

*University of Southern California Law
School*

Legal Studies Working Paper Series

Year 2018

Paper 261

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

Abby Wood*

Ann M. Ravel†

*University of Southern California, awood@law.usc.edu

†University of California, Berkeley School of Law, ann.ravel@gmail.com

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 and Ann M. Ravel

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**

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.

Internet platforms prefer self-regulation and have only recently come around to supporting proposed transparency legislation. 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. First, and most importantly, campaign finance regulators should require platforms to store and make available (1) ads run on their platforms, and (2) 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

*. Associate Professor of Law, Political Science, and Public Policy at University of Southern California (awood@law.usc.edu).

** . Senior Fellow, Maplight Digital Deception Project and former Chair of the Federal Election Commission and California Fair Political Practices Commission. This article 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, and Edward Prouty. Irina Dykhne’s seminar paper-turned-note on native political advertising was particularly influential for this piece, and we are grateful to her for her thoughts on our drafts.



paid distribution on social media, as well as all other online political advertising. Second, existing loopholes in transparency regulations related to online advertising should be closed. Congress has a role here as it has prevented regulatory agencies from acting to require disclosure from so-called dark money groups. Finally, government should require that platforms offer an opt-in system for social media users to view narrowly-targeted ads or disputed content.

TABLE OF CONTENTS

INTRODUCTION	1229
I. DOCUMENTING AND FRAMING THE PROBLEM.....	1233
A. FAKE NEWS IS POLITICAL ADVERTISING.....	1233
B. HOW DISINFORMATION CAN WEAKEN DEMOCRACY.....	1239
II. FIRST AMENDMENT, POLITICAL SPEECH, AND CHOICE OF REGULATOR	1242
A. CONSTITUTIONAL FRAMEWORK FOR CAMPAIGN ADVERTISING REGULATION.....	1243
B. CHOICE OF REGULATOR.....	1250
1. Industry Self-Regulation and Co-Regulation.....	1250
2. Government Regulation	1253
III. OUR CURRENT, INSUFFICIENT, REGULATORY FRAMEWORK FOR ONLINE POLITICAL ADVERTISING	1254
IV. CONSTITUTIONALLY-PERMISSIBLE REGULATIONS TO ADDRESS DISINFORMATION ADVERTISING	1260
A. IMPROVE TRANSPARENCY	1262
1. Require Platforms to Keep and Disclose all Political Communications and Audiences.....	1263
2. Close the Loophole for Disclaimers in Online Ads	1274
3. Eliminate Donor Anonymity for LLCs and 501(c) Organizations	1276
B. “NUDGE” AND EDUCATE SHARERS AND VIEWERS	1276
C. CONSIDERATIONS FOR PLATFORM EFFORTS TO REDUCE DISINFORMATION.....	1279
D. A NOTE ABOUT FEASIBILITY	1280
V. TASK ASSIGNMENT AND ACTION ACROSS MULTIPLE JURISDICTIONS	1282
A. FEDERAL AGENCY COMPETENCIES AND TASK ASSIGNMENT	1282
B. THE ROLE OF STATE AND LOCAL GOVERNMENT	1284
CONCLUSION.....	1285



2018]	<i>FOOL ME ONCE</i>	1229
APPENDIX.....		1287

INTRODUCTION

During the 2016 Presidential campaign, the average adult saw at least one “fake news” item on social media.¹ 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.² 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.³ The attacks are ongoing.⁴

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.⁵ The targeting aims to polarize and fragment the electorate. Tracing the money behind this kind of messaging is next to impossible under current regulations and advertising platforms’ current policies. Voters’ inability to “follow the money” has implications for our democracy,

1. Hunt Allcott & Matthew Gentzkow, *Social Media and Fake News in the 2016 Election*, 31 J. ECON. PERSP. 211, 227 (2017).

2. *Undermining Democratic Institutions and Splintering NATO: Russian Disinformation Aims: Hearing Before the H. Comm. on Foreign Affairs*, 115th Cong. 27 (2017) (statement of Peter Doran, Executive Vice President, Center for European Policy Analysis).

3. *Russian Interference in the 2016 U.S. Elections: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 72–76 (2017) (statement of J. Alex Halderman, Professor of Computer Science and Engineering, University of Michigan), 2 (Opening statement of Sen. Mark Warner), 17 (statement of Bill Priestap, Asst. Dir. Counterintelligence Div.).

4. See, e.g., *Homeland Security Threats*, C-SPAN (Sept. 27, 2017), <https://www.c-span.org/video/?434411-1/senior-officials-testify-homeland-security-threats> (statement of Sen. James Lankford, Member, S. Comm. on Intelligence); Devlin Barrett, *Lawmaker: Russian Trolls Trying to Sow Discord in NFL Kneeling Debate*, WASH. POST (Sept. 27, 2017), <http://wapo.st/2xeZkQY>.

5. *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel I: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 30–42 (2017) (statement of Clint Watts, Robert A. Fox Fellow, Foreign Policy Research Institute).

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 by 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 beliefs⁶ or on political agenda setting.⁷ 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.⁸ Still others offer media-based solutions,⁹ or emphasize that platforms are the only entities who can, or should, correct the problem while staying within the existing First Amendment framework.¹⁰ A few are ready to re-interpret the First Amendment in light of the new imbalance between speakers and listeners.¹¹ Yet other scholars have suggested that platforms should be regulated in a way that fits a pre-existing regulatory framework, such

6. Andrew Guess, Brendan Nyhan & Jason Reifler, *Selective Exposure to Misinformation: Evidence from the Consumption of Fake News During the 2016 U.S. Presidential Campaign* (Jan. 9, 2018) (unpublished manuscript), <http://www.dartmouth.edu/~nyhan/fake-news-2016.pdf>; Richard Gunther, Paul A. Beck & Erik C. Nisbet, *Fake News Did Have a Significant Impact on the Vote in the 2016 Election: Original Full-Length Version with Methodological Appendix* (2018) (unpublished manuscript), <https://u.osu.edu/cnep/files/2015/03/Fake-News-Piece-for-The-Conversation-with-methodological-appendix-11d0ni9.pdf>.

7. Chris J. Vargo, Lei Guo & Michelle A. Amazeen, *The Agenda-Setting Power of Fake News: A Big Data Analysis of the Online Media Landscape from 2014 to 2016*, 20 *NEW MEDIA & SOC'Y* 2028, 2028 (2018).

8. See, e.g., Mark Verstraete et al., *Identifying and Countering Fake News* 22–24 (Arizona Legal Studies Discussion Paper No. 17-15, Aug. 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3007971 (proposing a re-interpretation of section 230 of the Common Decency Act).

9. See, e.g., the Trust Project's standardized disclosures that provide clarity on a news organization's ethics. Sally Lehrman, *What People Really Want from News Organizations*, *ATLANTIC* (May 25, 2017), <https://www.theatlantic.com/technology/archive/2017/05/what-people-really-want-from-news-organizations/526902>.

10. Richard L. Hasen, *Cheap Speech and What It Has Done (to American Democracy)* 28 *FIRST AMEND. L. REV.* (forthcoming 2018) (manuscript at 3), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3017598; Nathaniel Persily, *The Campaign Revolution Will Not Be Televised*, *AM. INT.* (Oct. 10, 2015), <https://www.the-american-interest.com/2015/10/10/the-campaign-revolution-will-not-be-televised>.

11. TIM WU, *KNIGHT FIRST AMEND. INST., EMERGING THREATS: IS THE FIRST AMENDMENT OBSOLETE?*, 11 (2017), <https://knightcolumbia.org/sites/default/files/content/Emerging%20Threats%20Tim%20Wu%20Is%20the%20First%20Amendment%20Obsolte.pdf>.

as the way we regulate media organizations¹² or public utilities.¹³

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 themes among disinformation advertising are that it is false, it aims to affect people’s political opinions and the probability that they will turn out to vote, and the advertiser pays to produce or distribute it.

The First Amendment provides clear limits on the government’s ability to regulate politically-related messaging. However, the Constitution allows for more regulation than currently exists for political speech on social media. Courts have repeatedly upheld campaign finance disclaimers and disclosure of the funding behind political spending. At a minimum, the sources of 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,¹⁴ 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.¹⁵ Adding disinformation to the mix

12. Anders Åslund, *Regulate Social Media—Just Like Other Media*, THE HILL (Oct. 5, 2017), <http://thehill.com/opinion/national-security/354006-regulate-social-media-just-like-other-media>.

13. Jonathan Taplin, *Is It Time to Break Up Google?*, N.Y. TIMES (Apr. 22, 2017), <https://nyti.ms/2p7Emhp>.

14. 52 U.S.C. § 30121 (2012) (discussing contributions and donations by foreign nationals); 11 C.F.R. § 110.20 (2017) (prohibiting contributions, donations, expenditures, independent expenditures, and disbursements by foreign nationals).

15. Michael Gilbert’s work points out that there is a tradeoff between the loss of



further damages voters' ability to make the choice that best aligns with their preferences. While regulations responding to this problem have been proposed, the agency tasked with regulating is unlikely 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 for online political advertising, the lack of transparency originated with the platforms, 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 potential fixes. If platforms are unable or unwilling to act in those areas, government cannot step in.

In this Article, we propose three 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 they will help make visible the sources of political messaging online. Part I of this Article explains disinformation advertising as it existed in 2016—unregulated, from unknown sources, and aimed to fragment our politics—and how it 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 and regulation by platforms. In Part III, we discuss the loopholes in our existing regulatory system for online political advertising. 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. We also suggest guidelines for platform self-regulation to attack the problem. A brief review of regulations in several foreign jurisdictions,

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*, 14 ANN. REV. L. & SOC. SCI. (forthcoming Oct. 2018), <https://www-annualreviews-org.libproxy1.usc.edu/doi/pdf/10.1146/annurev-lawsofsci-110316-113428> [hereinafter Wood, *Campaign Finance Disclosure*] (highlighting various opportunities to expand the literature on campaign finance disclosure).

which concludes Part IV, demonstrates that social media platforms are already willing and able to comply with stricter regulations 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; rather, disinformation campaigns have the potential to impact city and state elections too, causing local government to begin regulating platforms for their own elections.

I. 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 U.S. presidential election. Fake news articles are distributed via social media to drive web traffic to websites.¹⁶

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.

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.¹⁷ Sophisticated disinformation is persuasive because it looks like credible journalism.¹⁸ But fake news is not “news.” It is native advertising and should be regulated as such.¹⁹ 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

16. See Allcott & Gentzkow, *supra* note 1, at 213.

17. See generally, *e.g.*, *id.* at 211–36.

18. See CHRISTOPHER PAUL & MIRIAM MATTHEWS, RAND CORP., THE RUSSIAN “FIREHOSE OF FALSEHOOD” PROPAGANDA MODEL: WHY IT MIGHT WORK AND OPTIONS TO COUNTER IT 7 (2016), <https://www.rand.org/pubs/perspectives/PE198.html> (summarizing literature in experimental psychology).

¹⁹ To our knowledge, the first law review publication noting the potential legal issues involved in native political advertising online is the award-winning student Note by Irina Dykhne. See generally *Persuasive or Deceptive? Native Advertising in Political Campaigns*, 91 SO. CAL. L. REV. 339 (2018).

untrustworthy or unfit for office,²⁰ or to sow division among Americans.²¹ During the 2016 presidential election, many 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 U.S. elections. Russia’s attack occurred (and continues) on social media platforms.²⁴ Expert estimates of the number of shares of Russian-sourced “fake news” on Facebook vary widely, from over 100 million to “into the billions.”²⁵ These estimates include content ranging from fake news articles to generic ideological statements from foreign sources with no disinformative content. The fact is, lack of disclosure

20. See Adam Entous, Craig Timberg & Elizabeth Dvoskin, *Russian Operatives Used Facebook Ads to Exploit Divisions Over Black Lives Matter and Muslims*, WASH. POST (Sept. 25, 2017), http://wapo.st/2fM3sNh?tid=ss_tw-bottom&utm_term=.dbb227bc4754.

