THE STEALTH MEDIA?
GROUPS AND TARGETS BEHIND DIVISIVE ISSUE CAMPAIGNS ON FACEBOOK

Young Mie Kim;[1] Jordan Hsu;[2] David Neiman;[3] Colin Kou;[4] Levi Bankston;[2] Soo Yun Kim;[5] Richard Heinrich;[6] Robyn Baragwanath;[5] and Garvesh Raskutt[7]

Forthcoming in *Political Communication*
(accepted pending the final editorial approval)

UPDATED on 04/17/2018

Statements on the Protection of Human Subjects in Research and Data Privacy & Security

The research followed the standard protocols for the protection of human subjects in research and has been approved by the Institutional Review Board for Protection of Human Subjects in Research at the University of Wisconsin-Madison (2015-1573). Only consented volunteers participated in the research. Neither the browser extension nor the survey collected personally identifiable information. We did not collect users' personal profiles or friends' networks. Data access is strictly limited to the IRB trained researchers in the team only. Furthermore, no third-party can access the data. Additionally, the browser extension works in a secured, encrypted web server and the data is stored on a secure data server. We have a server architecture that separates ad data, meta-information, and survey data. When matching ad data, its meta data, and survey responses, anonymized user identifiers (i.e., 36-digit user ID assigned at the installation of the browser extension) were utilized for data analysis. The publication of data analysis includes aggregate-level information only.

Author Contributions

*The order of authorship reflects the order of each author's contributions to the present research.

*The areas of contributions by each author as follows.

Kim, Y. M.: All, including project administration; conception; theoretical development; data collection; data analysis; and writing
Hsu: Project assistance; implementation of data analysis (Study 1 & Study 2); part of writing (literature)
Neiman: Data pull; part of data analysis (Study 1 & Study 2); and part of writing (Study 2)
Kou: Data management; data pull; part of data analysis (Study 1 & Study 2)
Bankston: Part of data analysis (Study 1); part of writing (literature)
Kim, S. Y, Baragwanath, and Heinrich: ad coding, qualitative analysis (Study 1)
Raskutti: Consultation (Study 2)

Author Notes

[1] Professor, School of Journalism and Mass Communication & Political Science (Faculty Affiliate), University of Wisconsin-Madison
[2] Graduate student, Political Science, University of Wisconsin-Madison
[3] Undergraduate student, Mathematics & Computer Science, University of Wisconsin-Madison
[4] Undergraduate student, Statistics & Mathematics, University of Wisconsin-Madison
[5] Graduate student, School of Journalism and Mass Communication, University of Wisconsin-Madison
[6] Graduate student, Life Science Communication, University of Wisconsin-Madison
[6] Assistant Professor, Statistics & Wisconsin Discovery Center (Machine Learning Group), University of Wisconsin-Madison

Acknowledgements

*This research is part of a larger research project, Project DATA (Digital Ad Tracking & Analysis) led by the Principal Investigator, Young Mie Kim (eyeonelections.com).

*Project DATA is funded by Center for Information Technology and Policy at Princeton University, the Democracy Fund, the John S. and James L Knight Foundation, Women In Science and Engineering Leadership Institute at the University of Wisconsin-Madison, and the Vice Chancellor's Office for Research of the University of Wisconsin-Madison.

*The authors would like to thank undergraduate student coders who assisted in content analysis of ads.

*The authors also would like to thank anonymous reviewers and the following colleagues who provided helpful comments: Barry Burden, David Canon, Michael Delli-Carpini, Brendan Fischer, Phil Howard, Larry Noble, Markus Prior, and Michael Xenos.

THE STEALTH MEDIA?
GROUPS AND TARGETS BEHIND DIVISIVE ISSUE CAMPAIGNS ON FACEBOOK

Young Mie Kim;[1] Jordan Hsu;[2] David Neiman;[3] Colin Kou;[4] Levi Bankston;[2] Soo Yun Kim;[5] Richard Heinrich;[6] Robyn Baragwanath;[5] and Garvesh Raskutt[7]

Abstract

In light of the foreign interference in the 2016 U.S. elections, the present research asks the question of whether the digital media has become the stealth media for anonymous political campaigns. By utilizing a user-based, real-time, digital ad tracking tool, the present research reverse engineers and tracks the groups (Study 1) and the targets (Study 2) of divisive issue campaigns based on 5 million *paid ads* on Facebook exposed to 9,519 individuals between September 28 and November 8, 2016. The findings reveal groups that did not file reports to the Federal Election Commission (FEC)—nonprofits, astroturf/movement groups, and unidentifiable "suspicious" groups, including foreign entities—ran most of the divisive issue campaigns. One out of six suspicious groups later turned out to be Russian groups. The volume of ads sponsored by non-FEC groups was four times larger than that of FEC- groups. Divisive issue campaigns clearly targeted battleground states, including Pennsylvania and Wisconsin where traditional Democratic strongholds supported Trump by a razor thin margin. The present research asserts that media ecology, the technological features and capacity of digital media, as well as regulatory loopholes created by *Citizens United v. FEC* and the FEC's disclaimer exemption for digital platforms contribute to the prevalence of anonymous groups' divisive issue campaigns on digital media. The present research offers insight relevant for regulatory policy discussion and discusses the normative implications of the findings for the functioning of democracy.

After a long silence, Facebook finally admitted that 3,000 ads linked to 470 Facebook accounts or Pages were purchased by groups linked to the Russian state during the 2016 U.S. Elections (Stamos, Facebook Newsroom, September 6, 2017). Facebook also noted that the ads primarily focused on divisive social and political issues such as guns, LGBT rights, immigration, and race, and targeted specific categories of individuals. Along with Facebook, Google and Twitter testified at public hearings conducted by the congressional Intelligence Committee that their ads were also purchased by the same Kremlin-linked Russian operations.

Foreign interference with US elections, of course, raised public indignation and dismay. The Founding Fathers held a firm belief that American democracy must be free from foreign interference: "The jealousy of a free people ought to be constantly awake, since history and experience prove that foreign influence is one of the most baneful foes of republican government" (George Washington, September 17, 1796; from Whitney, the Republic, January 1852). When digital media, where ordinary citizens routinely share information through social networks, were found to be used by foreign entities to spread false information and sow discord in the nation, the public was deeply alarmed, and rightly so. The foreign digital operations present a profound challenge to those who believe in the democratic potential of digital media, which includes the development of public passion on the issues of personal concern (e.g., Kim, 2009); the mobilization of decentralized, alternative voices (e.g., Karpf, 2011); and the organization of collective action (e.g., Bennett & Sergerberg, 2013).

However, some scholars argue that foreign involvement in the US election indeed is an unintended, yet inevitable consequence of the current election campaign system (Emmer, 2014). Following the Supreme Court's ruling on *Citizens United* (*Citizens United v. Federal Election Commission*), anonymous issue campaigns run by nonprofits drastically increased (Chand 2014, 2017), because the ruling paved the way for any group or individual—including foreign entity—to get involved in election campaigns with few campaign finance disclosure and reporting requirements. Furthermore, while broadcast campaigns identifying federal candidates near an election day are subject to disclaimer and disclosure requirements, currently, the same types of campaigns run on digital platforms can escape those requirements. Political campaigns on popular digital platforms have been exempt from the Federal Election Commission (FEC)'s disclaimer requirements because digital ads are considered to be too small to include a disclaimer and act like bumper stickers. No law currently exists to adequately address political campaigns on digital platforms. Thus, the *Citizens United* ruling, the lack of adequate law, as well as the lax disclaimer policies for digital platforms altogether created multi-level loopholes for campaigns run by anonymous groups, which potentially includes foreign countries' disinformation campaigns.

