a racial category combined with any other listed criteria, and similar. Even if this is the only trigger, the likelihood that a consumer advertisement would be swept up in a repository requirement is probably slim, as consumer data is not very predictive of political persuasion and not very useful for campaigns.169

(3) Identify political ad content by the speaker (and know the speaker)

Facebook has a political advertising sales and operations team – indeed, it has teams “specialized by political party, and charged with convincing deep-pocketed politicians that [Facebook does] have the kind of influence needed to alter the outcome of elections.”170 There are teams assigned to campaigns for each major party. Antonio Garcia Martinez, a former Facebook product manager who ran the targeted ads program, argues that Facebook is already set up to adopt a “know your customer” type approach, similar to those used in the banking sector to prevent money laundering. Platforms should be required to “log[] each and every candidate and SuperPAC that advertises on Facebook. No initial vetting means no advertising”171. For the platforms, the “know your customer” approach is useful for creating a “gate” that allows platforms to avoid obvious foreign regulations to get this information. Our hope is that after the first round of elections in which it occurs, the process will be much easier, though the diversity and instability of thousands of candidate-registry lists on websites nationwide will never mean that this is a simple task.

money and to intercept and stop foreign disinformation advertising in our elections. A similar intervention could be to require a U.S. bank account to purchase ads, which will not stop foreign intervention but will ease enforcers in tracing the source of advertisements.  

Facebook does not currently gate political account creation from the beginning. Political advertising is targeted in such a way that the platforms could identify Pages that attempt to circumvent the additional check on political content by passing off their advertising as commercial advertising. Subjecting political advertisers to a source check can be done by Facebook with little difficulty. In the interest of national security, government should require that the platforms report when an ad is obviously funded by a foreign source, in real time, or as soon as the platform becomes aware of it.

b) Limits to a repository requirement

The repository requirement cannot solve all challenges of online political advertising. We imagine a challenge to the scope of the repository. What is special about the online context – why not require a repository for offline messaging as well, such as mailers? Some cities, like Los Angeles, require that all messaging be retained and disclosed. We think that is a useful regulation but is less pressing than creating a repository for online ads, because mailers do not disappear like online ads currently can. While a disclaimer-free mailer makes it difficult to learn about the money behind the message, and the audience for a mailer is almost impossible to recover for counter-speech purposes, the permanence of the mailer means that recipients can coordinate with each other and authorities to “follow the money” and enforce the rules. Enforcement of our disclosure, disclaimer, and substantive campaign finance rules is almost impossible without the repository.

An administrability concern lies in another game-able aspect of the current regulatory framework, and it should be updated for the age of social media and viral ads. Some ads are placed for free but promoted via bots, sock puppets, and inauthentic social media users (machine or human). Their promotion “services” are designed to appear organic, and payment to secure the ad shares and re-tweets occurs off-platform. Platforms are now able to identify suspicious activity from accounts that have an outsized impact, so some of these

---

172 Facebook’s current proposal is to require a U.S. driver’s license and a social security number to promote content.

173 We are grateful to Antonio Garcia Martinez, a former Facebook employee, for this insight.

faux-organic posts are detectible now. Payments for ad promotion by humans and non-humans alike are important expenditures, and they should trigger reporting requirements once they reach a minimum threshold.\textsuperscript{175} In brief, political ads that would otherwise be subject to disclaimers if they were placed for a “fee” under the current regulations, but which are placed for “free” and promoted via paid bots should contain disclaimers. They aren’t “free” content. This is only administratively difficult where the group making the payments is inclined to avoid reporting payments to services providing bots, trolls, and other inauthentic users in order to boost their messages. Nevertheless, its violation provides an important enforcement “hook” to reduce disinformation online.

Close the Loophole for Disclaimers in Online Ads

Despite its recent embrace of it, Facebook has long opposed transparency in online political advertising. Political advertising placed “for free” is still political advertising, and the public has a right to know who paid for its creation or distribution.\textsuperscript{176} To enforce disclaimer requirements, platforms can deputize users to report disclaimer violations, in the same way that the platforms allow users to report violations of the terms of service. They can also perform random spot-checks to help enforce the requirement (and deter attempts to circumvent it), by asking users after the ad is shown whether it contained a disclaimer.