21. Indictment ¶ 6, United States v. Internet Research Agency LLC, No. 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018), <https://www.justice.gov/file/1035477>. Ads aimed at sowing division and not necessarily mentioning candidates would be more akin to issue advertising than campaign advertising or electioneering communications. Issue advertising is subject to fewer disclosure requirements, generally.

22. See *id.* ¶ 46.

23. Eric Lubbers, *The Man Behind Denver Guardian (and Many Other Fake News Websites) Is a Registered Democrat from California*, DENVER POST (Nov. 24, 2016, 1:29 PM), <http://www.denverpost.com/2016/11/23/the-man-behind-denver-guardian>.

24. The Alliance for Securing Democracy continues to track Russian social media activity in the United States. See GMF ALLIANCE FOR SECURING DEMOCRACY <https://dashboard.securingsdemocracy.org> (last visited Sept. 4, 2018). See also Molly K. McKew, *How Twitter Bots and Trump Fans Made #ReleaseTheMemo Go Viral*, POLITICO (Feb. 4, 2018), <https://www.politico.com/magazine/story/2018/02/04/trump-twitter-russians-release-the-memo-216935>.

25. *Social Media Influence in the 2016 U.S. Elections: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. (2017) (statement of Sen. Richard Burr, Chair, Sen. Intelligence Comm.); Craig Timberg, *Russian Propaganda may have been Shared Hundreds of Millions of Times, New Research Says*, WASH. POST (Oct. 5, 2017), <https://www.washingtonpost.com/news/the-switch/wp/2017/10/05/russian-propaganda-may-have-been-shared-hundreds-of-millions-of-times-new-research-says> (citing Jonathan Albright, *Itemized Posts and Historical Engagement—6 Now-Closed FB Pages*, TABLEAU, <https://public.tableau.com/profile/d1gi#!/vizhome/FB4/TotalReachbyPage> (last updated Oct. 5, 2017)).



of online political spending means that no one captured the entire universe of political ads. The best evidence we have so far, from a user-generated ad collection of 5 million ads by 10,000 Facebook users,²⁶ suggests that 86% of the groups running *paid ads* on Facebook in the last six weeks before the election were suspicious groups (53%),²⁷ astroturf movement groups (17.1%),²⁸ and questionable news outlets (15.8%)²⁹.

For a small fee, anyone can distribute content and generate impressions on social media.³⁰ Using Facebook as an example, political ads, including disinformation ads, could be promoted, or boosted, for a fee, just like any other ad.³¹ Boosted ads appear higher on users' newsfeeds. 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.³² 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 re-targeted people who had

26. Young Mie Kim et al., *The Stealth Media? Groups and Targets Behind Divisive Issue Campaigns on Facebook*, POL. COMM. (forthcoming 2018) (manuscript at 9), <https://doi.org/10.1080/10584609.2018.1476425>

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. *Id.* at 11. The Russian groups, which comprised 8.3% of total groups running ads over the time period, were identified as such by Facebook and the House Intelligence Committee. *Id.*

28. The authors define these as groups that have not registered with the National Center for Charitable Statistics, 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.* at 12.

30. See Tess Townsend, *Why Political Ads Are Regulated but Fake News on Facebook Isn't*, INC. (Dec. 9, 2016), <https://www.inc.com/tess-townsend/facebook-fake-news-political-ads.html>.

31. *How to Boost Your Posts*, FACEBOOK BUSINESS, <https://www.facebook.com/business/a/online-sales/promoted-posts> (last visited Sept. 4, 2018). See also Townsend, *supra* note 30.

32. Elizabeth Dwoskin et al., *Russians Took a Page From Corporate America by Using Facebook Tool to ID and Influence Voters*, WASH. POST (Oct. 2, 2017), <http://wapo.st/2xPIDZ6>.

visited their sites with further political messaging.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.³⁴ If these tools remain available to advertisers in future elections, it is likely that disinformation advertisers will use them in the future as well.

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.³⁵ Social media users can easily build a large social media following using cheap third-party services to promote their Twitter or Facebook accounts.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.³⁷

There is spending at many steps of this process, including in

33. *Id.* Facebook reported that only 1% of the ads they turned over to Congress from the 2016 election used Custom Audiences. Elliot Schrage, *Hard Questions: Russian Ads Delivered to Congress*, FACEBOOK NEWSROOM (Oct. 2, 2017), <https://newsroom.fb.com/news/2017/10/hard-questions-russian-ads-delivered-to-congress>. 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.

34. Antonio García Martínez, *How Trump Conquered Facebook—Without Russian Ads*, WIRED (Feb. 23, 2018, 10:06 AM), <https://www.wired.com/story/how-trump-conquered-facebook-without-russian-ads>. In its recent proposals, Facebook has recognized aspects of this problem and proposed changes., *Shutting Down Partner Categories*, FACEBOOK NEWSROOM (Mar. 28, 2018), <https://newsroom.fb.com/news/h/shutting-down-partner-categories>.

35. *See Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel I: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 48 (2017) (statement of Clint Watts, Robert A. Fox Fellow, Foreign Policy Research Institute). *See also* Indictment ¶ 44, *United States v. Internet Research Agency LLC*, 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018), <https://www.justice.gov/file/1035477>; *Undermining Democratic Institutions and Splintering NATO: Russian Disinformation Aims, Before the H. Comm. on Foreign Affairs*, 115th Cong. 30 (2017) (statement of the Hon. Daniel Baer).

36. Ten thousand Twitter followers cost \$39.89; five hundred Facebook shares cost less than \$25. *See Buy Twitter Followers*, SOZIALY, <https://www.sozialy.com/buy-twitter-followers> (last visited Sept. 4, 2018). *See also The Most Reliable Place to Buy Facebook Shares*, BUY REAL MARKETING, <https://www.buyrealmarketing.com/buy-facebook-shares> (last visited Sept. 4, 2018).

37. *See Undermining Democratic Institutions and Splintering NATO: Russian Disinformation Aims: Hearing Before the H. Comm. on Foreign Affairs*, 115th Cong. 11 (2017) (prepared statement of Toomas Hendrik Ilves, former President of the Republic of Estonia); *Undermining Democratic Institutions and Splintering NATO: Russian Disinformation Aims: Hearing Before the H. Comm. on Foreign Affairs*, 115th Cong. 30 (2017) (statement of the Hon. Daniel Baer).

salaries and production costs to make the content in the first place.³⁸ Some of this spending triggers the existing rules. 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, are subject to regulation under existing rules.³⁹ We also know that some of the advertisers violated the ban on foreign expenditures in connection with a U.S. election because they were paid for by foreign sources, providing another example of existing rules applying to disinformation ads.⁴⁰ Disaggregated ads and audiences, disappearing ads, and other difficulties would complicate enforcement efforts, even for a motivated agency. The problem is data availability to establish the fact of the violation and facilitate enforcement. Therefore, at a minimum, effective enforcement of existing rules requires retaining data and advertising content. And in order to allow groups to counter disinformation against them or their preferred candidates, we must also retain the audience targeting information, which we discuss in Part IV.

* * *

Media organizations are exempt from campaign finance regulations. Even if we are correct that “fake news” is better thought 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 press (or “media”) exemption from campaign finance regulation.⁴¹ The exemption allows legitimate media

38. See Checks and Balances for Economic Growth, MUR 6729 (FEC Oct. 24, 2014) (statement of Vice Chair Ann M. Ravel), <http://eqs.fec.gov/eqsdocsMUR/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. A 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 Opinion 2017-12 (Dec. 15, 2017), <http://saos.fec.gov/aodocs/2017-12.pdf>.

40. 11 C.F.R. § 110.20(f) (2018).

41. See, e.g., 52 U.S.C. § 30101(9)(B)(i) (2012) (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 (requiring disclosure for political committees).

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, however, the FEC would run afoul of the First Amendment by burdening the speech of legitimate news media.⁴²

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 its ‘legitimate press function.’”⁴³ To determine whether a publication or organization is a press entity, the FEC asks “whether the entity in question produces on a regular basis a program that disseminates news stories, commentary, and/or editorials.”⁴⁴ When analyzing whether a press entity is acting “in its legitimate press function,” the FEC looks at “(1) whether the press entity’s materials are available to the general public, and (2) whether the materials are comparable in form to those ordinarily issued by the press entity.”⁴⁵ 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. As such, the test may be too lax: because it does not consider indicia of traditional journalism when granting the exemption, the Russian government propaganda outlet, *Russia Today*, was deemed a “legitimate press entity” by the FEC.⁴⁶

Even under this minimalist test, the FEC would not consider much of the disinformation on social media to be the product of a “press entity.”⁴⁷ Take the *Denver Guardian* as an example. It existed only

42. *Turner Broad. Sys. v. FCC*, 512 U.S. 622, 659 (1994). *See also* Note, *Defining the Press Exemption from Campaign Finance Restrictions*, 129 HARV. L. REV. 1384, 1385–86 (2016).

43. FEC, Advisory Opinion 2016-01, at 3 (Apr. 8, 2016). *See also* Reader’s Digest Ass’n v. FEC, 509 F. Supp. 1210, 1215 (S.D.N.Y. 1981).

44. FEC, Advisory Opinion 2010-08, at 5 (June 11, 2010), <http://saos.fec.gov/aodocs/AO%202010-08.pdf>.

45. FEC, Advisory Opinion 2011-11, at 7 (June 30, 2011), <https://www.fec.gov/files/legal/aos/76329.pdf> (citing *FEC v. Mass. Citizens for Life*, 479 U.S. 238, 251 (1986)); FEC Advisory Opinion 2000-13 (June 23, 2000) (concluding that a website was “viewable by the general public and akin to a periodical or news program distributed to the general public”).

46. *See* RTTV America, Inc., MUR 6481 (May 27, 2014) (dismissing action against RTTV and Ron Paul 2012 Presidential Campaign Committee in a letter), <http://eqs.fec.gov/eqsdocsMUR/14044354314.pdf>.

47. The disinformation at issue is not “clickbait” headlines with spins on true (or mostly

briefly before running a story about a murder-suicide committed by “an FBI agent believed to be responsible for the latest [DNC] email leaks.”⁴⁸ Its registered address is actually a parking lot.⁴⁹ The site had ads, Denver’s weather, and no more than two news stories during its entire existence.⁵⁰ Similarly, Facebook pages that disseminated content and memes, like the “Blacktivist” page, would not be considered press entities. They were created in the months before the election and claimed to be activists, not journalists.⁵¹

B. HOW DISINFORMATION CAN WEAKEN DEMOCRACY

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

[F]actual 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. . . . [K]nowledge 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.⁵²

Disinformation advertising works like other kinds of propaganda, by sowing doubt about institutions.⁵³ Here, the propaganda uses a fake

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 in Apparent Murder-Suicide*, SNOPE (Nov. 5, 2016), <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. INTERNET ARCHIVE: WAYBACK MACHINE, http://web.archive.org/web/*/http://denverguardian.com (last visited Sept. 4, 2018).

51. See generally Donie O’Sullivan & Dylan Byers, *Exclusive: Fake Black Activist Accounts Linked to Russian Government*, CNN (Sept. 28, 2017, 11:40 AM), <https://money.cnn.com/2017/09/28/media/blacktivist-russia-facebook-twitter/index.html>.

52. MICHAEL X. DELLI CARPINI & SCOTT KEETER, WHAT AMERICANS KNOW ABOUT POLITICS AND WHY IT MATTERS 3, 5 (1996). Scholars of deliberative democracy also list information as paramount. See, e.g., Simone Chambers, *Deliberative Democratic Theory*, ANN. REV. POL. SCI. 307, 309, 319–20 (2003); James S. Fishkin & Robert C. Luskin, *Experimenting with a Democratic Ideal: Deliberative Polling and Public Opinion*, 40 ACTA POLITICA 284, 285 (2005).