This raises pressing questions: *Just as a stealth bomber shoots at a target without being detected by radar, do digital media platforms function as stealth media---a system that enables the deliberate operations of political campaigns with undisclosed sponsors/sources, furtive messaging of divisive issues, and imperceptible targeting? What types of groups engage in such campaigns? How do such campaigns target the public?*

The present paper addresses these pertinent and vitally important questions with an empirical analysis of paid Facebook ads. Using a user-based, real-time,

digital ad tracking app that enabled us to trace the sponsors/sources of political campaigns and unpack targeting patterns, the present research examines 5 million ads exposed to nearly 10,000 Facebook users. To the best of our knowledge, this is the *first*, large-scale, systematic empirical analysis that investigates who operated divisive issue campaigns on Facebook (Study 1) and who was targeted by these issue campaigns (Study 2).

Drawing upon the theories of political strategies and group politics that have long been developed in political communication literature (e.g., Hillygus & Shields, 2014; Howard, 2005), the present research explains why certain types of groups are prone to thriving on digital platforms and why certain types of individuals are targeted by such campaigns on digital media. The present research also offers insight relevant to current policy debates and discusses the normative implications for the functioning of democracy.

Stealth Electioneering: Anonymous Groups, Divisive Issue Campaigns, and Microtargeting

Groups behind Electioneering: Outside Groups and Dark Money Group Campaigns

Coinciding with the declining mobilizing power of mainstream political parties (Dalton 2000), increasingly diverse interests among the public (Cigler, Loomis, & Nownes, 2015), and the drastic increase in the number of nonprofits (especially issue-based public advocacy groups; Berry 2003; Walker 1991), the influence of outside groups[1] in U.S. politics has grown over the past decades, especially through the means of election campaign interventions, namely electioneering.

The most popular method for groups to engage in elections is issue campaigns, which promote or demote a political issue, with or without explicit support or defeat of a candidate[2]. In the interest of public education and to protect such groups under the First Amendment, since *Buckley v. Valeo* (424 U.S. 1, 1976), issue campaigns that do not expressly advocate[3] the election or defeat of a clearly identified candidate and do not coordinate with a candidate[4] are often exempt from the FEC's reporting requirements (Francia, 2010).

Citizens United v. Federal Election Commission (558 U.S. 310, 2010) provided groups even more opportunities to further engineer elections. First, the Court decreed that so long as these groups engaged in political activities without coordinating with candidates, candidate committees, or political parties, limits on their campaign spending based on a group's identity were unconstitutional under the First Amendment. The decision thereby resulted in unlimited campaign contributions from *any* source, opening the door for election campaign interventions by any individual or group including nonprofits,[5] corporations—and as an oversight, even foreign groups (Emmer, 2014).

Second, *Citizens United* also allowed groups including nonprofits with ideological and single issue groups to use their general revenue to purchase ads calling for the direct election or defeat of a candidate as long as the groups do not directly coordinate their campaigns with candidates, candidate committees, or political parties. The Court's ruling permits tax-exempt nonprofits to fund electioneering campaigns by using general revenue funds, as long as they do not directly coordinate with candidates. While Super PACs[6] must be registered with the FEC for disclosure and reporting, nonprofits, whose primary purpose is generally considered non-political,[7] do not have to disclose donors and have few FEC reporting requirements. These groups, hence, have been dubbed *dark money groups*.

Taking advantage of the loophole, nonprofits created a complex group structure for various types of electioneering. Social welfare groups (501c4), for example, conduct much of their work under their 501c4 status, but also can be associated with 501c3 status for tax-exempt gifts and various types of issue campaigns. They also loosely connect to traditional PACs that are able to make a direct contribution to candidates, as well as Super PACs that can raise unlimited donations for independent expenditures. For dark money groups, a501c status indeed serve as a vehicle to make contributions to associated Super PACs, while avoiding the FEC disclosure and reporting requirements imposed upon 501c4s. As they have the dual benefit of donor anonymity and unrestricted election campaign intervention, nonprofits' dark money campaigns have become the most prominent method for electioneering (Chand, 2014; Tobin, 2012).

In a similar vein, astroturf/movement groups, which do not necessarily reveal their identities publicly, also engage in issue campaigns. Howard (2005) identified the increase in issue campaigns run by astroturf organizations behind candidates as the biggest change in recent election campaign practices. Astroturf/movement groups are often organized by anonymous lobbyists and organizations as tactical alliances to push a particular policy agenda. They collect issue publics, who consider a particular issue personally important based on values, identities, and self-interests (Kim 2009; Krosnick 1990), to demonstrate the representation and significance of a particular issue of concern. Such issue campaigns are designed to activate the grievance or passion of issue publics and promote their support for a particular candidate. However, few members of astroturf/movement groups are aware that they are organized by anonymous lobbyists and groups (Howard 2005). Donors, sponsors/groups, and candidates behind astroturf/movement campaigns remain largely unknown.

Since *Citizens United*, dark money groups have spent more than $600 million (OpenSecrets, December 7, 2017). Spending by outside groups was nearly $1.4 billion in the 2016 elections, surpassing both major parties' total spending, which was $290 million. Issue campaigns run by nonprofits made up nearly half of the TV ads in senate races nationwide, outpacing candidate ads by a 2 to 1 margin and ads by Super PACs by a 6 to 1 margin (Maguire, OpenSecrets, February 25, 2016).

Behind Digital Electioneering: No Disclosure, Furtive Messaging and Microtargeting

Interestingly, however, nonprofits' electioneering communications decreased from $308 million in the 2012 presidential election to $181 million in the 2016 presidential election. It has been suggested that digital media, among other factors, replaced dark money groups' campaigns on the airwaves (Choma, *Mother Jones*, June 15, 2015). The overall digital ad spending in the 2016 election surpassed cable spending, exceeding $1.4 billion (Borrell Associates, January 2017). It was nearly five thousand times more than that of the 2008 elections.

Has the digital media become the *stealth media*? We define the stealth media as the media system that enables deliberate operations of political campaigns with undisclosed identities of sponsors/sources, furtive messaging of divisive issues, and imperceptible targeting. Ecological, technological, and regulatory factors explain why anonymous groups, including foreign entities, find digital platforms to be conducive to the deliberate operation of secretive political campaigns, such as disinformation campaigns and dark money group campaigns.

Ecological factors. Television viewership, especially among younger voters (ages 18-24, Nielsen 2017) has continually declined while the use of digital media (including social media) has increased. More than 90% of Americans are now online in daily life, and nearly 70% of the population use social media. By far, Facebook is the most popular digital media platform today (Pew 2017).