The FEC is again feeling public pressure to close the loophole for disclaimers in online ads.\textsuperscript{177} It seems unlikely that the FEC itself will make much progress in the near term.

As for the content of disclaimers, at a minimum, the disclaimers should reveal the same information required when ads are run on television or radio.\textsuperscript{178} Since Citizens United, legislators and activists have urged that disclaimers on all ads (online or not) contain the names of the top donors to the entity running the ad. This strikes us as reasonable, and political science research has shown aspects of these more detailed disclosures to be effective.\textsuperscript{179}

\textsuperscript{177} FEC Advisory Op. 2017-12, supra note 39.
\textsuperscript{179} Research in political science suggests that this kind of enhanced disclosure can moderate the effectiveness of negative advertising. Dowling & Wichowsky 2013, Dowling & Wichowsky 2015, supra note \textit{Error! Bookmark not defined.}. Given that disinformation advertising is almost all negative against one candidate, enhanced disclaimers should reducing their
Eliminate Donor Anonymity for LLCs and 501(c) Organizations

Under our current disclosure and disclaimer framework, the public only sees the actual names of donors under certain circumstances, such as when the donors give to a campaign, party, SuperPAC, or other outside group subject to disclosure requirements. Even if the loophole for online advertising disclaimers is closed, the broader problem of LLC and 501(c) disclosure will remain. This loophole matters for disinformation advertising, because even if the disclaimer requirements are extended to online ads run and distributed by LLCs and 501(c) groups, without extending disclosure requirements to corporations making independent expenditures, voters cannot “follow the money”.

Why does this matter? For starters, the holdings in *Citizens United* and *SpeechNow* combine to imply that limits on independent expenditures are unconstitutional. Mega donors to outside groups can – and do – seek anonymity by making their independent expenditures through either their own anonymous LLCs or through 501(c) groups. Money is passed from group to group in a “daisy chain” of limited transparency.

We do not know what share of online ads are currently run by groups without disclosure requirements. The current legal regime means that there is no limit to the amount of political messaging that could come from anonymous sources. Moreover, corporate anonymity can hide foreign influence in our elections. We know that disinformation advertising was produced by a domestic corporation (DisinfoMedia, Inc.) and was also produced abroad. Saving ads run by corporations in the repository without requiring disclosure of their funders truncates voters’ ability to follow the money to learn about candidates and policies that matter to them.

B. “Nudge” and Educate Sharers and Viewers

We now turn our attention to ways the government can help reduce the spread of disinformation advertising through sharing, liking or commenting on disinformation advertising they see online. Education is paramount. Scholars call

effectiveness and, as a result, disincentivize their production and circulation in the first place. We also know that negative ads cite more sources than positive ads, so losing them entirely, while unlikely, may actually reduce voter competence. See Matthew P. Motta & Erika Franklin Fowler, *The Content and Effect of Political Advertising in U.S. Campaigns*, OXFORD RES. ENCYCLOPEDIA OF POL. (Dec. 2016), Fig. 4, http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-217.

180 See Wesleyan Media Project and Kennedy & Tausanovitch, *supra* note 131.
efforts to preempt disinformation via education ‘inoculation’. There are various successful forms of inoculation, such as educating users about the “potentially misleading effect of false-balance media coverage”, preemptive warnings to people about tactics used to spread misinformation, and even online games that teach the six main strategies of disinformation.

A simple education campaign on platforms can inoculate users. Education campaigns can also help users learn how to avoid spreading disinformation, by tightening their security settings and not interacting with disinformation in their newsfeeds, because the algorithms promote content based on interactions with it. If government required platforms to inoculate users, the platforms would be unlikely to protest it as “compelled speech”, mostly for political reasons. Alternatively (and more expensively), the government could pay to place inoculating ads on the platforms.