53. Jason Stanley, *In Defense of Truth, and the Threat of Disinformation*, in CAN PUBLIC DIPLOMACY SURVIVE THE INTERNET? BOTS, ECHO CHAMBERS, AND DISINFORMATION 71 (Shawn Powers & Markos Kounalakis eds., 2017).

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.⁵⁴ 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 fire hose which has diluted trusted sources of information”⁵⁵ 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.”⁵⁶

Scholars have argued that an informed electorate is a constitutional value and that we should recognize a canon of “effective accountability” which relies upon an informed electorate.⁵⁷ Many voters are poorly informed about the candidates and issues on the ballot. Most also lack a basic understandings of government structure and policies.⁵⁸ Indeed, the “limited effects” found by Alcott and Gentzkow of disinformation in the 2016 election may be floor effects that result from the already low level of information among the electorate.⁵⁹ 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.⁶⁰ More generally, voters

54. Paul & Matthews, *supra* note 18, at 3. *See also* Wu, *supra* note 11, at 15.

55. Hasen, *supra* note 10, at 2.

56. Wu, *supra* note 11, at 15.

57. Christopher S. Elmendorf, *Refining the Democracy Canon*, 95 CORNELL L. REV. 1051, 1076–93 (2009). *See* Gilbert, *supra* note 15, at 1858–61, 1866–69 (discussing voters’ interest in relevant information accountability in relation to campaign finance). *See also* *Citizens United v. FEC*, 558 U.S. 310, 364 (2010); *McConnell v. FEC*, 540 U.S. 93, 201 (2003); *Buckley v. Valeo*, 424 U.S. 1, 64 (1976).

58. There is a tremendous amount of literature in political science on these points. *See, e.g.*, Larry M. Bartels, *Uninformed Votes: Information Effects in Presidential Elections*, 40 AMER. J. POL. SCI. 194 *passim* (1996). *See also* James Druckman, *Does Political Information Matter?*, 22 POL. COMM. 515, 515–17 (2006) (summarizing the academic literature).

59. *See* Alcott & Gentzkow, *supra* note 1, at 229.

60. Elizabeth Garrett, *The Law and Economics of “Informed Voter” Ballot Notations*, 85 VA. L. REV. 1533, 1539–41, 1587 (1999). Additional information has varying sized effects, and more work is needed in the area. For example, party endorsements result in an increase in vote share of about eight percentage points. Thad Kousser, Seth Masket & Eric McGhee, *Kingmakers or Cheerleaders? Party Power and the Causal Effects of Endorsements*, 68 POL. RES. Q. 443, 453–54 (2015). The marginal effect of additional campaign finance information is harder to establish, at least in an information-saturated environment. *See* David M. Primo, *Information at the Margins: Campaign Finance Disclosure Laws, Ballot Issues, and Voter Knowledge*, 12 ELECT. L.J. 114,

have informational workarounds. They use heuristics, or informational shortcuts, to help them reach a decision.⁶¹ Uninformed voters can also take cues from elites they trust. If the cues from elites, or the information they provide, 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.⁶² Moreover, corrections can be misremembered and serve to further entrench the faulty information.⁶³

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 deepen 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.⁶⁴

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

127–28 (2013). See generally Wood, *Campaign Finance Disclosure*, *supra* note 15.

61. Arthur Lupia, *Shortcuts Versus Encyclopedias: Information and Voting Behavior in California Insurance Reform Elections*, 88 AM. POL. SCI. REV. 63, 63–64, 72 (1994).

62. Emily Thorson, *Belief Echoes: The Persistent Effects of Corrected Misinformation*, 33 POL. COMM. 460, 462 (2015).

63. Ian Skurnik et al., *How Warnings About False Claims Become Recommendations*, 31 J. CONSUMER RES. 713, 722–23 (2005).

64. See Christopher S. Elmendorf & Abby K. Wood, *Elite Political Ignorance: Law, Data, and the Representation of (Mis)Perceived Electorates*, 52 U.C. DAVIS L. REV. (forthcoming Dec. 2018) (manuscript at 35) (footnote omitted), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3034685.

the election, undermining a key First Amendment value that campaigning enhances the “marketplace of ideas.”

Online “echo chambers” are asymmetric and more common among conservatives than liberals.⁶⁵ Cass Sunstein proposes that a diversity of information and views are necessary to fix the problem of group polarization.⁶⁶ 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.”⁶⁷ 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.⁶⁸

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, makes 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.

II. FIRST AMENDMENT, POLITICAL SPEECH, AND CHOICE OF REGULATOR

Political opinions and information posted online are indisputably political speech and thus protected by the First Amendment. Activities that are less obviously “speech” have also been constitutionalized by courts deregulating in the name of the First Amendment. This includes political expenditures. The “constitutionalization” of campaign finance has implications for regulation of online political advertising, including

65. Pablo Barberá et al., *Tweeting from Left to Right: Is Online Political Communication More Than an Echo Chamber?*, 26 *PSYCHOL. SCI.* 1531–42 (2015) (arguing that echo chambers are more prevalent among political issues, like a presidential election, than issues described as a “national conversation,” like the Boston Marathon Bombing).

66. See Cass R. Sunstein, *The Law of Group Polarization*, 10 *J. POL. PHIL.* 175 *passim* (2002).

67. See Eytan Bakshy, Solomon Messing & Lada A. Adamic, *Exposure to Ideologically Diverse News and Opinion on Facebook*, 348 *SCIENCE* 1130, 1131 (2015).

68. See Craig Silverman, *This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook*, *BUZZFEED NEWS* (Nov. 16, 2016, 5:15 PM), <https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>.

disinformation advertising. 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. A lot of the remaining responsibility for reducing disinformation on social media falls to social media platforms. This is because doing so involves banning or restricting speakers or their speech—actions that would be unconstitutional for the government to require. Yet here's the rub: however much the platforms claim they want to self-regulate, their short-term profit motives suggest platforms will be, at best, unreliable and inconsistent self-regulators.

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.⁶⁹ Campaign finance cases analyze regulations differently depending on whether they ban speech or merely burden it in some way. Courts apply strict scrutiny to content regulation of political speech.⁷⁰ Several legislative attempts to regulate the content, amount, or source of political speech have met their demise under this standard.⁷¹ In order to survive strict scrutiny, the government must show that a regulation is necessary to serve a compelling state interest and is narrowly drawn to achieve that end.

The Court has granted “compelling interest” status to a limited set of campaign and election-related interests that governments try to protect via regulation. Preserving fair and honest elections and preventing foreign influence in our elections are compelling

69. Hasen, *supra* note 10, at 17 (citing Steven J. Heyman, *The Conservative-Libertarian Turn in First Amendment Jurisprudence*, 117 W. VA. L. REV. 231 (2014)).

70. 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 citations omitted). See also *281 Care Comm. v. Arneson*, 766 F.3d 774 (8th Cir. 2014).

71. See generally *McCutcheon v. FEC*, 572 U.S. 185 (2014) (striking down aggregate individual contribution limits); *Citizens United v. FEC*, 558 U.S. 310 (2010) (striking down a ban on independent expenditures from corporations’ treasuries); *Republican Party of Minn. v. White*, 536 U.S. 765 (2002) (discussing judicial issue-related speech).

government interests.⁷² Courts have acknowledged that the government “indisputably” has a compelling interest⁷³ in protecting election integrity and have upheld narrowly-tailored government regulations of some kinds of speech around elections. For example, the Court has upheld restrictions on our right to political speech in physical proximity to an election place, such as requiring a physical setback for political activities near polling places, banning campaign signs and clothing that advocates for a candidate or initiative near people who are voting.⁷⁴ And in *Bluman v. FEC*, the Supreme Court voiced strong views that the government has a compelling interest in limiting direct campaign contributions by foreign nationals, though the language is somewhat uncertain about other involvement of foreign nationals.⁷⁵

When it comes to the government’s interest in preventing fraud on the electorate, the Court has stopped short of calling the interest “compelling”, saying that it “carries special weight during election campaigns when false statements, if credited, may have serious adverse consequences for the public at large.”⁷⁶ T. Nevertheless, given the existing case law permitting restrictions in space, if not yet time (campaign season), the possibility remains open (though admittedly

72. See *Eu v. S.F. Cty. Democratic Cent. Comm.*, 489 U.S. 214, 231–32 (1989); *Bluman v. FEC*, 800 F. Supp. 2d 281, 288 (D.D.C. 2011), *aff’d*, 565 U.S. 1104 (2012).

73. See *Eu*, 489 U.S. at 230.

74. See *Burson v. Freeman*, 504 U.S. 191, 193–94, 197, 199 (1992). The Court recently struck down a vaguely-worded Minnesota law banning “political” apparel at polling stations. See *Minn. Voters All. v. Mansky*, 138 S. Ct. 1876, 1891–92 (2018). The Court analyzed it as a restriction in a nonpublic forum, and restrictions in such forums are reviewed only for reasonableness. *Id.* at 1885–86.

75. *Bluman v. FEC*, 800 F. Supp. 2d 281, 288 (D.D.C. 2011) (holding that the government may “bar foreign citizens . . . from participating in the campaign process”), *aff’d*, 565 U.S. 1104 (2012). See also *Oversight of Federal Political Advertisement Laws and Regulations: Testimony Before the Subcomm. on Info. Tech. of the Comm. on H. Oversight and Gov’t Reform*, 115th Cong. 5–12 (2017) (statement of Ian Vandewalker, Senior Counsel, Democracy Program, Brennan Center for Justice at NYU School of Law) (discussing the different steps Congress could take to regulate foreigner-sponsored political advertisements online), <https://www.brennancenter.org/sites/default/files/analysis/Testimony-IT-Subcom-U.S.House-Vandewalker-10.24.17.pdf>; Alyssa Markenson, *What’s at Stake: Bluman v. Federal Election Commission and the Incompatibility of the Stake-Based Immigration Plenary Power and Freedom of Speech*, 109 NW. U. L. REV. 209, 228–37 (2014). Rick Hasen points out a potential tension here with dicta in *Citizens United*, which, read at its broadest, could say that “the identity of the speaker does not matter for First Amendment purposes.” See Hasen, *supra* note 10, at 19. That would be a particularly aggressive read of *Citizens United*, effectively overturning *Bluman*. The prohibition upheld in *Bluman* was interpreted to exclude issue advocacy by foreign nationals. *Bluman*, 800 F. Supp. 2d at 284.

76. *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 349 (1995).

quite distant) that a that a narrowly-tailored prohibition on fraudulent online political speech could survive constitutional scrutiny where prior prohibitions on fraudulent speech have failed.⁷⁷ In the meantime, 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.⁷⁸

Where government regulation of political speech 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 overriding⁷⁹ or sufficiently important⁸⁰ government interest, which is substantially related,⁸¹ or even narrowly tailored,⁸² to meet it.⁸³ The primary government interest supported by the disclosure regulations the Court upheld in *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

77. We do not need to regulate fraudulent political speech for our proposed regulations; we merely note that the question is an open one. The Eighth Circuit struck down a regulation as being overbroad and specifically declined to decide whether preventing fraud on the electorate is a compelling government interest. *See* 281 Care Comm. V. Arneson, 766 F.3d 774, 787 (8th Cir. 2014). (“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.”). *United States v. Alvarez*, 567 U.S. 709, 714–16 (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. *Id.* at 714. 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 generally* Rebecca Brown, *The Harm Principle and Free Speech*, 89 S. CAL. L. REV. 953 (2016).

78. *Alvarez*, 567 U.S. at 721–22, 727 (“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.

79. *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 347 (1995).

80. *Citizens United v. FEC*, 558 U.S. 310, 339 (2010).