Increasing public distrust in traditional media also fosters political campaigns' going digital (Gurevitch, Coleman, & Blumer, 2009; Ladd, 2012). According to Gallup (Swift, Gallup, September 14, 2016), only 32% of Americans think that mass media report current affairs fully, accurately, and fairly. The recent sharp decline of trust in traditional media was especially prominent among Republican voters—about 80% of Republicans distrust traditional mass media (Harvard-Harris Poll, May 2017). Social media, which consist of personal networks of friends and acquaintances, are considered to be more authentic, credible, and truthful (Lee, 2016).

Technological factors. A digital platform such as Facebook offers technological features and capacity that contribute to the amplification of anonymous groups' secretive, divisive issue campaigns: native advertising and microtargeting capacity.

Native advertising is an advertising strategy for paid content,[8] but it is deliberately designed to look like non-paid, user-generated content. On Facebook, for example, a native advertisement appears in News Feeds (as a Sponsored Feed, or Promoted Page; see Figure 1A) that resembles news, videos, games, memes, or other non-marketing content embedded among regular posts by social media users. Even with an unnoticeable disclaimer label that indicates the content is a paid message (e.g., *sponsored* in the case of Facebook; *promoted tweet* on Twitter), users are often unable to distinguish native advertising from non-promotional content.

Groups behind digital electioneering can utilize native advertising, such as Facebook Sponsored News Feeds, for issue campaigns without revealing their identity, or by using very generic names (e.g., American Veterans) for the Facebook landing pages linked to their native advertisements. In fact, many among the sample of Russian Facebook ads released by the Intelligence Committee appeared to utilize Sponsored News Feeds, Facebook's native advertising format, with an extremely generic and benign group name (e.g., United Muslims of America).[9] Users then are prone to share the messages that look like a regular post and thus amplify the disinformation campaign on Facebook.[10]

It is important to note that native advertising messages can be posted without appearing on the sponsor/source's Facebook page. This suggests that specific ad messages could be completely hidden from the public unless collected in real time by the user who is exposed to the messages. This makes public monitoring of digital ads impossible and poses significant methodological challenges for researchers or journalists when using the conventional scraping approach to gathering digital data.

Publicly inaccessible digital ads, namely dark posts, illuminate the way digital advertising operates in general: its microtargeting capacity. Microtargeting refers to a narrowly defined, individual-level audience targeting, media placement, and message customization strategy (Kim, 2016). Microtargeting can go as narrow as targeting each and every individual in the nation, but the term encompasses a general trend: the shift in targeting, placement, and customization from the aggregate (such as a media market) to the individual, as narrowly as possible.

By gathering a vast amount of data, including digital trace data, and by utilizing predictive modeling techniques, campaigns create enhanced profiles that identify and target specific types of individuals, and then customize their messages. Different individuals therefore are targeted with different messages. For instance, in the 2016 U.S. election campaign, the firm Cambridge Analytica created psychographic classifications of voters by harvesting Facebook users' posts, likes, and social networks and matching them with their comprehensive voter profile data. Cambridge Analytica then customized ad messages in accordance with the audience's psychographics, geographics, and demographics (Guardian, November 2015). For example, while issue campaigns concerning guns would be concentrated in rural areas in Wisconsin, campaigns promoting racial conflict would be concentrated in Milwaukee, Wisconsin. Among Wisconsin individuals interested in guns, those who have a high level of insecurity would be targeted with fear appeals (e.g., "Hillary will take away your guns") while those who are family-oriented would receive messages like "guns protect your loved ones." Data-driven, digitally enabled targeting strategies have been increasingly adopted by political campaigns (Hersh, 2015; Kreiss, 2016).

While data analytics and targeting decisions may require resources as well as sophisticated knowledge and skill, the mechanics of targeting specific types of voters and selectively displaying specific ads to targeted

voters is easy to accomplish on most digital platforms, even for those with little resource, knowledge, or skill concerning data analytics or microtargeting. For instance, Facebook offers anyone who pays for promotional messages a menu-style, microtargeting tool for free that includes an array of options for the type of targets based on users' demographics, geographics, media consumption patterns, political profiles, issue interests, hobbies, friends' networks (e.g., number of friends), Facebook engagement (e.g., liked a post by NRA), and the like. It also offers strategic targeting suggestions based on their data and audience matrices (such as a targeting index). The all-in-one, one-stop targeting menu can be applied across affiliated digital platforms (e.g., Facebook-Instagram) as well. Microtargeting is also enhanced by real-time re-targeting algorithms, a constant loop between users' voluntary choices (e.g., liking) and the machine's feedback on their choices. A user will receive the same news feeds when a sponsored message is liked by one's friend, amplifying the promotion of the message among the target's friends' networks that have similar traits. Thus, even low-resourced groups now directly buy individual targets at an affordable cost as opposed to buying costly media markets or ad spots.

With microtargeting, groups who engage in electioneering on digital media focus on issue campaigns by narrowly identifying particular issue interests and targeting issue publics rather than widely reaching out to the electorate with a broad appeal. In this way, these campaign interventions remain completely unmonitored, yet groups can still reach out to their niche, the most persuadable segment of the electorate.

Microtargeting is also particularly useful for anonymous groups who intervene in election campaigns by dividing the opposing candidate's coalition with wedge issues or by suppressing the vote from the supporters of the opposing candidate (Kim, 2016). In support of this, Hillygus and Shields (2009) found that campaigns that have narrower targeting capacity (in their case, direct mail) are more likely to focus on wedge issue interest than ads on broadcast media.[11] Furthermore, microtargeting with wedge issues is more likely to be prominent in competitive, battleground states (Hillygus & Shields 2009). *Regulatory factors*. Currently, no law adequately addresses digital political campaigns. Despite the wide adoption of digital media, the current election campaign regulatory policies contain few requirements concerning digital political campaigns. Electioneering communications are subject to FEC's disclosure and disclaimer requirements, but by definition, electioneering communications are only applied to broadcast, cable, and satellite. Express advocacy ads or political ads run by candidates, PACs, and parties would have been subject to the disclaimer requirements, per FEC's interpretation, political ads on popular platforms such as Google, Twitter, or Facebook have been exempt from the disclaimer requirements because ads on digital platforms are so "small" that the inclusion of disclaimers is impractical because it has to use an unreasonable proportion of ad space. Google even claimed that political ads on Google should be considered similar to "bumper stickers" on a car (Bauerly, 2013).

Due to the limited understanding of the unique technological factors of digital campaigns, the technological advancements outpacing regulatory policies, and the FEC's ad hoc policies, advisory opinions often lack consistency. For example, while the FEC ruled that Google's proposal to include the link to a landing page (source) would be a sufficient disclaimer, the FEC failed to make a decision on Facebook's argument that political ads on Facebook should not be required to link to a landing page with a disclaimer (Bauerly 2013).

The lack of regulations or guidelines created a loophole for outside groups—including foreign entities—to run political ads on popular digital platforms, with almost no requirements, while concealing their true identities. Even though foreign campaign interventions are strictly prohibited by current law, the multi-layered loopholes (the non-disclosure rule for nonprofits, the lack of adequate law on digital political campaigns, and the disclaimer exemption for digital media) make regulatory monitoring and enforcement extremely difficult.