Viewing less disinformation in the first place is important. We are bad at recognizing and remembering corrections to false information. Disinformation, especially when repeated, persists in our minds. Users can view less disinformation if platforms provide an opt-out or opt-in system to viewing disinformation and viewing content from sources that have regularly spread disinformation. An opt-out system for advertising already exists. AdChoices, run by Digital Advertising Alliance, allows Internet users to opt out of being tracked by advertisers who are members of the alliance, who use “cookies” and tracking to present ads to Internet users based on previous internet activity. Only a small number of people actually opt out, making the stronger opt-in regulation more preferable in the disinformation advertising context. An opt-in (or out) system would reduce ad revenues for platforms selling political ads, but political ads are a miniscule part of platforms’ overall advertising revenue. As for the constitutionality of the opt-in or opt-out requirement, there is no case directly on point. It would be a content restriction that the user chooses, akin

---

182 Sander van der Linden et al., Inoculating Against Misinformation, 358 Science 1141 (2017).
184 Another technological fix could be a browser or app plug-in that automatically filters out disinformation advertising that fact checkers have flagged as false, which would have to be a private-sector fix, rather than a government project. Facebook has moved away from using flags for now. Flags actually encouraged more clicks. If it went back to identifying disinformation, Facebook could probably encode the fact that a fact checker disputes the information in the underlying code, for the app or plug-in to filter out.
186 See Elmendorf & Wood, supra note Error! Bookmark not defined..
to Google “Safe” search settings, where the default setting is to not show the user offensive content in search results.

These interventions will not stop everyone who shares disinformation. Some people are particularly motivated to share it. Partisan perceptual bias and motivated reasoning present additional challenges to efforts to convince people to stop spreading disinformation advertising.\footnote{See generally, Jennifer Jerit & Jason Barabas, \textit{Partisan Perceptual Bias and the Information Environment}, 74 J. OF POLITICS 672 (2012)} Partisan perceptual bias is distortion of “actual-world information” in the direction of “preferred-world states”, which can occur when a fact has positive or negative implications for one’s party.\footnote{Id. at 673, internal citation removed.} Motivated reasoning, observed here as \textit{directionally} motivated reasoning, “leads people to seek out information that reinforces their preferences, counterargue information that contradicts their preferences, and view proattitudinal information as more convincing than counterattitudinal information.\footnote{D.J. Flynn, et. al, \textit{The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs about Politics}, ADVANCES IN POL. PSYCH., 127, 132 (2017), http://onlinelibrary.wiley.com/doi/10.1111/pops.12394/epdf (internal parentheses omitted); citing C.S. Taber & M. Lodge, \textit{Motivated skepticism in the evaluation of political beliefs}, 50 AMER. J. OF POL. SCI. 755, 757 (2006), http://onlinelibrary.wiley.com/doi/10.1111/pops.12394/epdf} People have partisan and issue commitments. Partisan bias and motivated reasoning mean that it may be difficult to affect the utility calculations of people “under the sway” of disinformation that agrees with their preferred policy positions.\footnote{They can change, but correcting misinformation is difficult. See, generally, Jennifer L. Hochschild and Katherine Levine Einstein, \textit{Do Facts Matter? Information and Misinformation in American Politics}, 130 POLITICAL SCIENCE QUARTERLY 585 (2015). One way of correcting information, you have to “hit them between the eyes” with factual information. James H. Kuklinski, et. al, \textit{Misinformation and the Currency of Democratic Citizenship}, 62 J. POLITICS 791, 805 (2000). However, corrections can backfire. See Brendan Nyhan and Jason Reifler, \textit{When Corrections Fail: The Persistence of Political Misperceptions}, 32 POL. BEH. 303 (2010).} Some social media users do not care that the items they share on social media have been debunked by third party fact checkers. Political scientists Brendan Nyhan and Jason Reifler have observed that corrections to factual misperceptions can backfire to the point that “corrections actually increase misperceptions” among the group whose ideology is threatened by the correction, an effect observed (so far) among those who describe themselves as “very conservative”.\footnote{Nyhan and Reifler, \textit{supra} note 190, at 323 (Noting that there is also a great deal of evidence that liberals and Democrats also engage in motivated reasoning, though the backfire effect, in particular, was not observed in this particular project.)} In sum, our politics may be so group-based that users
could happily circulate news with contested content as long as it supports their candidate.