81. *Buckley v. Valeo*, 424 U.S. 1, 64 (1976).

82. *McIntyre*, 514 U.S. at 347.

83. *See* *Wis. Right to Life v. FEC*, 551 U.S. 449, 451 (2007) (citing *First Nat. Bank of Boston v. Bellotti*, 435 U.S. 765, 786 (1978)).



weight to different speakers and messages.”⁸⁴

The *Buckley* Court fleshed out the assumption, saying, “[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.”⁸⁵ 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.⁸⁶

Social science findings support the *Buckley* court’s hypothesis that disclosure informs voters. In a series of experiments, Dowling and Wichowsky have shown that campaign finance transparency affects voter opinion.⁸⁷ Adam Bonica has shown, using campaign finance data from decades of elections and legislator voting records at the state and federal level, that that campaign finance contributions are as strong a predictor of legislative behavior—as informative, in other words—as

84. See *Citizens United*, 558 U.S. at 371. 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. See *Citizens United*, 558 U.S. at 364; *McConnell v. FEC*, 540 U.S. 93, 201 (2003); *Buckley*, 424 U.S. at 64. One of us has argued elsewhere that a broader set of benefits is at play with campaign finance disclosure. For example, the government has an interest in securing the data necessary to evaluate its own campaign finance 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). See also Wood, *Campaign Finance Disclosure*, *supra* note 15.

85. *Buckley*, 424 U.S. at 66–67.

86. *Id.* 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 forty years. See, for example, the majority opinion in *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.” *Citizens United v. FEC*, 558 U.S. 310, 370–71 (2010).

87. Connor M. Dowling & Amber Wichowsky, *Does It Matter Who’s Behind the Curtain? Anonymity in Political Advertising and the Effects of Campaign Finance Disclosure*, 41 AM. POL. RES. 965 *passim* (2013) [hereinafter Dowling & Wichowsky (2013)]; Connor M. Dowling & Amber Wichowsky, *Attacks Without Consequence? Candidates, Parties, Groups, and the Changing Face of Negative Advertising*, 59 AM. J. POL. SCI. 19 *passim* (2015) [hereinafter Dowling & Wichowsky (2015)]; Travis N. Ridout et al., *Sponsorship, Disclosure and Donors: Limiting the Impact of Outside Group Ads*, 68 POL. RES. Q 154 *passim* (2015).

incumbent legislators' prior votes.⁸⁸ We also have evidence that voters demand disclosure and learn from a group or candidate's decision to not disclose.⁸⁹

While there is little judicial guidance on the constitutionality of government actions we propose in Part IV, the courts should uphold government efforts to educate voters and social media users about disinformation and fact-checking. Similarly, the courts would likely 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.⁹⁰

* * *

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 jurisprudence, and like all law, they were created in a specific historical context.⁹¹ The jurisprudence developed at a time when listeners were plentiful and speech less so. Recent Supreme Court majorities have interpreted the First Amendment to protect speakers, not listeners. Our transparency proposals fit this existing framework comfortably. But should government be able to do more to protect listeners from the "flood" of disinformation advertising before elections?

88. Adam Bonica, *Inferring Roll Call Scores from Campaign Contributions Using Supervised Machine Learning*, AMER. J. POL. SCI. (forthcoming 2018) (manuscript at 15), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732913.

89. See generally Abby K. Wood, *Show Me the Money: "Dark Money" and the Informational Benefit of Campaign Finance Disclosure* (Ctr. for Law & Soc. Sci., Research Paper No. CLASS17-24, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3029095. 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 15.

90. For more on the constitutionality of an opt-in or opt-out requirement, see Elmendorf & Wood, *supra* note 64, 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.") (footnotes omitted).

91. Wu, *supra* note 11 ("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.") (footnotes omitted).



The Internet platforms themselves lack a coherent theory of the First Amendment.⁹² Platforms are not merely a venue for debates in the “marketplace of ideas,” in which truth can eventually win out. The truth stood 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.⁹³ Nor are the platforms exclusively supportive of speakers’ personal autonomy to say whatever they want—another theory of the First Amendment. Terms of service for even the most libertarian platforms forbid behavior that is offensive, despite not being illegal. Platform users are speakers *and* listeners; and platforms should want to balance their interests. Unfortunately, only speakers pay platforms for their services, leading platforms to cater their terms of service to speakers rather than listeners. 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.⁹⁴ At best, they have adopted an inconsistent amalgam of these ideas.⁹⁵

As Volokh explains, with the advent of “cheap speech” online, intermediaries are weakened.⁹⁶ Speakers, freed from editorial gatekeeping, have 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.”⁹⁷ 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

92. Nabiha Syed, *Real Talk About Fake News: Towards a Better Theory for Platform Governance*, 127 YALE L.J. FORUM 337, 342–43 (2017).

93. 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 et al., *The Spread of False and True News Online*, 359 SCIENCE 1146, 1146–51 (2018).

94. Public discourse theory is not prominent in this libertarian age of free speech, but cases that fit its paradigm are not entirely unheard of. See, e.g., *Red Lion Broad. Co. v. Fed. Comm’n*, 395 U.S. 367, 367–68 (1969) (upholding broadcast fair time requirement on coverage of issues of public importance). See Robert Post, *The Constitutional Status of Commercial Speech*, 48 UCLA L. REV. 1, 7–8 (2000) (describing the theory and referring to several other works about it).

95. Syed, *supra* note 92, at 342–45.

96. Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805, 1834–38 (1995).

97. *Id.* at 1834–38, 1843.

through” than ever.⁹⁸ 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.”⁹⁹ 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.¹⁰⁰ Nevertheless, prior libertarian efforts to build a case for a “substantial overbreadth” doctrine would be less likely to succeed in the wake of the 2016 election campaign. Regulators can now show demonstrable damage,¹⁰¹ intent by meddlers (both foreign and domestic) to mislead *and* to affect elections, and involvement by two entities with little First Amendment protection: foreigners and non-humans.¹⁰²

98. Wu, *supra* note 11, at 13.

99. *Id.* at 23. 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. *Id.* at 25. 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 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.

100. Hasen, *supra* note 10, at 19–23.

101. These are serious harms. See generally Brown, *supra* note **Error! Bookmark not defined.** (describing an approach to free speech which takes into account the actual manner in which expression is alleged to cause harm). 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. Cecilia Kang, *Fake News Onslaught Targets Pizzeria as Nest of Child-Trafficking*, N.Y. TIMES (Nov. 21, 2016), <https://nyti.ms/2f0L9G9>. After the election, a man entered the pizza shop and fired three shots. Spencer S. Hsu, *Comet Pizza Gunman Pleads Guilty to Federal and Local Charges*, WASH. POST (Mar. 24, 2017), <http://wapo.st/2mZBNtT>.

102. Bots are essentially code, and whether code is speech is not yet clear. See Neil Richards, *Apple’s “Code = Speech” Mistake*, MIT TECH. REV. (Mar. 1, 2016), <https://www.technologyreview.com/s/600916/apples-code-speech-mistake> (arguing that the Government can and should regulate bots, as distinct from speech). However, even if it is speech, the level of scrutiny to be applied to computer code speech is not set in stone. See Universal City



B. CHOICE OF REGULATOR

Negative market externalities justify regulation. Market externalities are often conceived of as negative effects from market activity on our environment or public health—say, from air pollution. Here, the market activities are platforms chasing profits without exercising gatekeeping or transparency responsibilities, and the externalities are costs 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.

1. 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.”¹⁰³ The platforms are well situated, technologically, to minimize the amount of disinformation advertising that reaches their users and have already experienced some success in that regard.

Facebook and Twitter were the locations of most of the “attacks” in the 2016 election, and so this Article focuses on them. After dragging their heels,¹⁰⁴ both companies have taken steps to prevent future attacks, actions that are also aimed at heading off government regulation. The platforms have also continued to experience disinformation attacks.

The problem with leaning on platforms to self-regulate is their 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 scarcer

Studios v. Reimerdes, 111 F. Supp. 2d 294, 326–27 (S.D.N.Y. 2000). Following *Reimerdes*, the court in *Universal City Studios v. Corley*, 273 F.3d 429, 450 (2d Cir. 2001) found that code could have both speech and non-speech components, such that the functional (but not expressive) elements of the code may be targeted.

103. Persily, *supra* note 10.

104. *Id.*

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 implement, within a week, he had softened his stance and had begun to “both-sides” the issue, saying “[b]oth sides are upset about ideas and content they don’t like.”¹⁰⁵ 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.”¹⁰⁶ 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, their current efforts 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.¹⁰⁷ Industry self-regulation is almost never “pure” self-regulation, but involves a nexus to a government co-regulator. Government agencies provide legal

105. Zeynep Tufekci, Opinion, *Zuckerberg’s Preposterous Defense of Facebook*, N.Y. TIMES (Sept. 29, 2017), <https://nyti.ms/2yxUydy>.

106. *Id.* See also Nicholas Thompson & Fred Vogelstein, *Inside the Two Years that Shook Facebook—and the World*, WIRED (Feb. 12, 2018, 7:00 AM), <https://www.wired.com/story/inside-facebook-mark-zuckerberg-2-years-of-hell>.

107. Lisa L. Sharma et al., *The Food Industry and Self-Regulation: Standards to Promote Success and to Avoid Public Health Failures*, 100 AM. J. PUB. HEALTH 240, 242 (2010), (citing Neil Gunningham & Joseph Rees, *Industry Self-Regulation: An Institutional Perspective*. 19 LAW & POL’Y 363 (1997)).

backstops to the self-regulation negotiated by industry participants, along with imposition of civil or criminal penalties on violators.¹⁰⁸ Co-regulation stands the best chance of success when certain conditions exist. Most importantly, industry actors must be committed to the purpose of the regulation.¹⁰⁹ 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 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.”¹¹⁰

An analogy to co-regulation by an industry group closely related to the issue at hand illustrates industry self-regulation with government backstops. The Digital Advertising Alliance runs an opt-out program from online advertisements based on cookie-tracking.¹¹¹ The industry enforcement process consists of confidential review of complaints by a committee, followed by board-level censure, membership suspension or expulsion, referral to the Federal Trade Commission or law enforcement, and publicity for non-compliance.¹¹² By comparison, the platforms’ initial offerings to address disinformation advertising are paltry. It took Facebook over a year to even suggest it would reach out to other companies to “share information on bad actors and make sure they stay off all platforms.”¹¹³ We are a long way from effective and comprehensive industry self-regulation or co-regulation. Therefore, we must consider ways the government can constitutionally, and effectively, regulate in this area.

108. Neil Gunningham & Joseph Rees, *Industry Self-Regulation: An Institutional Perspective*, 19 LAW & POL’Y 363, 401–02 (1997).

109. Edward J. Balleisen & Marc Eisner, *The Promise and Pitfalls of Co-Regulation: How Governments Can Draw on Private Governance for Public Purpose*, in NEW PERSPECTIVES ON REGULATION 128 (David Moss & John Cisternino eds., 2009), https://www.tobinproject.org/sites/tobinproject.org/files/assets/New_Perspectives_Ch6_Balleisen_Eisner.pdf.

110. *Id.* at 129.

111. *Online Behavioral Advertising Compliance*, DATA & MARKETING ASS’N, <https://thedma.org/resources/compliance-resources/online-behavioral-advertising-compliance> (last visited Sept. 6, 2018).

112. The “failure to correct” report includes a list of the guidelines violated. DATA & MKTG. ASS’N, DMA ANNUAL ETHICS COMPLIANCE REPORT, JANUARY–DECEMBER 2016, at 21 (2016), <https://thedma.org/wp-content/uploads/Jan-Dec-2016-Ethics-Compliance-Report.pdf>.

113. Josh Constine, *Facebook Will Hire 1000 and Make Ads Visible to Fight Election Interference*, TECHCRUNCH (Oct. 2, 2017), <https://techcrunch.com/2017/10/02/facebook-will-hire-1000-and-make-ads-visible-to-fight-election-interference>.