Given the ecological environment, technological features and capacity, and multiple regulatory loopholes created by *Citizens United* as well as the FEC's special exemption policies altogether, we expect to observe divisive issue campaigns by a large volume of anonymous groups—groups with no true identity, astroturf/movement groups, nonprofits, and even foreign entities. We also expect to witness microtargeting, especially on divisive issue campaigns that target specific issue interests concentrated in battleground states. The present research attempts to empirically evidence the aforementioned patterns. More specifically, this research tracks the groups (Study 1) and targets (Study 2) of divisive issue campaigns on Facebook.

Overview of the Project

This section explains the overall methodological strategy of the present research including data collection methods and analytical framework commonly adopted by both Study 1 and Study 2.[12] [13]

Overall Strategy: Reverse Engineering with User-Based, Real-Time, Longitudinal Tracking

While campaign information is publicly accessible in the case of television advertising, digital campaigns operate behind the scenes; therefore, it is nearly impossible for researchers to systematically collect and analyze digital campaign content, sponsors/sources, and targets (cf. for a non-interactive simple web display ad analysis, Ballard, Hillygus, & Konitzer, 2016).[14] This project strives to uncover the behind-the-scenes operations of digital campaigns with a reverse engineering approach.

Reverse engineering refers to the process of taking a piece of software or hardware, analyzing its functions and information flow, and then interpreting those

processes (Computer World, 2001). A typical reverse engineering approach uses bots that scrape web pages or replicate algorithms while the machine simulates humans and identifies the patterns revealed in the replication. Scraping, however, has a number of limitations in collecting the actual content exposed to human beings in real time. Bots' approximation of algorithms is also, at best, opaque compared to algorithms based on an actual human behavior (Hamilton et al. 2014). Most notably, collecting data by crawling/scraping occurs at the aggregate-, platform-level, which does not capture individually targeted messages.

To overcome the limitations of the conventional reverse engineering method, this project employed an alternative approach: user-based, real-time, longitudinal observation (i.e., crowdsourced algorithm audit measure, Sandvig et al., 2014).[15] As opposed to the aggregate-, platform-level random crawling/scraping of content at the time of data analysis, we recruited volunteered research participants and asked them to use an app that automatically captured the campaign messages exposed to users and the associated meta information at the time of user exposure (for details, *Campaign Data Collection and Reverse Engineering Tool)*. As opposed to a bot's approximation of algorithms, our reverse engineering was enabled by matching sponsors/sources and the content exposed to users with the same users' comprehensive profiles.

User Recruitment and Sampling Procedure

U.S. citizens 18 years old or older who were eligible to vote and able to understand written English were defined as the population as well as the recruitment pool. Volunteers were recruited through a social science and marketing research firm, GfK (formerly Knowledge Network).[16] GfK utilized a screen questionnaire at the time of recruitment to make the sample mirror the U.S. census in terms of gender, race/ethnicity, education, household income, age, state (50 states plus Washington D.C.), and voter registration.[17] The sample of research participants was generally similar to the U.S. Census.[18]

Campaign Data Collection and Reverse Engineering Tool

The digital campaign data collection was enabled by EScope, an ad data collection/reverse engineering tool. EScope is a browser extension the research team developed for this project.[19] It works like an ad blocker, but instead of blocking ads, it detects and collects them. Unlike a typical ad blocker that is only compatible with a normal web browser and only blocks display ads, EScope collects various formats of promotional messages across different digital media platforms including Facebook (Sponsored Feeds, Page Promotion, Right Column ads).

The participants of our 2016 General Election Study installed EScope at the time of recruitment[20] and kept it until Election Day, November 8, 2016 (about 6 weeks). Once a consented user signed into the project site and installed the program as an add-on to the user's browser, the browser extension automatically detected and collected the campaign messages exposed to the user with their meta-information in an unobtrusive way. The campaign messages and their associated meta-information were sent and saved onto the research server. The meta-information includes each message's sponsor (text, if self-identified), source (i.e., the full URL of the landing page to which the campaign message ultimately directs users; it may or may not be the same as the sponsor), time-stamp (time of user exposure), as well as an anonymized unique user ID assigned to each individual user who was exposed to the message. Actual texts of the captured campaign messages were extracted, and any image files included in the messages were saved in real time. The digital campaign data thus enables us to not only examine the content of each campaign message, but to track back who sent the particular message (sponsor/source), and to whom (target).

In order to detect potential selection biases in the adoption of EScope, we examined the differences among a) the online population, of which demographic profiles were obtained through GfK; b) those who installed EScope (~17,000+) only; and c) those who installed EScope *and* completed the baseline survey (10,509; see *User Surveys*). We did not find any systematic difference in terms of demographics, suggesting no significant selection biases in the sample.

User Surveys

To better understand who was targeted, the project also administered user surveys. Once installing EScope, users were directed to the baseline survey that asked about users' demographics, issue positions, candidate preferences, as well as political predispositions (e.g., party identity). Each individual user was assigned a unique anonymized user ID, which linked each and every campaign message exposed to the user and the survey responses from the same user. A total of 10,509 users completed the baseline survey.

Facebook Data

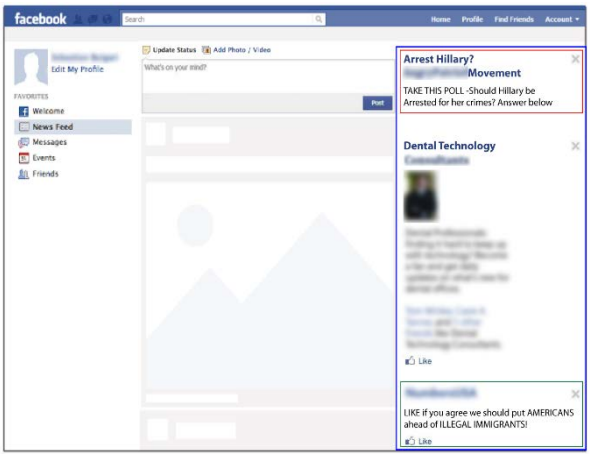
The present research focuses on Facebook ads exposed to 9,519 active participants between September 28 and November 8, 2016. It is important to emphasize that among the Facebook data pool, we investigated Facebook' ***paid*** *ads* only, Sponsored Feed Ads (a total of 1,362,098 ads exposed to 8,377 unique users), and Right Column Ads (a total of 3,737,379 ads to 7,905 unique users). Based on trained coders' hand-labeling, we estimated that approximately 1.6 million ads are political ads.[21]

Sponsored Feeds appear on Facebook News Feeds along with the posts by users' Facebook friends. Although noted as "sponsored" in small type, Sponsored Feeds look the same as regular Facebook posts. Sponsored Feeds are often paired with other Facebook promotions, such as Page promotions ("Like Page"). The exposure to Sponsored News Feeds are determined

by multiple factors in Facebook's algorithms, including sponsor's direct targeting (custom audience), location, demographics, user interest, user behavior/engagement, social connections, and friends' engagement (e.g., if a user's friends, especially those who share similar characteristics, liked the post). Right Column Ads appear on the right-side column on Facebook and look more like conventional ads. Right Column Ads also offer targeting capacity and include call-to-actions such as "click," "join," or "sign up" (Figure 1A: Sample Sponsored News Feed; Figure 1B: Sample Right Column Ads).[22]

Figure 1A. Sample Sponsored News Feed

Figure 1B. Sample Right Column Ads



Notes. The screenshot image is replicated based on the ad texts and images collected by the research team
Figure 1A. Sponsored News Feed: "Demand Answers on Clinton Corruption," is replicated based on an ad on the candidate scandal (Hillary corruption) run by a non-FEC nonprofit.
Figure 1B. Right Column ads: [Top] "Arrest Hillary?" is replicated based on an ad run by an astroturf/movement/unregistered group. [Middle] Non-political Right Column ad. [Bottom] "AMERICANS ahead of ILLEGAL IMMIGRANTS!" is replicated based on an ad run by a nonprofit.