Therefore, platforms may need to be very active to reduce sharing of disinformation. A one-time opt-in (or out) process may not suffice to reduce disinformation. That brings us to general approaches that the platforms can use, which probably would not survive a constitutional challenge if done by government regulators.

C. Considerations for Platform Efforts to Reduce Disinformation

Disinformation is “sticky.” A series of papers by Nyhan and coauthors suggest that “political myths are extremely difficult to counter.”\(^\text{192}\) Reducing the amount of disinformation that voters are subjected to is useful from a human cognition standpoint, and as we have argued, from the standpoint of a thriving democracy. After an early period of minimizing its role,\(^\text{193}\) Facebook has begun to address its disinformation problem.\(^\text{194}\) It has experimented with using third party fact checkers to identify and label disinformation, with mixed results.\(^\text{195}\) Its latest attempt involves offering “related” stories that serve as fact correctives, polling users on which news sources they trust most, and suppressing all news in its users’ newsfeeds.\(^\text{196}\) It has not landed on a set of strategies.

Three general considerations will help any private regulatory framework to be effective. First, any efforts to label and identify questionable (or trustworthy\(^\text{197}\)) stories or sources should be consistent across platforms. All voters should be able to quickly identify untrustworthy content across platforms and trust that all platforms use the same standards to classify it. Second, the platforms should aim at incentives. They can do so in overt ways, such as Facebook’s plan


\(^\text{195}\) Jeff Smith, Grace Jackson, & Seetha Raj, Designing Against Misinformation, Medium.com (Dec. 20, 2017), https://medium.com/facebook-design/designing-against-misinformation-e5846b3aa1e2.


\(^\text{197}\) See Lehrman, supra note 10.
to temporarily ban advertisers who repeatedly share disinformation advertising that has been marked by fact checkers as “false news”.\textsuperscript{198} They can also aim at incentives in deeper ways, such as the way Facebook’s algorithm demotes ads that provide “low quality” experiences when users click through.\textsuperscript{199} Third, the platforms can turn down the volume of disinformation advertising by enforcing their terms of service, which prohibit bots and “inauthentic likes”.\textsuperscript{200}

**D. A Note about Feasibility**

As much as the social media companies argue that the best answer is self-regulation, a broader look around the world shows that social media companies comply with fairly tight regulations in other countries. Some of their regulations would not survive First Amendment muster or might not be otherwise desirable in the United States. Nevertheless, platform compliance with regulations elsewhere belies their platforms’ claim that the U.S. government regulations would be overly-burdensome.

Consider several examples. First, Germany passed a law that fines media platforms for failure to delete “illegal, racist, or slanderous posts within 24 hours of being notified to do so.” Because disinformation ads are often slanderous, a lot of disinformation ads will expose the platforms to penalties if not removed. The fines are steep: up to €50 million ($57 million USD), and estimates are that it will cost the platforms around €530 million ($622 million USD) a year to increase monitoring to avoid fines.\textsuperscript{201} Germany has apparently seen a decline in disinformation on Facebook since the law was implemented in summer 2017.\textsuperscript{202} The Czech Republic is particularly concerned about Russian efforts to destabilize their democracy. Its interior ministry has launched a Center Against Terrorism and Hybrid Threats, to “identify and counter fake news”.\textsuperscript{203} Dozens of jurisdictions worldwide observe “election silence”, or a media blackout, in the time leading up to voting day, or during voting day itself.\textsuperscript{204} These blackouts range from not allowing the mention of candidates aside from the fact that the

\textsuperscript{198} Flynn, supra note 193.
\textsuperscript{199} Mosseri, supra note 194.
\textsuperscript{202} Id.
\textsuperscript{203} Id.
\textsuperscript{204} Voting Day(s), ACE ELECTORAL KNOWLEDGE NETWORK, https://aceproject.org/ace-en/topics/me/mef/mef04/mef040d (last updated 2012).
candidate voted (France) to halting advertising except online and billboard advertising placed before the blackout period and not altered during it (Ontario, Canada).205

Many of these regulations would be considered government censorship beyond that which is tolerated for political speech in our country. It is certainly true that autocratic leaders may use “combating disinformation” as a convenient excuse for a crackdown on speech and expression. The broader point, for our purposes, is that social media platforms are subject to regulations worldwide and tolerate a good deal of regulation in order to enjoy the benefits of doing business in other countries. They can certainly handle some government-imposed transparency requirements here in the United States.