2. 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 platforms to collect information and provide it to the government or directly to the public in a uniform format. Standardized reporting allows the public, watchdog groups, journalists, and scholars to compare across platforms and over time in their data analysis. 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 policymakers have been so quiet in the face of disinformation advertising and multiple strong statements by national security experts sends important signals to the attackers and the public. The attackers learn that they may continue with impunity. The public may perceive that government does not take the attacks seriously.

Government regulation also matters because law has expressive value.¹¹⁴ 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.¹¹⁵ 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,

114. See generally RICHARD H. MCADAMS, *THE EXPRESSIVE POWERS OF LAW: THEORY AND LIMITS* (2015) (proposing that, under certain circumstances, an expressive mechanism causes compliance with a law more so than deterrence or legitimacy); Robert Cooter, *Expressive Law and Economics*, 27 J. LEGAL STUD. 585, 585–608 (1998) (discussing an economic theory of expressive law); Richard H. McAdams, *An Attitudinal Theory of Expressive Law*, 79 OR. L. REV. 339 (2000) (discussing a “causal theory for the expressive effect of law”) [hereinafter McAdams, *An Attitudinal Theory*]; Richard H. Pildes & Cass R. Sunstein, *Reinventing the Regulatory State*, 62 U. CHI. L. REV. 1, 66 (1995) (discussing the expressive dimensions of legal and political decision-making).

115. McAdams, *An Attitudinal Theory*, *supra* note 114, at 342–43. Similarly, removing legal requirements also affects behavior. See, e.g., Patricia Funk, *Is There an Expressive Function of Law? An Empirical Analysis of Voting Laws with Symbolic Fines*, 9 AMER. L. & ECON. REV. 135, 148–51 (2007).

policymakers should keep in mind that

[p]olicy 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.¹¹⁶

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 address the disinformation problem head-on. 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 III.

III. OUR CURRENT, INSUFFICIENT, REGULATORY FRAMEWORK FOR ONLINE POLITICAL ADVERTISING

In the years leading up to the 2016 election, voters learned 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

116. Pildes & Sunstein, *supra* note 114, at 66.

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.”¹¹⁷ 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. First, it is more likely to be disguised as informational content, or “native.” 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. And fourth, it is much cheaper. All of these features matter to shaping a regulatory framework that helps the public trace the source of the (dis)information they view online and the government keep foreign influence out of our elections. In this Part, we describe the current regulatory framework and its gaps.

“Public communications.” 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.¹¹⁸ Importantly, the current definition excludes Internet ads “except for communications placed for a fee on another person’s or entity’s website.”

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.”¹¹⁹ On broadcast, cable, and satellite political messages, the FEC requires

117. Eric Lichtblau, *F.E.C. Can’t Curb 2016 Election Abuse, Commission Chief Says*, N.Y. TIMES (May 2, 2015) (internal quotation omitted), <https://nyti.ms/1E4sjOu>. See generally Russ Choma, *Get Ready for a Flood of Online Campaign Ads that Will Target and Track You*, MOTHER JONES (Sept./Oct. 2015), <http://www.motherjones.com/politics/2015/08/digital-political-election-ads-dark-money> (describing how online advertising can be used by political groups to gain valuable information about voters with minimal disclosure).

118. 11 C.F.R. § 110.11(a)(1) (2018).

119. *Id.* § 110.11(b)(2)–(3). Examples taken from FED. ELECTION COMM’N, SPECIAL NOTICES ON POLITICAL ADS AND SOLICITATIONS 4 (2006), https://transition.fec.gov/pages/brochures/spec_notice_brochure.pdf.

disclaimers on all public communications (1) made by a political committee, (2) expressly advocating for the election or defeat of a “clearly identified” candidate, or (3) soliciting contributions.¹²⁰ Disclaimers 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 sixty days or fewer before a general election or thirty days or fewer before a primary.¹²¹ When we apply these four disclaimer triggers to Internet communications, regulatory coverage and disclaimer requirements decrease substantially. The first three triggers, for communications from political committees, containing express advocacy or solicitations, apply only where the communication is “placed for a fee.”¹²² The fourth, electioneering communications, is completely inapplicable, because electioneering communications are defined to *exclude* political messaging on the Internet.¹²³

As noted in Part I, 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. Because they were placed online, we do not know who paid for them.¹²⁴

When we combine the current definition of political communications with the current disclaimer requirements, we end up

120. 11 C.F.R. § 110.11(a)(1)–(3).

121. *Id.* § 110.11(a)(4); *Id.* § 100.29(a)(1)–(3). The FEC has recently upheld the disclaimer requirement for paid Facebook ads featuring express advocacy. FEC, Advisory Opinion 2017-12 (Dec. 15, 2017).

122. 11 C.F.R. § 100.26 (2018) (“*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.”) (emphasis added); *Id.* § 110.11(a) (defining the scope of disclaimer requirements as limited to public communications, as defined in 11 C.F.R. § 100.26 (2018), and electioneering communications, which, as defined in 11 C.F.R. § 100.29(c)(1) (2018), exclude communications over the Internet).

123. *Id.* § 100.29(a), (c)(1) (2018).

124. *See Id.* § 100.29(c)(1).

with the following: 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 is either willing to disregard the regulatory requirements, is spending below the threshold requiring regulatory compliance, or would claim an exemption under the “small items” or “impracticable” exceptions to disclaimer requirements.¹²⁵ 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.¹²⁶ The impracticable exception applies to communications in skywriting, water towers, and clothing, where it would be too difficult to include a disclaimer.¹²⁷ However, applying these exceptions to political advertising would have been disingenuous. 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 provided 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 fewer than 200 characters of text could qualify under either exception;¹²⁸ a 3-3 vote resulted that was long interpreted as an exemption.¹²⁹ The FEC has since clarified that a disclaimer is required, but they could not agree on the rationale.¹³⁰ The FEC has also recently failed to decide whether nonconnected political

125. *Id.* § 110.11(f)(1)(i)–(ii).

126. *See Id.* § 110.11(f)(1)(i).

127. *See Id.* § 110.11(f)(1)(ii).

128. Facebook, FEC Advisory Op. Request 2011-09 (Apr. 26, 2011), <http://saos.fec.gov/aodocs/1174825.pdf>; FEC, Advisory Opinion 2011-09 (June 15, 2011) (Facebook) (certification of vote), <http://saos.fec.gov/aodocs/1176290.pdf>; FEC, Advisory Opinion 2011-09 (June 15, 2011) (Facebook) (agenda), <http://saos.fec.gov/aodocs/1176195.pdf>.

129. Google’s AO request did propose a disclaimer on a landing page. Google, FEC Advisory Op. Request 2010-19 (Aug. 5, 2010), <http://saos.fec.gov/saos/searchao?AONUMBER=2010-19>.

130. FEC, Advisory Opinion 2017-12, at 2 n.1 (Dec. 15, 2017).



committees¹³¹ may use Twitter without placing a disclaimer on their Twitter profiles.¹³² 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.¹³³ Campaigns, party committees, and PACs must all submit regular reports to the FEC, disclosing their contributions and expenditures.¹³⁴ 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 either make independent expenditures or to support groups that do.¹³⁵ These “dark money” groups are not required to publicly disclose their donors.¹³⁶ 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.)¹³⁷

131. Nonconnected committees are a class of committees that includes Leadership PACs and SuperPACs. *Types of Nonconnected PACs*, FED. ELECTION COMM'N, <https://www.fec.gov/help-candidates-and-committees/registering-pac/types-nonconnected-pacs> (last visited Sept. 6, 2018).

132. FEC, Advisory Opinion 2017-05 (Sept. 20, 2017), <https://www.fec.gov/files/legal/aos/83543.pdf> (Great America PAC & The Committee to Defend the President).

133. See Liz Kennedy & Alex Tausanovitch, *Secret and Foreign Spending in U.S. Elections: Why America Needs the DISCLOSE Act*, CTR. FOR AMER. PROGRESS (July 17, 2017), <https://www.americanprogress.org/issues/democracy/reports/2017/07/17/435886/secret-foreign-spending-u-s-elections-america-needs-disclose-act>. See generally *WMP/CRP Special Report Outside Group Activity, 2000–2016*, WESLEYAN MEDIA PROJECT (Aug. 24, 2016), <http://mediaproject.wesleyan.edu/blog/disclosure-report> (examining outside group advertising in elections).

134. *The FEC and the Federal Campaign Finance Law: Disclosure*, FED. ELECTION COMM'N, <http://classic.fec.gov/pages/brochures/fecfeca.shtml#Disclosure> (last visited Sept. 6, 2018).

135. Although the primary purpose of 501(c)s must be non-political, they may participate in limited election activities so long as they do not solicit funds with the specification that they will be used for an election-related purpose. 26 U.S.C. § 501(c)(4)(a) (2012). See also ERIKA FRANKLIN FOWLER ET AL., *POLITICAL ADVERTISING IN THE UNITED STATES* 33 (2016). Instead, 501(c)s solicit money generally and may direct some of their resources toward political activities such as purchasing issues ads.

136. See *Political Nonprofits (Dark Money)*, OPEN SECRETS, https://www.opensecrets.org/outsidespending/nonprof_summ.php (last updated Sept. 6, 2018).

137. *Wyden Demands Documents on Possible Links Between Russian Money and NRA*, CBS

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.¹³⁸ Congress has prohibited the Securities and Exchange Commission from using appropriated funds to draft or implement rules requiring the corporations it regulates to disclose political spending.¹³⁹

Transaction-level disclosures are important. In order to aid enforcement on broadcast, cable, satellite, and radio ads, the Federal Communications Commission (“FCC”) requires reporting of the financial details of a transaction purchasing an ad, 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.

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.¹⁴⁰ The restriction was upheld in *Bluman v. Federal Election Commission*.¹⁴¹ 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.¹⁴²

Of course, some disinformation ads are merely “issue ads.” They

NEWS (Feb. 2, 2018), <https://www.cbsnews.com/news/wyden-demands-documents-on-possible-links-between-russian-money-and-nra>.

138. Andy Kroll, *How Secret Foreign Money Could Infiltrate US Elections*, MOTHER JONES (Aug. 8, 2012), <http://www.motherjones.com/politics/2012/08/foreign-dark-money-2012-election-nonprofit>.

139. Consolidated Appropriations Act, Pub. L. No. 115-31, 131 Stat. 135 (2017). A similar prohibition exists for IRS.

140. 11 C.F.R. § 110.20(e)–(f) (2018).

141. See *Bluman v. FEC*, 800 F. Supp. 2d 281, 288 (D.D.C. 2011). See also 52 U.S.C. § 30121 (2012); 11 C.F.R. § 110.20 (2018); Matea Gold, *Did Facebook Ads Traced to a Russian Company Violate U.S. Election Law?*, WASH. POST (Sept. 7, 2017), http://wapo.st/2wL7Mpc?tid=ss_tw-bottom&utm_term=.d298c9e82dd8.

142. 11 C.F.R. § 100.16 (2018).

seek to influence voters by shifting public perception, but do not advocate for the election of or defeat of any particular candidate or even mention a candidate. Under our current regulatory framework, a hostile foreign government can 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.¹⁴³

In sum, because of outdated loopholes, we face the reality that disinformation advertisements, which often mention or display candidate names and images and would be considered electioneering communications if placed elsewhere, are distributed online with no disclaimers, little disclosure, and, sometimes, with 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 communicate with voters in the very near future.¹⁴⁴ Excluding a large portion of online advertising from disclosure and disclaimer regulations is problematic, particularly in light of the studies reviewed in Part II suggesting that disclaimers and disclosures provide information that affects voter decisions, and the court's longstanding belief that using disclosure to inform voters is a compelling government interest.