Study 1
Groups: Who Are Behind Issue Campaigns

Analytical Procedure

Study 1 investigates the sponsors or sources of issue campaigns on Facebook. Due to the lack of prior knowledge on the groups who ran political ads on Facebook, we first had to take an organic, qualitative, "bottom-up" approach to tracking sponsors/sources who ran issue campaigns placed in Sponsored Feeds or in Right Column. In other words, we started with a qualitative analysis of a small random sample of ads, tracked sponsors/sources, and then ran a large scale search (group name match) throughout our entire Facebook data and quantified the results. The analysis of Study 1 was conducted in the following order.

Random sampling. As an initial step, from the entire data pool of Facebook's paid ads, Sponsored Feeds, and Right Column ads, we randomly drew approximately 50,000 ads.

Identifying issue campaigns. With keyword matching, we identified the ads containing the keyword[23] of policy-relevant issues including abortion, LGBT, guns, immigration, nationalism, race, terrorism, as well as candidates' scandals (e.g., Access Hollywood, Clinton email sever, Clinton Foundation). Hand coders examined the content of identified issue campaigns. Ads were removed if the content of an ad was not political (i.e., false positive) or if it was political, but no direct policy implication or election relevance (e.g., "It's time to conserve").[24] The average intercoder reliability, Cohen's Kappa, was .99.

Tracking groups (sponsors/sources). Human coders then investigated who posted the ad by tracking a) the name of the group, if identified;[25] b) the Facebook Page linked to the ad if any; and c) the landing page linked to the ad, if any. If a Facebook Page or landing page was not accessible (i.e., the Facebook page was taken down or banned; the landing page did not exist; a server access error, etc.), we further investigated sponsors/sources by searching the group name (if identified) or the exact slogan/text in the ad.

Generating frequencies. We counted groups by group type (see *Results*) and also generated the number of ads (unique impressions) associated with each Once hand-coders identified the sponsor or source and its website link, the research team ran a large scale name search through the entire Facebook paid ad pool (Sponsored Feeds and Right Column ads) by a) matching the human-coder identified group *names* with "sponsor" names (in the case of Sponsored Feeds) or ad titles (in the case of Right Column ads), and by b) matching the human-coder identified *landing pages* (linked website) with the landing pages in our Facebook data collection.

Results

We classified the groups into eight types: a) suspicious groups; b) suspicious groups that turned out to be the ads sponsored by Russia (groups associated with the Internet Research Agency, identified by Facebook as a Russian company operating disinformation campaigns); c) astroturf/movement/unregistered groups; d) nonprofits, non-FEC-groups; e) FEC groups; f) questionable "news" groups; g) news groups with extreme ideological biases; f) others (click-bait, meme generator, entertainment).

Suspicious group. A group running an issue campaign is defined as a suspicious group if a) the group's Facebook page (Facebook page linked to the ad) or landing page was taken down or banned by Facebook (Facebook took down Facebook pages linked to Russian ads identified by Facebook, or banned the groups operated by the Internet Research Agency since September 6, 2017) and no information about the group (if the name of the group was indicated in the ad or on the landing page URL) exists; b) the group's Facebook or website exists but shows little activity since Election Day and no information about the group exists elsewhere; or c) the group's Facebook page or landing page is accessible, but no information about the group exists elsewhere.[26]

Suspicious group, Russian. In the midst of our data analysis, Facebook announced they had verified Russia's election meddling (September 6, 2017). While Facebook was holding up the data, we obtained an investigative news report published by the Russian news network, RBC (October 17, 2017, written in Russian), on the Internet Research Agency and associated groups that engaged in political activities including advertising on social media. Later, the House Intelligence Committee publicly released copies of some of the Russian ads that ran on Facebook (November 2, 2017), which verified the Russian groups associated with Internet Research Agency.

We matched our sponsor name in our data or landing page information (including the full URL of the Facebook Page) with that of the data released by the Intelligence Committee. Some of the suspicious groups we identified previously turned out to be Russian ads, thus re-labeled as "suspicious group, Russian". Examples include Black Matters and Defend the 2nd.

Astroturf/movement/unregistered group. An astroturf/movement/non-registered group is defined as a group or organization that has *not* registered with the National Center for Charitable Statistics (NCCS),[27] GuideStar,[28] or the FEC. The groups also exclude stand-alone "news" production organizations. Most of these groups were active online, running a movement style campaigns (e.g., "Stop Obamanation") and generating a substantial level of engagement (e.g., likes, comments, etc.) during the election, yet they are relatively less known to the general public. Examples include the Angry Patriot Movement and Trump Traders.

Nonprofits, n*on-FEC groups*. A nonprofit (501c3, 501c4, 501c6, and other charitable groups) registered to the NCCS or GuideStar as a tax-exempt nonprofit, yet unreported to the FEC is classified as a "nonprofit, non-FEC" group. A foreign-based, yet legitimate charitable, religious organization (501c3 if based in US) is classified as nonprofit, non-FEC group (e.g., the International Christian Embassy Jerusalem). Groups indeed ran a various types of issue campaigns including candidate attack campaign, as well as a call-to-action type issue campaign (e.g., "sign *the* [sic] petition to urge the next president to stand with Israel ... to recognize Jerusalem as Israel's capital and move the US Embassy there"), without revealing their identity. Most of the groups were identified by tracking the landing page information. Examples include Judicial Watch and Numbers USA.

FEC groups. We matched the identified group names with the FEC data that contained the groups that disclosed political activities in the 2016 elections, such as Political Action Committees (PACs), Super PACs, Carey PACs, and other groups that reported independent expenditures or electioneering communications.[29] Examples include Future in America and Stop Hillary PAC (Committee to Defend the President).

Questionable news group. A group is classified "questionable news group" when it meets all of the following criteria: a) it regularly produces "news;" b) is unaffiliated with any existing non-news groups such as a nonprofit; c) has little self-identification with a group; and d) is 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"). Examples include Freedom Daily and American Flavor.

News group with extreme bias. A stand-alone news production group considered ideologically extreme by more than two media watchdog organizations, but has not been identified as one that routinely conducts false reporting.

Table 1 indicates that out of 228 groups behind the issue campaigns that human coders tracked, about half of the identified groups fall into the suspicious group category. One out of six suspicious groups turned out to be Russian-linked groups.