5. TASK ASSIGNMENT AND ACTION ACROSS MULTIPLE JURISDICTIONS

Who should implement the government regulations? In this Part, we briefly survey existing federal regulator capabilities, as well as identify cities who have started to act in the absence of federal government regulation.

A. Federal Agency Competencies and Task Assignment

Administrative agencies have a wide variety of missions, specializations, and clients.206 The FEC’s core mission is to “protect the integrity of the federal campaign finance process by providing transparency and fairly enforcing and administering federal campaign finance laws.”207 Its clients are comprised of voters (beneficiaries) and the candidates, parties, outside groups who finance messaging, and elected officials (regulated entities). Its position is complex, because the regulated entities also control their funding. Perhaps as a result, the FEC’s mission statement is heavy on transparency and tepid on enforcement and administration.

FEC enforcement is slow. By law, the FEC is a bipartisan agency and can have no more than three out of six commissioners from one political party. Partisan gridlock frequently prevents enforcement actions from progressing.208 The FEC’s enforcement procedures require multiple rounds of voting: to proceed

to an investigation, to allow the general counsel to conduct formal discovery and issue subpoenas, to determine whether there is “probable cause” to believe a violation has occurred, and to litigate the matter in court if a settlement cannot be reached. Resolving a matter can take years.

For a decade, Republican commissioners have resisted updating campaign finance laws and enforcing the existing ones. Even as Facebook disclosed that Russian-linked trolls had purchased political ads on its platform during the 2016 election, the Republican FEC commissioners expressed worry that changing its policies would hinder “First Amendment rights to participate in the political process.”

The FEC is charged with enforcing the ban on foreign contributions and expenditures, though its jurisdiction only extends to civil penalties. Its partisan gridlock has been cited as a reason why government regulation of political advertising online will not work. Another challenge is the skill set required to combat disinformation advertising. The FEC lawyers who conduct investigations are not expert in tracing money to its source using sophisticated computer-assisted tracing and data investigations. Even if it could escape partisan gridlock, the FEC is probably not the best fit for pursuing enforcement actions against disinformation advertising.

Our election security would be better served by placing investigation and enforcement capabilities in other agencies. One candidate is the U.S. Treasury’s Financial Crimes Enforcement Network (FinCEN), which has a core mission

---

210 Id.
212 Id.
214 Editorial, Deadlocked in Regulation, WASH. POST (June 15, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/06/14/AR2009061402400.html (“The three Republican appointees are turning the commission into The Little Agency That Wouldn't: wouldn't launch investigations, wouldn't bring cases, wouldn't even accept settlements that the staff had already negotiated. This is not a matter of partisan politics. These commissioners simply appear not to believe in the law they have been entrusted with enforcing.”); Ciara Torres-Spelliscy, The Justice Department Is Now on the Campaign Finance Beat, BRENNAN CTR. FOR JUST. (Oct. 12, 2015), https://www.brennancenter.org/blog/justice-department-now-campaign-finance-beat (“With the Federal Election Commission hopelessly deadlocked, campaign finance enforcement is now coming as federal criminal cases.”).
entirely related to financing, national security, and intelligence: “safeguard the
financial system from illicit use and combat money laundering and promote
national security through the collection, analysis, and dissemination of financial
intelligence and strategic use of financial authorities.” Other candidates to aid in
investigation and enforcement are the FBI’s Cyber Crimes Division and the FCC.
The FCC is ostensibly the regulator of social media companies. They do keep of
the Political File for television ads, but they have not regulated of social media.