IV. CONSTITUTIONALLY-PERMISSIBLE REGULATIONS TO ADDRESS DISINFORMATION ADVERTISING

We now turn to our proposals. We focus on transparency, education, and “nudges” that government can constitutionally implement. The reforms we propose would reach any political advertising that is placed, promoted, or produced for a fee. 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: (1) cost and (2) intent to influence peoples' votes. Political ads cost money to

143. See *Bluman*, 800 F. Supp. 2d at 284; Entous, *supra* note 20.

144. Sydney Ember, *Digital Ad Spending Expected to Soon Surpass TV*, N.Y. TIMES (Dec. 7, 2015), <https://nyti.ms/1Qq9rTV>.

produce, post, or disseminate—including payments for microtargeting, any off-platform payments to “bot farms,” and paid “likes” and “shares” for distribution. Political ads also aim to influence elections. Evidence that an ad aims to influence the election, rather than merely discuss “issues” is a 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 the window is meaningless in the online setting, in which an ad can persist over time.

An example may help 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 federal rules, no matter when it runs, and 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 federal 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 federal rules, this meme requires 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 federal 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” its 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.

Before social media, most ads appeared on television, radio, or in print. They were fewer in number, limited in time, and targeted large groups of the electorate. In that context, it was easier to police the line between electioneering advertising and issue 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

As more political advertising moves online, without regulatory changes, the likelihood that voters see untraceable ads increases. 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 these funding sources 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 making political expenditures offline.¹⁴⁵ A regulation adopting disclosure and disclaimer rules for online advertisements would be a step in the right direction. We also propose a repository to facilitate real-time transparency of all online political ads as well as ex post enforcement of campaign finance rules. In this Section, we discuss three transparency-related regulatory changes for online political advertising.

1. Require Platforms to Keep and Disclose all Political Communications and Audiences

Government should require political advertisers on large social media 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, across platforms, 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 political 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

145. For a discussion of the media exemption, see *supra* Part I. But we reiterate here that Facebook Pages and fake newspapers like the nonexistent “Denver Guardian” do not qualify for the media exemption. We discuss below why we think the current proposal in the Senate, with its \$500 threshold, is too high.

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 we propose is simply an improved version of the Political File for television commercials. The design of the Political File is outdated,¹⁴⁶ and our political advertising repository will better serve our current technological abilities and democratic needs, with which political advertisers already comply, and which reveals their targets.¹⁴⁷ Of course, political advertisers will protest that this disclosure burdens their speech by requiring that they disclose their microtargeting strategies. The objection is weak, considering they reveal targets via the Political File already. Crucially, the Political File contains targeting information, because the broadcaster, time of day, and programming are all disclosed. A media company’s audience at a

146. The Political File 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 handwritten, making it difficult to glean systematic data quickly.

147. The Federal Communications Commission’s (“FCC”) 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) [(2018)]) (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 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.

About Public Inspection Files, FED. COMM’NS COMM’N, <https://publicfiles.fcc.gov/about-station-profiles> (last visited Sept. 7, 2018). The Political File requirements for cable (47 C.F.R. § 76.1701(d) (2018)) and satellite (47 C.F.R. § 25.701(d) (2018)) 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.” *About Public Inspection Files*, FED. COMM’NS COMM’N, <https://publicfiles.fcc.gov/about-station-profiles> (quoting 47 C.F.R. § 76.1701(d) (2018)) (last visited Sept. 7, 2018).

certain time of day for a certain program is a particular set of people the advertiser is targeting.

Consider an example to illustrate how television advertising already embeds audience information. When a campaign runs a television ad during an 8:30 p.m. 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.¹⁴⁸ Online targeting can be “narrower,” in that the communications can be targeted to a smaller group of people, but just because online targeting strategies are more precise does not grant the speakers more First Amendment protection. The size of the audience is irrelevant to the constitutional question of 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 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.¹⁴⁹

The repository is particularly helpful when it comes to enforcement. Advertisers peddling disinformation—particularly those located abroad—have little incentive to make truthful and timely disclosures and disclaimers. Penalties occur long after the election after all. The current enforcement mechanism is triggered with a complaint to the FEC. It is a purely reactive system, and it relies on a complainant

148. Hillary Clinton’s campaign paid \$3,000 for a thirty-second spot on March 9, 2016, during “Blackish” on KDNL-TV, in the St. Louis area. *Hillary For America Political File*, KDNL-TV, FED. COMM’N’S COMM’N, <https://publicfiles.fcc.gov/tv-profile/kdnl-tv/political-files/2016/federal/president/a1315a49-66c8-b09e-306f-20b3b4e49d9a> (follow “Hillary for America” hyperlink) (last visited Sept. 7, 2017).

149. *U.S. v. Alvarez*, 567 U.S. 709, 726–27 (2012) (“The remedy for speech that is false is speech that is true.”). *Arizona Free Enterprise Club v. Bennett* contains dicta implying that facilitating more speech is not a valid regulatory objective under the First Amendment. *Ariz. Free Enter. Club v. Bennett*, 564 U.S. 721, 750 (2011) (“‘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. *Id.* at 727–28. Here, the regulation we propose (along with 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*.

actually seeing the offending content. The advertising repository we propose facilitates decentralized enforcement by allowing groups to flag disclaimer violations after they occur. It is therefore crucial that the repository hold communications for a reasonable length of time. Television stations and cable and satellite companies are required to maintain the Political File for two years. The Honest Ads Act, a Senate bill introduced in 2017—which calls for a repository—would require platforms to retain the communication for four years.¹⁵⁰ Facebook’s current advertising archive holds ads for seven years. Maintaining the repository for the duration of the campaign plus a reasonable amount of time post-campaign is important.¹⁵¹

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, act based on it, and report to the public the current state of affairs in online political advertising. And yes, opposing campaigns can run counter-messaging based on it, just as they can with disclosures to the Political File for television.

150. Honest Ads Act, H.R. 4077, 115th Cong. (2017).

151. Antonio García Martínez, who “helped create Facebook’s ad machine,” is skeptical that a repository of every ad run would be informative to viewers. Antonio García Martínez, *I Helped Create Facebook’s Ad Machine. Here’s How I’d Fix It*, WIRED (Sept. 22, 2017, 3:55 PM) [hereinafter García Martínez, WIRED], <https://www.wired.com/story/i-helped-create-facebooks-ad-machine-heres-how-id-fix-it>.

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.

Id. 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 content.” *Id.* The regulatory cat-and-mouse game that emerges is fairly obvious. Advertisers will be incentivized to bury truly objectionable or hateful content as a needle in a haystack of otherwise fairly neutral content, but we are confident that it is not beyond the technological reach of sophisticated campaigns and analysts to find and expose the problematic content.

These transparency requirements should also have the effect of reducing the incentives to produce disinformation advertising and other any divisive advertising microtargeted at small subsets of the population. Microtargeting is not, in itself, bad. But 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 about the political preferences of constituencies.¹⁵² 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, targeting people who had expressed interest in “LGBT community, black social issues, the Second Amendment, and Immigration.”¹⁵³ If advertisers are required to post every version of every ad on the same site, along with targeting information, voters could detect when a group is trying to “divide and conquer” parts of the electorate. The message will reach voters via informational intermediaries. 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.¹⁵⁴

i. Triggering Conditions

Which online messages should be subject to transparency rules? Three, non-exclusive options are possible: (1) the traditional bright line rule of candidate or ballot initiative mentions; (2) a more-easily

152. See Elmendorf & Wood, *supra* note 64, at 33; Ryan D. Enos & Eitan D. Hersh, *Campaign Perceptions of Electoral Closeness: Uncertainty, Fear and Over-Confidence*, 47 BRIT. J. POL. SCI. 501, 502 (2015).

153. Carol D. Leonning et al., *Russian Firm Tied to Pro-Kremlin Propaganda Advertised on Facebook During Election*, WASH. POST (Sept. 6, 2017), <http://wapo.st/2gN5NLF>.

154. 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 plugins, and as clever activists attempt to “gamify” learning about campaign advertising.

automated rule of identifying political content by targeting; and (3) 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.¹⁵⁵ Inclusion in the repository does not mean that disclaimers 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 Section IV.C.

a. 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 for the ballot. Given that disinformation advertising preceded the 2016 election by more than a year, we believe this modest temporal expansion for electioneering communications is wise given the realities of campaigning. We also believe that tying the expansion to declarations of candidacy and ballot qualification—when campaigning heats up—helps its chances against a First Amendment challenge.¹⁵⁶ Our proposal is also gameable, encouraging groups to place as many ads as they can without repository capture before their

155. 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 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.

156. We are not alone. *See, e.g.*, Kennedy & Tausanovitch, *supra* note 133. Facebook has gone beyond this in its current iteration of the Archive, with all political ads, issue or advocacy, subject to retention in the archive whenever they are placed. *Shining a Light on Ads with Political Content*, FACEBOOK NEWSROOM (May 24, 2018), <https://newsroom.fb.com/news/2018/05/ads-with-political-content>. Their choice is less “gameable” and less administratively intense than our proposal, which is a more modest extension of current regulations.

preferred candidate declares, in hopes that they will still be circulating as the election approaches. Nevertheless, without more research into the realities of online political messaging over time, our proposal is as far as we think policymakers can confidently go within the bounds of the First Amendment.

Facebook already monitors ad content in order to minimize the amount that violates its terms of service.¹⁵⁷ It prohibits or restricts advertising for tobacco, drugs (illegal or prescription), weapons, adult content, “sensational content” (“[a]ds 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—until the post-2016 disinformation advertising political maelstrom—was entirely automated, though Facebook has begun to include humans in advertising review. Our broader point is that reviewing ads for mentions of candidates and political issues is not difficult, particularly with human involvement.¹⁵⁸

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 about the content of their ads. 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.

b. Political Targeting Categories

157. Facebook’s ad review process says that Facebook will “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 Sept. 7, 2018).

158. One aspect of our trigger proposal would be more difficult to administer than the all-ads system that Facebook chose: the platforms would need a complete list of all candidates running for office anywhere in the country to only archive ads placed after candidates announce and issues appear on the ballot. They can work with federal, state, and local regulators 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. On the other hand, if platforms adopt Facebook’s approach of archiving all political ads without regard to the timing of the election, this is an example of private regulation going further than public regulation might be able to.

Another triggering criteria would be easy for social media companies to automate. 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 other similar categories. 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.¹⁵⁹

c. 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.”¹⁶⁰ There are teams assigned to campaigns for each major party. Antonio García Martínez, 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 right to political advertising.”¹⁶¹ For the platforms, the “know your customer” approach is useful for creating a “gate” that allows platforms to avoid obvious foreign money and to intercept and stop foreign disinformation advertising in our elections. A similar intervention could 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.¹⁶²

159. EITAN HERSH, HACKING THE ELECTORATE: HOW CAMPAIGNS PERCEIVE VOTERS 168–69 (2015).

160. Antonio García Martínez, *I'm An Ex-Facebook Exec: Don't Believe What They Tell You About Ads*, GUARDIAN (May 2, 2017), <https://www.theguardian.com/technology/2017/may/02/facebook-executive-advertising-data-comment>.