It is important to highlight that nonprofits (501c3, 501c4) unreported to the FEC were actively running paid issue campaigns on Facebook. The number of non-FEC nonprofits turns out to be about the same as that of Russian groups. When combined with astroturf/movement/unregistered groups that are also concerned with policy-relevant issues, the number (56) is eight times larger than that of FEC groups (7).

As shown in Table 1, the ads generated by suspicious groups are about the same volume as that of FEC groups. Combined with Russian ads, the number increased to 6,229, which is about 60% larger than that of FEC groups. The ads run by non-FEC nonprofits and unregistered groups also outnumber those of FEC groups. With the two categories combined, the volume of ads run by non-FEC groups is almost four times larger than that of FEC groups.

When counting the number of issue ads by type of group, it appears that the "other" category, including

clickbait and memes, generated a high volume of ads. However, this interpretation merits some caution: most of the ads in this category contained sensational, misleading headlines, yet did not include self-identified group names. When tracking their landing pages, it led to a meme generator, for instance. It is worth noting that Russian ads turned out to be often linked to meme generators, consistent with anecdotal case reports (Confessore & Wakabayshi, *New York Times*, October 9, 2017).

As with the content generated by suspicious groups, our qualitative examination found the issue campaigns run by astroturf/movement/unregistered groups and non-FEC reported nonprofits to be misleading. They often convey misinformation, conspicuous arguments, overtly negative emotions, or a blatant candidate attacks[30] (see Figure 1A, 1B; also Appendix 2A and 2B for more examples). Compared to the paid content by questionable news groups—which is equally misleading as that of unregistered groups and non-FEC-reported nonprofits—the number of ads run by non-FEC nonprofits is almost twice as large as that of FEC groups.

Table 1. Group Frequencies & Ad Frequencies, by Group Type

	Groups		Ads	
Group Type	N	%	N	%
Suspicious Group	102	44.7	4148	11.2
Suspicious Group, Russian	19	8.3	2081	5.6
Astroturf/Movement/unregistered	39	17.1	7443	20.1
Nonprofit (501c3, 501c4) Non-FEC	17	7.5	7447	20.1
FEC-groups	8	3.5	3958	10.7
News, Questionable	36	15.8	1935	5.2
News, Bias	4	1.8	15	0
Other (Click-bait, meme)	3	1.3	9919	26.8
Total	228	100	36961	100

Study 2
Targets: Who Is Targeted by Issue Campaigns

Analytical Procedure

Study 2 investigates the targets of issue campaigns: the individuals exposed to issue campaigns. Study 2 focuses on the same eight issue domains Study 1 investigates. While Study 1 uses a "bottom-up", qualitative approach, Study 2 employs a "top-down" approach starting from a large-scale quantitative analysis of the entirety of our data. With this top-down approach, Study 2 includes issue campaigns run by groups beyond our pre-identified groups in Study 1, thereby (potentially) diversifying the data pool of users exposed to issue campaigns.

To increase the validity, however, we take a relatively conservative methodological approach. First, selecting only unambiguous, obvious issue keywords that unarguably describe the focused issues (94 keywords across the eight focused issues; Appendix 3 for relevance rate). Second, we analyzed the entirety of more than 1.3 million Sponsored Feed ads as baseline data, but dropped Right Column ads. From Study 1, we learned that a substantial number of political ads in the Right Column contained sensational headlines, but did not include group names in the ad,[31] which require human coders to track landing pages as an alternative validity check (as in Study 1). Since each landing page is unique, without prior knowledge, little machine approximation can be achieved and a small random sample-based verification does not warrant a high level of validity.

Study 2 focuses on the targets of issue campaigns, especially the issue ads run by non-FEC reported groups. The rationale behind the decision to exclude FEC groups is specific. Many, including political communication scholars, believe that campaigns do not microtarget individual voters, especially due to the lack of sufficient resources and skills, low efficiency, and uncertainty on outcomes (e.g., Baldwin-Philippi, 2017). However, little empirical evidence beyond anecdotal observations or campaigners' own words support this argument. With a large scale, systematic empirical investigation, yet with a relatively conservative methodological approach, we strive to demonstrate that any group—even low-resourced groups—could effectively carry out microtargeting on Facebook (see Karpf, 2016). Therefore, we excluded the ads and associated targets by FEC groups (e.g., the National Rifle Association, Planned Parenthood, Super PACs, as well as candidate committees), which are known to be relatively high-resourced.

Once the ad data pool was defined, we tracked the demographic profiles of the users who were exposed to the ads. With anonymized unique individual identifiers (user IDs), we matched the ad data pool with the survey responses of the users who were exposed to the ads and created the user data pool that included demographic

profiles of the users. After all this, Study 2 focuses on a total of 26,820 ads (run by 3,046 groups) exposed to 2,615 unique individuals.

Targeting Index: Conditional Probability and Marginal Probability

We use an index to rate how likely it is a certain segment of the population (e.g., people living in Wisconsin) is being targeted with a certain type of issue campaign on Facebook (e.g., ads on the gun issue). We base the index off the conditional probability of an ad being a certain issue type given that someone in a certain segment of the population was exposed to that ad. The formula for our index is indeed the same as the one most commonly used in marketing and consumer research for targeting (Simmons's Index in Simmons® National Consumer Research Database by Experian, Inc.).

$$100 \times \frac{P(X = 1 \mid Y = 1)}{P(X = 1)}$$

For example, the targeting index for Wisconsin in regard to the gun issue should be the probability of a gun issue ad being exposed to anyone living in any state given that any ad was exposed to people living in Wisconsin (% of Wisconsin people exposed to a gun issue ad) divided by the probability of a gun issue ad being exposed to anyone in any state in the country (% of the population exposed to a gun issue ad).[32]

It is important to note that this index is calculated based on the Voting Age Population (VAP) in the Census data (the American Community Survey of the Census, April 2016; a total of 250 million individuals). Because the baseline denominators of our index are provided by the Census, this index is indeed weighted based off the voting age population of the Census, considering the population as the baseline comparison point.

An index of 100 indicates that a certain segment of the population is exposed to a certain type of ad at the same rate as the population as a whole. An index below 100 indicates that the segment is exposed to a certain type of ad at a lower rate than the national average, with an index of 0 indicating that the segment is not exposed to any ads of this type (i.e., no individual was exposed to the ad). An index greater than 100 indicates that the segment is exposed to a certain type of ad at a higher rate than the average of the population.

We consider a certain group highly targeted with a certain type of issue (HIT: *High Issue Target)* when a) the number of ads on an issue type (e.g., guns) seen by a certain segment of the population (e.g., Wisconsin) divided by the number of all the ads on the same issue type (i.e., reach) should be higher than the average share (i.e., the percentage of gun ads in a state assuming an equal probability) and b) a targeting index should be higher than 115 (100 being the national average).[33] A targeting index of 120, for example, should read as the segment is 20% more likely to be targeted than the voting age population of the nation as a whole.

Results

The results indicate that clear geographic targeting patterns exist in issue campaigns on Facebook: individuals in certain states were targeted with ads on a particular issue. Overall, it appears that Pennsylvania, Virginia, and Wisconsin were the most targeted states, with ads on each issue domain tailored for different issue interests.