B. The Role of State and Local Government

Regulation occurs at all levels of government. Individual cities and states
control their own elections and can – and do – regulate the financing of those
elections. Some states have already regulated disclaimers for online ads, for
example, to provide more transparency than the federal regulatory regime
requires.215 These state laws currently target the advertiser and not the platforms,
but if the states are comfortable departing from the low bar set by the federal
government in this realm, they should also be comfortable doing so to keep
disinformation out of their state and local elections. In the same way that the
platforms are already accustomed to dealing with multiple regulatory
jurisdictions across the world, they can handle a diversity of regulations
domestically. If an overarching regulatory framework that protects voters in all
elections does not emerge soon, local and state governments will act to protect
voters in their own elections from disinformation.216

As of this writing, the Maryland legislature has passed legislation
requiring the platforms to retain all ads and audiences.217 The California
legislature is considering a similar bill.218 Washington State and the city of Seattle
are enforcing a longstanding legal requirement that “commercial advertisers”
disclose the “exact nature and extent” of ads, the “names and addresses” of ad
purchasers, and specific payment details.219 The Seattle enforcement body is
interpreting the ordinance to require copies of the ads in question and information
about their intended and actual audiences – in other words, Seattle is requiring a
repository very similar to the one we recommend for all jurisdictions.220

---


216 Chris Elmendorf, et. al, supra note 157.


219 SEATTLE, WA., CHARTER ch. 2.04.280 (2018),
https://library.municode.com/WA/seattle/codes/municipal_code?nodeId=TIT2EL_CH2.04ELCA
CO_SUBCHAPTER_IICAD1_2.04.280COADDURE.

220 Eli Sanders, Seattle Says Facebook Has Failed to Follow Law on Election Ad Transparency,
THE STRANGER (Feb. 5, 2018), https://www.thestranger.com/slog/2018/02/05/25781471/seattle-
says-facebook-has-failed-to-follow-law-on-election-ad-transparency.
Angeles already requires candidates to store all advertisements. Along with Chris Elmendorf, we have urged the City of San Francisco to adopt our model.

CONCLUSION

Fake news is not news; it is native advertising to spread disinformation, and it belongs to the broader category of “disinformation advertising”. We have proposed a menu of ways for government to regulate online political advertising, including disinformation advertising. We believe that signaling matters and that the government must act, rather standing by while Facebook slowly comes around to partial self-regulation and attempts to drag a couple of its competitors along. The platforms have too many conflicts of interest and are too politically vulnerable to be trusted to carry out comprehensive self-regulation. Within the constraints of the First Amendment, the government must regulate – and while the jurisprudence may need updating in light of the rapid change in our communications, our proposed regulations should pass muster under the current jurisprudence.

Most of what scholars have studied and courts assume about the effects of campaign finance regulations developed with “offline” political advertisements as the motivating example. The underlying behavioral expectations around regulating political advertising online should hold in a broad sense, but the 2016 election drove home four features of online advertising that distinguish it from television advertising. First, it is more likely to be disguised as informational content. Second, it is more likely to contain disinformation. Third, it is more likely to be untraceable by the public or candidates hoping to speak to the same audience. Fourth, it is much cheaper. All of these features matter to shaping a regulatory framework that will help the public to trace the source of the (dis)information they view online and the government keep foreign influence out of our elections.

Government must extend and update existing campaign finance transparency regulations for use online. Our proposals will facilitate enforcement, improve voter competence, and facilitate counter-speech. They have the ancillary benefit of reducing the attractiveness of online political microtargeting. It defies logic that political ads run on television, cable, and radio, and are accessible to the public long after they run, but we have such large transparency deficits when it comes to online political advertising.

222 See, Elmendorf et al, supra n. 157.
Whether government can constitutionally require platforms to inoculate users or provide opt-in and opt-out regimes are both open questions under the First Amendment. Of course, nothing (except their financial conflict of interest) is preventing the platforms from instituting these reforms without being required to by government. Direct content regulation should under no circumstances be performed or required by the government. If the platforms are unable or unwilling to reduce disinformation advertising, government cannot step in.

Democracy in the United States is at a crucial point. A foreign regime attempted to destabilize our democracy using disinformation, and their attacks are ongoing. Opportunists, foreign and domestic, are also producing political disinformation to make a quick buck. Transparency for online political advertising will shed light on a dark process and enable enforcement against people attempting to sow conflict and discord.