161. García Martínez, WIRED, *supra* note 151.

162. Facebook’s current proposal is to require a U.S. driver’s license and a social security number to promote content. Sarah Perez, *Facebook’s New Authorization Process for Political Ads Goes Live in the US*, TECHCRUNCH (Apr. 23, 2018), <https://techcrunch.com/2018/04/23>

Facebook does not currently gate political account creation from the beginning.¹⁶³ 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.

ii. 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—perhaps it is underinclusive. What is special about the online context—why not require a repository for offline messaging as well, such as mailers and print ads? Some cities, like Los Angeles, require that all campaign and independent expenditure communications be retained and disclosed, which includes any “message that conveys information or views in a scripted or reproduceable format, including but not limited to paper, audio, video, telephone, electronic, Internet, Web logs, and social media.”¹⁶⁴ Requiring retention and disclosure of printed communications is helpful and important, but it is less urgent than creating a repository for online ads, because printed materials do not disappear like online ads currently can. Enforcement of our disclosure, disclaimer, and substantive campaign finance rules for online political advertising 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 faux-organic

[/facebook-new-authorization-process-for-political-ads-goes-live-in-the-u-s.](#)

163. We are grateful to Antonio García Martínez, a former Facebook employee, for this insight.

164. L.A., CAL., CODE § 49.7.2.F, § 49.7.31–.32 (2018), https://ethics.lacity.org/PDF/laws/law_CFO.pdf.

posts are detectible now.¹⁶⁵ 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.¹⁶⁶ 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.

iii. Current Efforts to Aggregate Ads

Facebook is the most advanced of the platforms in its efforts to collect political communications, but its efforts still fall short of what its users deserve. In May 2018, Facebook posted an Archive of Ads with Political Content. The Archive discloses the Page that paid for the ad, all ads run by the Page, and the audience makeup, but not the targeting criteria.¹⁶⁷ While the Facebook’s Archive addresses several reforms we have requested publicly in the past eighteen months, their design falls short in several important ways.¹⁶⁸ First, because it does not require information about the true source of the communications, voters still do not know who is speaking to them. Rather, they know who paid to boost an ad into their feeds. Second, the Facebook Archive does not provide the targeting categories or an audience ID for a list of users that were targeted with the political communication. The Archive reveals age and gender distribution of the audience, as well as the state in which they reside, but those are certainly not the only targeting

165. As we finalize this Article, Twitter has purged 70 million fake accounts and bots—around 20% of its user base. Craig Timberg & Elizabeth Dwoskin, *Twitter Is Sweeping Out Fake Accounts Like Never Before, Putting User Growth at Risk*, WASH. POST (July 6, 2018), <https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk>.

166. See Indictment ¶¶ 6–7, U.S. v. Internet Research Agency, L.L.C., 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018), <https://www.justice.gov/file/1035477>.

167. This is an improvement over what was promised, which was disclosure of “which page paid for an ad, [and the ability to] visit an advertiser’s page and see the ads they’re currently running to any audience on Facebook.” Mark Zuckerberg, FACEBOOK (Sept. 21, 2017), <https://www.facebook.com/zuck/posts/10104052907253171>.

168. Christopher S. Elmendorf et al., Opinion, *Open Up the Black Box of Political Advertising*, S.F. CHRON. (Sept. 23, 2017), <http://www.sfchronicle.com/opinion/openforum/article/Open-up-the-black-box-of-political-advertising-12221372.php>.



criteria used. For any given ad, the women and men of various ages were not targeted merely because of their age, sex, and location; they were targeted because of other information that Facebook knows about them, such as what issue-oriented groups or other candidates they like or follow on the platform. A candidate who is the subject of a disinformation campaign would not be able to speak to the same audience unless she spoke to the entire population in the geographic areas targeted by the disinformative campaign. This is no remedy for disinformation attacks on social media. Moreover, the First Amendment does not require this level of protection for disinformative political speech. Facebook should make targeting criteria plain, to enable counter speech. Third, the Archive affects only one corner of the vast world of social media, when we know industry-wide coordination is needed.

Looking around the industry, each platform has suggested its own “fixes,” all of which suffer the ills of not providing targeting criteria and not requiring information about the true source of the communication.¹⁶⁹ Moreover, the platforms’ proposals are not coordinated, but will create an overlapping web of platform-specific fixes. Voters want to know who is trying to influence them, and to accomplish this, they need one online “file” for all political communications, which is easily searchable, and which is divided into categories of who was targeted and for what reason.

The Honest Ads Act 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.¹⁷⁰ 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

169. See, e.g., Kent Walker, *Supporting Election Integrity Through Greater Advertising Transparency*, GOOGLE: KEYWORD (May 4, 2018), <https://www.blog.google/outreach-initiatives/public-policy/supporting-election-integrity-through-greater-advertising-transparency>.

170. Honest Ads Act, H.R. 4077, 115th Cong. (2017).

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.¹⁷¹ For \$250, an ad will have 25,000 “impressions,” appearing in the newsfeeds of 25,000 people.¹⁷² 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.¹⁷³ 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.

2. 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

171. See generally HERSH, *supra* note 159 (discussing the consequences of the use of microtargeting by campaigns during elections); SASHA ISSENBERG, *THE VICTORY LAB: THE SECRET SCIENCE OF WINNING CAMPAIGNS* (2012) (discussing how social science and analytics are changing political campaigns); DANIEL KREISS, *PROTOTYPE POLITICS: TECHNOLOGY-INTENSIVE CAMPAIGNING AND THE DATA OF DEMOCRACY* (2016) (providing an analytical framework for understanding why and how campaigns are newly “technology-intensive”).

172. Impressions are simply “eyeballs on ads”. The cost every time someone clicks on an ad through to a landing page (the “click through” rate) is higher, ranging from around 22 to 30 cents per click over the time we’ve written this Article. However, many disinformation ads clicked through to non-functioning landing pages, meaning that they are probably placed for impressions, rather than clicks. Constant repetition in one’s newsfeed from outlandish headlines with provocative pictures may be enough to suppress one’s enthusiasm for a candidate or conversely to mobilize her opponents.

173. García Martínez 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. García Martínez, *supra* note 151.

“for free” is still political advertising, and the public has a right to know who paid for its creation or distribution.¹⁷⁴ 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.¹⁷⁵ It held a hearing about online advertising disclaimers,¹⁷⁶ but given the political and institutional realities of that body in 2018 (with a bare quorum and inability to agree on many issues), 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.¹⁷⁷ 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.¹⁷⁸

174. FEC, Advisory Opinion 2010-19 (Oct. 8, 2010) (Google, Inc.); FEC, Advisory Opinion 2011-09 (June 15, 2011) (Facebook) (certification of vote); FEC, Advisory Opinion 2011-09 (June 15, 2011) (Facebook) (agenda); FEC, Advisory Opinion No. 2017-05 (Sep. 20, 2017) (Great America PAC & Comm. to Defend the President).

175. FEC, Advisory Opinion 2017-12 (Dec. 15, 2017) (Take Back Action Fund).

176. *FEC Holds Hearing on Internet Communication Disclaimers*, FED. ELECTION COMM’N (June 28, 2018), <https://www.fec.gov/updates/fec-holds-hearing-internet-communication-disclaimers>.

177. *Basic Rules for Disclaimers on Radio and TV Ads*, FED. ELECTION COMM’N (Oct. 21, 2014), <https://www.fec.gov/updates/basic-rules-for-disclaimers-on-radio-and-tv-ads>.

178. Research in political science suggests that this kind of enhanced disclosure can moderate the effectiveness of negative advertising. Dowling & Wichowsky (2013), *supra* note 87; Dowling & Wichowsky (2015), *supra* note 87. Given that disinformation advertising is almost all negative against one candidate, enhanced disclaimers should reduce their 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 POL. (Dec. 2016) (Figure4), <http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-217>.

3. 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, voters cannot “follow the money” without extending disclosure requirements to corporations making independent expenditures.

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.¹⁷⁹ Money is passed from group to group in a “daisy chain” of limited transparency.

We do not know what share of online ads is 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. 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. User education is paramount. Scholars call 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,”¹⁸⁰ preemptive warnings to people about

179. See WMP/CRP *Special Report Outside Group Activity, 2000–2016*, *supra* note 133; Kennedy & Tausanovitch, *supra* note 133.

180. John Cook et al., *Neutralizing Misinformation Through Inoculation: Exposing Misleading Argumentation Techniques Reduces Their Influence*, 12 PLOS ONE 1, 10 (2017).

tactics used to spread misinformation,¹⁸¹ and even online games that teach the main strategies of disinformation.¹⁸²

A simple education campaign on platforms can inoculate users, helping them learn how to avoid spreading disinformation. For example, users can be taught how to tighten their security settings and reminded not to interact with disinformation in their newsfeeds, because the algorithms promote content based on interactions with it. Whether this requirement would invite a challenge as “compelled speech” under normal circumstances, it seems unlikely that platforms would protest it in this political climate. On firmer constitutional ground, though much more expensively, the government could pay to place inoculating ads on the platforms.

Viewing less disinformation in the first place is important, because 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.¹⁸³ An opt-out system for consumer and service 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. Default settings can be sticky.¹⁸⁴ For example, under the AdChoices program, only a small number of people actually opt out.¹⁸⁵ If government required platforms to default users to not view narrowly targeted political or issue ads, and instead platforms

181. Sander van der Linden et al., *Inoculating Against Misinformation*, 358 SCIENCE 1141, 1141 (2017).

182. See *Bad News*, GETBADNEWS, getbadnews.com (last visited Sept. 8, 2018) (hosting a game designed by Cambridge Social Decision-Making Lab members).

183. 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.

184. See Omri Ben-Shahar & John A.E. Pottow, *On the Stickiness of Default Rules*, 33 FLA. ST. U. L. REV. 651 *passim* (2005).

185. Kate Kaye, *Study: Consumers Don't Know What AdChoices Privacy Icon Is*, AD AGE (Jan. 29, 2014), <http://adage.com/article/privacy-and-regulation/study-consumers-adchoices-privacy-icon/291374>.

offered to users the choice to opt-in to viewing that content, low uptake would reduce the amount of disinformation that each viewer encounters. 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 a government-imposed opt-in or opt-out requirement, there is no case directly on point.¹⁸⁶ Government action is not strictly required here, if platforms are willing to sacrifice a bit of profit. They can create an opt-in system voluntarily.

These interventions will not stop everyone who shares political 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.¹⁸⁷ 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.¹⁸⁸ Motivated reasoning, observed here as *directionally* motivated reasoning, "leads people to seek out information that reinforces their preferences (i.e., confirmation bias), counterargue information that contradicts their preferences (i.e., disconfirmation bias), and view proattitudinal information as more convincing than counterattitudinal information (i.e., prior attitude effect)."¹⁸⁹ 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.¹⁹⁰ Some social media users

186. See Elmendorf & Wood, *supra* note 64, at 39–40.

187. See generally Jennifer Jerit & Jason Barabas, *Partisan Perceptual Bias and the Information Environment*, 74 J. POLITICS 672 (2012) (finding that people's perceptions of the world are shaped by their political views).

188. *Id.* at 673 (internal citation omitted).

189. D.J. Flynn et al., *The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs About Politics*, 38 ADVANCES POL. PSYCHOL. 127, 132 (2017) (citing C.S. Taber & M. Lodge, *Motivated Skepticism in the Evaluation of Political Beliefs*, 50 AMER. J. POL. SCI. 755, 757 (2006)).

190. They can change, but correcting misinformation is difficult. See generally Jennifer L. Hochschild & Katherine Levine Einstein, *Do Facts Matter? Information and Misinformation in American Politics*, 130 POL. SCI. Q. 585 (2015) (discussing how people exposed to misinformation resist corrections). One way of correcting information, is to "hit them between the eyes" with factual information. James H. Kuklinski et al., *Misinformation and the Currency of Democratic Citizenship*, 62 J. POL. 791, 805 (2000). However, corrections can backfire. See Brendan Nyhan & Jason Reifler, *When Corrections Fail: The Persistence of Political Misperceptions*, 32 POL. BEH. 303, 311–22 (2010).

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.”¹⁹¹ 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 would be a helpful start, but the amount of disinformation that persists may still be damaging to democracy. That brings us to general approaches that the platforms can use, which probably would not survive a constitutional challenge if the efforts were required 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.”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,¹⁹³ Facebook has begun to address its disinformation problem.¹⁹⁴ It has experimented with using third-party fact checkers to identify and label disinformation, with mixed results.¹⁹⁵ It has also experimented with offering “related” stories that serve as fact correctives, polling users on which news sources they trust

191. Nyhan & Reifler, *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).

192. Brendan Nyhan, *Why the “Death Panel” Myth Wouldn’t Die: Misinformation in the Health Care Reform Debate*, 8 FORUM 1, 15 (2010). See also Nyhan, *supra* note 190, at 311–22.