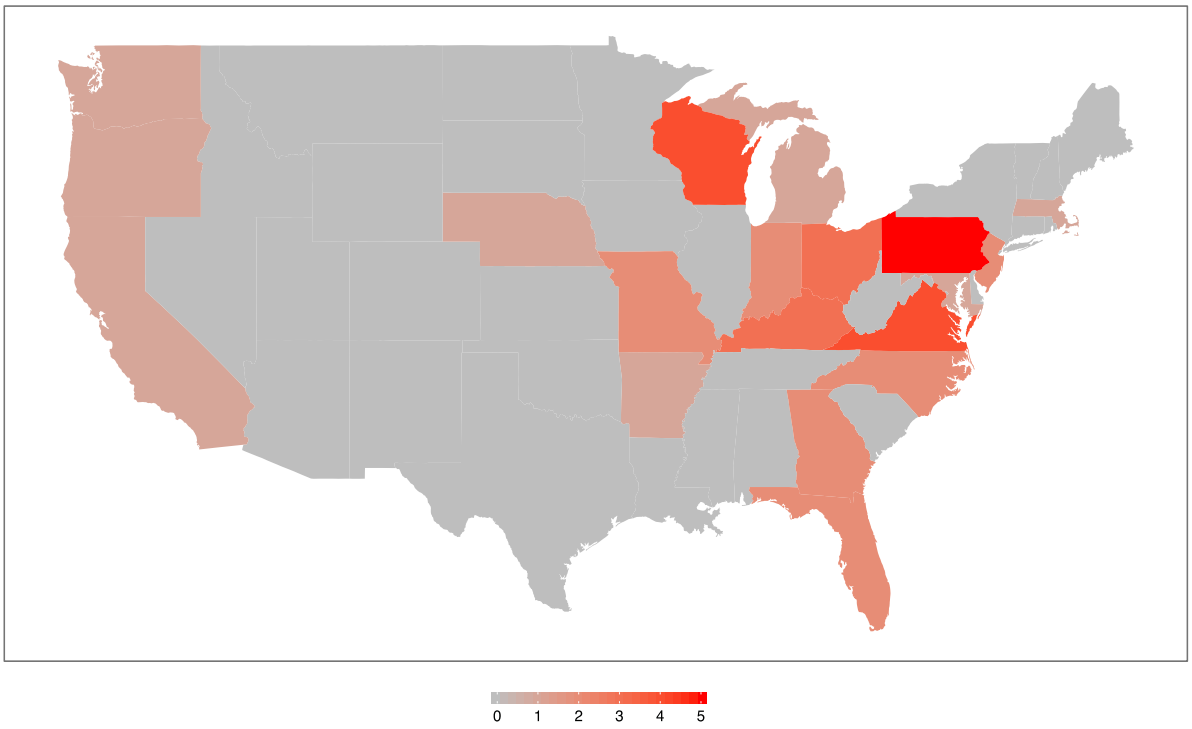
Figure 2.1.

Figure 2.1 shows a choropleth of states with a map of the HIT (High Issue Target) index indicating the degree to which users in those states were targeted with issue campaigns across our eight issue categories. Pennsylvania scored the highest on the heat map with the HIT shown in five issue categories, followed by Virginia and Wisconsin (the HIT indicated in four issue categories). Other states traditionally considered battleground states such as Ohio, Florida, and North Carolina also showed relatively high levels of geographic targeting.

Notably, the most highly targeted states—especially Pennsylvania and Wisconsin—generally overlap with the battleground states with razor thin margins. To contextualize, the average audience reach of divisive issue campaigns in each of the two most targeted states (7.6%, Pennsylvania; 2.6%, Wisconsin) is well above its vote margin (0.7%, Pennsylvania; 0.8%, Wisconsin; for vote margins in the battleground states in the 2016 elections, see Appendix 4).

Table 2 shows geographic targeting patterns by issue. For instance, ads regarding race were concentrated in North Carolina, Wisconsin (battleground states), as well as Indiana, Kentucky, and Missouri (other states). Individuals in Michigan, North Carolina, and Wisconsin (battleground), as well as New Jersey received a high volume of ads concerning terrorism (IS, the Middle East/Israel). The abortion issue, however, is the only campaign issue that Arkansas received that was more than the national average (For details for geographic targeting patterns, see Appendix 5A and 5B).

Figure 2.1. Targeted Individuals by State



Notes. A cholopleth of states by an index demonstrating the degree to which individuals in those states were exposed to ads across our eight issue categories. Pennsylvania scored the highest on this index showing evidence that it was targeted significantly more than the national average across five out of the eight focused issue domains (HIT=5). Next, Wisconsin and Virginia were targeted in four issue domains (HIT=4). Florida, Kentucky and Ohio show higher issue ad exposure in three issue domains. States colored in grey demonstrate no evidence of targeting in any of the eight focused issue domains. See Table 2 for targeting patterns by specific issue domains.

Table 2. Targeted Individuals, by State and by Issue Domain

Issue	Battleground	Non-Battleground
Abortion	PA, VA	AR, MO
Gun	PA, WI	IN, KY, OR
LGBT	OH, PA, VA	CA, GA, MD, WA
Immigration	OH, PA	NJ
Nationalism/Alt-Right	FL, VA	MA, NE
Race	NC, WI	IN, KY, MO
Terrorism	MI, NC, WI	NJ
Candidate Scandal	FL, OH, PA, VA, WI	GA, KY

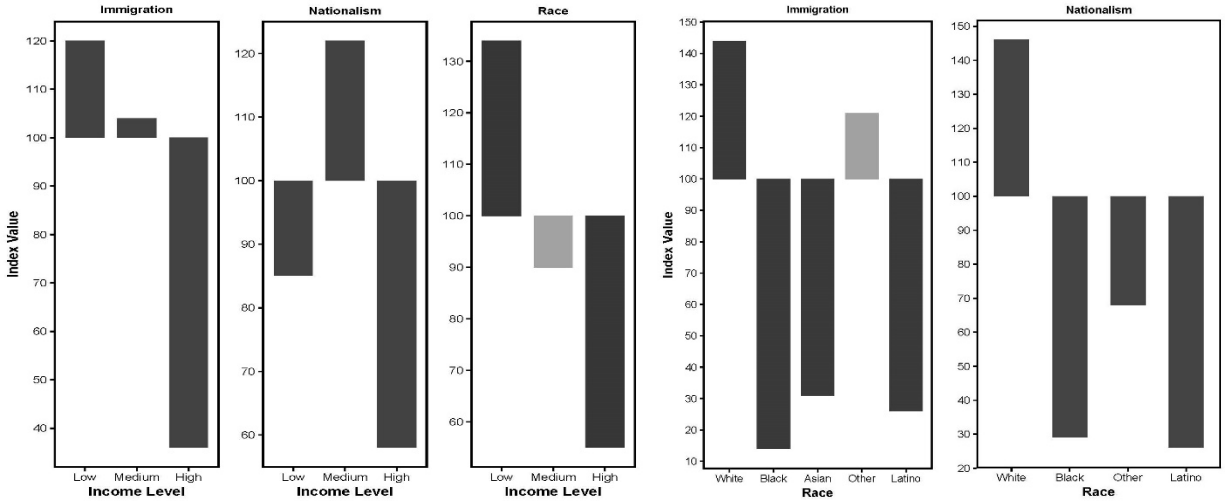
Our analysis also indicates that issue campaigns on Facebook targeted certain demographic groups. Figure 2.2A shows that compared to the national average, the low-income (household income <$40,000) were specifically targeted with ads on the issues of immigration and racial conflict. On the other hand, the middle-income ($40,000~$120,000) were targeted with issue ads on nationalism more than the national average.[34]