193. Kerry Flynn, *Facebook Is Going After One of the Big Ways Fake News Spreads*, MASHABLE (Aug. 28, 2017) [hereinafter Flynn, MASHABLE], <http://mashable.com/2017/08/28/facebook-fake-news-advertising-crackdown/#BrL7D4yVkaqM>.

194. Adam Mosseri, *Working to Stop Misinformation and False News*, FACEBOOK NEWSROOM (Apr. 6, 2017), <https://newsroom.fb.com/news/2017/04/working-to-stop-misinformation-and-false-news>.

195. Jeff Smith et al., *Designing Against Misinformation*, MEDIUM (Dec. 20, 2017), <https://medium.com/facebook-design/designing-against-misinformation-e5846b3aa1e2>.

most, and suppressing all news in its users' newsfeeds.¹⁹⁶ Finally, it has begun to move away from including news in newsfeeds.¹⁹⁷ That is a move away from publishers, but not necessarily a move away from disinformation, since so much disinformation seems to have emerged from Pages set up by so-called astroturf groups¹⁹⁸ and amplifying fake media sites.

Three general considerations will help any private regulatory framework to be effective. First, any efforts to label and identify questionable (or trustworthy¹⁹⁹) 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 to temporarily ban advertisers who repeatedly share disinformation advertising that has been marked by fact checkers as "false news."²⁰⁰ 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.²⁰¹ Third, the platforms can turn down the volume of disinformation advertising by enforcing their terms of service, which prohibit bots and "inauthentic likes."²⁰²

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

196. Emma Hinchliffe, *Facebook Just Quietly Rolled Out Its Long-Awaited Solution to Fake News*, MASHABLE (Mar. 4, 2017), <http://mashable.com/2017/03/04/facebook-fake-news-rollout/#.IUNWbQIkOqM>. Though note that hoaxes have long existed on Facebook. See, e.g., Karissa Bell, *Facebook Is Cracking Down on Hoaxes in Your News Feed*, MASHABLE (Jan. 20, 2015), <http://mashable.com/2015/01/20/facebooks-news-feed-hoaxes/#glusvpOnwmqJ>; *How is Facebook Addressing False News Through Third-Party Fact-Checkers?*, FACEBOOK HELP CENTER, <https://www.facebook.com/help/1952307158131536> (last visited Sept. 8, 2017) (placing false stories lower in users' feeds, and reducing distribution of stories from repeat offenders).

197. Sapna Maheshwari & Sydney Ember, *The End of the Social News Era? Journalists Brace for Facebook's Big Change*, N.Y. TIMES (Jan. 11, 2018), <https://www.nytimes.com/2018/01/11/business/media/facebook-news-feed-media.html>.

198. See *supra* note **Error! Bookmark not defined.** for definition.

199. See Lehrman, *supra* note 9.

200. Flynn, MASHABLE, *supra* note 193.

201. Mosseri, *supra* note 194.

202. Patrick Kulp, *Facebook Cracks Down on Bogus 'Likes' and Zombie Accounts in Battle Against Fake News*, MASHABLE (Apr. 15, 2017), <https://mashable.com/2017/04/15/facebook-shuts-down-fake-likes/#0DujDggJ5Pqw>. See also Timberg & Dwoskin, *supra* note 165.

media companies comply with fairly tight regulations in other countries. Some of these regulations would not survive First Amendment muster or might not be otherwise desirable in the United States. Nevertheless, platform compliance with regulations elsewhere belies platforms' claim that the U.S. government regulations would be overly-burdensome.

Consider several examples from European regulations. First, Germany passed a law that fines media platforms for failure to delete "illegal, racist or slanderous comments and posts within 24 hours of being notified to do so."²⁰³ 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), and estimates are that it will cost the platforms around €530 million (\$622 million) a year to increase monitoring to avoid fines.²⁰⁴ Germany has apparently seen a decline in disinformation on Facebook since the law was implemented in summer 2017.²⁰⁵

In the Czech Republic, the government is particularly concerned about Russian efforts to destabilize their democracy. Its interior ministry has launched a Center Against Terrorism and Hybrid Threats "tasked with identifying and countering fake news."²⁰⁶ Dozens of jurisdictions worldwide observe "election silence," or a media blackout, in the time leading up to voting day, or during voting day itself.²⁰⁷ These blackouts range from not allowing the mention of candidates aside from the fact that the candidate voted (France) to halting advertising except online and billboard advertising placed before the blackout period and not altered during it (Ontario, Canada).²⁰⁸

Many of these regulations would be considered government censorship beyond that which is tolerated for political speech in the

203. Scott Roxborough, *How Europe Is Fighting Back Against Fake News*, HOLLYWOOD REP. (Aug. 21, 2017), <http://www.hollywoodreporter.com/news/how-europe-is-fighting-back-fake-news-1030837>.

204. *Id.*

205. *Id.*

206. *Id.*

207. *Voting Day(s)*, ACE: ELECTORAL KNOWLEDGE NETWORK, <https://aceproject.org/ace-en/topics/me/mef/mef04/mef040d> (last updated 2012).

208. Catherine Nicholson, *French Media Rules Prohibit Election Coverage over Weekend*, FRANCE 24 (May 7, 2017), <https://www.france24.com/en/20170506-france-media-rules-prohibit-election-coverage-over-weekend-presidential-poll>; *Media Rules During an Election*, ELECTIONS ONTARIO, <http://www.elections.on.ca/en/media-centre/media-rules-during-an-election.html> (last visited Sept. 9, 2018).

United States. It is certainly true that autocratic leaders may use “combatting disinformation” as a convenient excuse for a crackdown on speech and expression. However, 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. Therefore, they can certainly handle some government-imposed transparency requirements here in the United States.

V. 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 and states that 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.²⁰⁹ 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.”²¹⁰ 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 its funding. Perhaps as a result, the FEC’s mission statement is heavy on transparency and tepid on enforcement and administration. Nevertheless, it moves slowly, is gridlocked by partisan balance, and its skills are no match for sophisticated disinformation agents.

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.²¹¹ The FEC’s enforcement procedures

209. See STEVEN J. BALLA & WILLIAM T. GORMLEY, JR., *BUREAUCRACY AND DEMOCRACY*, 129–72 (4th ed. forthcoming 2018); Yoon-Ho Alex Lee, *Beyond Agency Core Mission*, 68 ADMIN. L. REV. 551, 553–66 (2016) (reviewing literature on agency mission).

210. *Mission and History*, FED. ELECTIONS COMM’N, <https://www.fec.gov/about/mission-and-history> (last visited Sept. 9, 2018).

211. Ann Ravel, Opinion, *Dysfunction and Deadlock at the Federal Election Commission*,

require multiple rounds of voting: to proceed to an investigation; to allow the general counsel to conduct formal discovery and issue subpoenas;²¹² 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.²¹³ Resolving a matter can take years.

FEC suffers from partisan gridlock.²¹⁴ For a decade, Republican commissioners have resisted updating campaign finance laws and enforcing the existing ones.²¹⁵ 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.”²¹⁶

FEC’s jurisdiction and its employee skills do not match those needed to combat disinformation. It is charged with enforcing the ban on foreign contributions and expenditures, though its jurisdiction only extends to civil penalties.²¹⁷ Tracking down disinformation advertisers will require skills with money tracing. 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

N.Y. TIMES (Feb. 20, 2017), <https://www.nytimes.com/2017/02/20/opinion/dysfunction-and-deadlock-at-the-federal-election-commission.html>.

212. See FED. ELECTION COMM’N, GUIDEBOOK FOR COMPLAINANTS AND RESPONDENTS ON THE FEC ENFORCEMENT PROCESS, FED. ELECTIONS COMM’N 12 (2012), https://transition.fec.gov/em/respondent_guide.pdf.

213. *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.”).

215. Richard L. Hasen, *The FEC Is as Good as Dead*, SLATE (Jan. 25, 2011), http://www.slate.com/articles/news_and_politics/jurisprudence/2011/01/the_fec_is_as_good_as_dead.html.

216. Ann Ravel, *How the FEC Turned a Blind Eye to Foreign Meddling*, POLITICO (Sept. 18, 2017), <https://www.politico.com/magazine/story/2017/09/18/fec-foreign-meddling-russia-facebook-215619>.

217. 52 U.S.C. § 30106(b)(1) (2012); *Id.* § 30121(a). The Department of Justice prosecutes “serious and willful” violations of our campaign finance laws, as well as criminal issues like fraud.



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, which has a core mission 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."²¹⁸ 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 keep the Political File for television ads, but have shown no interest in regulating political advertising on 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.²¹⁹ 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 continue to create new frameworks to protect voters in their own elections from disinformation.²²⁰

As of this writing, the main state-level action has been in New

218. *Mission*, FIN. CRIMES & ENFORCEMENT NETWORK, <https://www.fincen.gov/about/mission> (last visited Sept. 9, 2018).

219. *See, e.g.*, CAL. GOV'T CODE § 84504.3 (West 2018); CONN. GEN. STAT. § 9-621 (2018); DEL. CODE ANN. tit. 15, § 8021 (2018); ME. REV. STAT. tit. 21-A, § 1014 (2017); MINN. STAT. ANN. § 211B.04 (West 2017).

220. Elmendorf et al., *supra* note 168.

York and Maryland. New York’s Democracy Protection Act requires disclosure of all online ads, advertiser verification and registration with the NY Board of Elections, and an online archive.²²¹ The State of Maryland has enacted legislation requiring the platforms to retain all ads and audiences.²²² The California legislature is considering a similar bill.²²³ 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.²²⁴ 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.²²⁵ Los Angeles already requires candidates to store all political communications.²²⁶ Along with Chris Elmendorf, we have urged the City of San Francisco to adopt our model.²²⁷

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

221. 2018 N.Y. Sess. Laws Ch. 59 (S. 7509-C) (McKinney) (to be codified at N.Y. ELEC. LAW §§ 14-100, 14-106, 14-107, 14-126).

222. Online Electioneering Transparency and Accountability Act, MD. CODE ANN., ELEC. LAW §§ 1-101(a), (dd-1), (ll-1), (k); 13-306(a)–(e); 13-307(a)–(e), 13-401; 13-403; 13-405; 13-405.1; 13-403; 13-405.2) (West 2018).

223. 2018 Cal. A.B. 2188, Political Reform Act of 1974: Campaign Disclosures: Advertisements.

224. SEATTLE, WASH., CHARTER ch. 2.04.280 (2018), https://library.municode.com/WA/seattle/codes/municipal_code?nodeId=TIT2EL_CH2.04ELCACO_SUBCHAPTER_IICADI_2.04.280COADDURE.

225. Eli Sanders, *Seattle Says Facebook Has Failed to Follow Law on Election Ad Transparency*, 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>.

226. L.A., CAL., CODE § 49.7.31–.32 (2017), https://ethics.lacity.org/PDF/laws/law_CFO.pdf.

227. See Elmendorf et al., *supra* note 168.



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 state of First Amendment 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. 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. Our current regulatory framework is insufficient to fully address disinformation advertising online.

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.

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 in these ways, 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

2018]

FOOL ME ONCE

1287

conflict and discord.

APPENDIX

Since we finalized this Article, the platforms have continued to battle political disinformation. None has provided audience identifiers to enable counter speech. Nor have they joined together or formed a co-regulatory arrangement with the government. Some are attempting to “nudge” users, but none has provided an opt-in or opt-out for narrowly-targeted political content. As it stands, without co-regulation or comprehensive industry self-regulation, any positive reforms they make may be changed at any time, with no accountability.