Whites, compared to other racial/ethnic groups, were also highly targeted with the issue of immigration, as well as that of nationalism.[35] In particular, 87.2% of

all the immigration ads (43.7% more than the average of the voting age population) and 89% of all ads concerning nationalism were concentrated among whites (46.3% more than the average of the voting age population). No other racial/ethnic group indicated evidence of targeting. (For details of demographic targeting patterns, see Appendix 6A and 6B).

Figure 2.2A. Targeted Individuals, by Income Levels

Figure 2.2B. Targeted Individuals, by Race/Ethnicity



Notes. Bars indicate Targeting Indices by individuals' income level. Targeting Index =100 (85-114) indicates the probability of the individuals being targeted is the same as the national average of the voting age population (VAP).
Figure 2.2A. The index for the middle income (= 90) exposed to the racial issue is about the same as the national average; therefore, the segment should not be considered targeted. The index bar, thus, is indicated with a lighter shade.
Low income (household income): < $40,000. Medium income: $40,000-1200,000. High income: >$120,000
Figure 2.2B. Income/Immigration: Although "Other" racial/ethnic group appears to be targeted with the immigration issue, the percentage of the immigration ads targeted to "Other" racial/ethnic group (reach) indeed was significantly lower than the average share with an equal probability assumed. Therefore, the "Other" racial/ethnic segment should not be considered targeted. The index bar, thus, is indicated with a lighter shade.

Discussion

With a user-based, real-time digital ad tracking tool, the present research traced the sponsors/sources behind the issue campaigns of 5 million Facebook Sponsored Feeds and Right Column ads, including the ads whose sponsor was *not* previously known (Study 1). Unlike conventional methods of digital data collection, such as bots scraping or archival analysis that only permits an aggregate level message analysis, this research unpacked microtargeting patterns of issue campaigns at the individual level by matching the ads exposed to each individual user with the user's profile obtained from our own survey of approximately 10,000 users. Contrary to a typical reverse engineering approach, such as simulation- or machine-based approximation of publicly available, aggregate data, our method enabled us to uncover the ads run by previously unidentified actors and the microtargeting patterns in the ads that were *not* publicly available but selectively shown and customized to specific individuals. To our knowledge, this research is the *first*, large-scale, systematic empirical analysis of who ran the issue campaigns (Study 1) and who was targeted with the issue campaigns (Study 2) on Facebook in the 2016 Elections.

Our analysis revealed striking findings. First, the results indicate that most of the groups behind issue campaigns did not report to the FEC. Almost half of the groups were classified in the "suspicious" category, some of which (20% of the "suspicious" groups) turned out to be Russian-linked groups, verified with the partial data release by the Intelligence Committee. The volume of ads run by suspicious groups was 60% larger than that of FEC-groups. The volume of ads run by non-FEC groups (nonprofits and astroturf/movement groups) was almost four times larger than that of FEC-groups. It appears that the majority of groups behind issue campaigns on Facebook are "anonymous" groups whose true identity is little known to the public.

Second, the results of our data analysis reveal clear microtargeting patterns of issue campaigns in terms of geographics and demographics. The most targeted states with divisive issue campaigns—Pennsylvania and Wisconsin—overlapped with those usually considered strong for Democratic candidates, yet turned to Trump with a razor thin margin. For example, voters in Wisconsin were targeted with the gun issue by 71.5%

more than the national average of the voting age population, and with the issue of race by 83.1% more than the national average of the voting age population. Other states heavily concentrated with divisive issues are also consistent with states that have historically been considered battleground states such as Florida, North Carolina, Ohio, and Virginia. Consistent with the theories of issue publics and microtargeting (e.g., Hillygus & Shields 2008; Kim 2009; Krosnick 1990), ads on particular issues narrowly targeted those interests. Especially, we found that ads on immigration and nationalism were particularly salient and intensively focused on white voters. Our results clearly demonstrate that data-driven political campaigns are adopted not just by resourceful political parties (Hersh 2015; Kriess 2016), but also relatively low-resourced groups (Karpf, 2016).

Firmly grounded on normative concerns for democracy, as well as the theoretical predictions long developed in political communication, we embarked on the present research with a question: Does the digital media function as the stealth media---the system enabling deliberate operations of political campaigns with undisclosed sponsors/sources, furtive messaging of divisive issues, and imperceptible targeting? The empirical evidence we have accumulated in this research, unfortunately, confirms that that is indeed the case.

It should be noted that we employed relatively conservative analytical approaches in drawing this conclusion. First of all, we only focused on the most explicit type of Facebook *paid ads*, i.e., Sponsored Feeds and Right Column ads only, excluding any ambiguous promotional methods (e.g., promoted Pages). Second, we excluded from our analysis all the unambiguous issue ads that were only designed for public education. We focused on the issue campaigns that are relevant to elections including expressive advocacy for candidates, implicitly or explicitly support or defeat of a candidate, current affairs and policy-relevant information discussed by candidates or parties; and other election relevant information. Third, in analyzing microtargeting patterns, we excluded FEC-groups who are generally considered capable of sophisticated microtargeting. Fourth, we only focused on unarguably clear-cut demographic and geographic categories (states) in analyzing microtargeting patterns, rather than operationally defined categories (e.g., cross-pressures, strong partisans, etc.). Finally, we excluded all the ads that generated low levels of validity and reliability from the analysis (e.g., ads associated with the keywords that generated a high false positive rate).

Our conservative approach indeed offers insight into better contextualizing the pressing issues in contemporary political digital campaigns and for suitably defining the scope of policy suggestions. In light of the Russian state's campaign intervention, digital platforms as a whole—which were touted for bringing about democratic revolutions such as the Arab Spring—were condemned by popular media. Various fixes have been suggested for Facebook, ranging from censorship, quality evaluation, removing engagement/reactions, stronger gatekeeping that aligns with traditional news practices, and abandoning algorithms all together (Manjoo & Roose, *New York Times*, October 31, 2017). Unfortunately, however, such fixes for Facebook or digital platforms as a whole only would ultimately conflict with the First Amendment and has the potential to freeze out marginalized voices.

In contrast, we have narrowly defined the problem as loopholes in current regulations on political advertising—the lack of (or limitations in) disclosure requirements, especially for groups engaging in issue campaigns, the exemption of disclaimers for digital political ads, and most fundamentally, no law that adequately addresses digital political campaigns. Given the increasing influence of social media on the public's informed political decision-making, increasing adoption of native advertising, and the growth of digital ads, the lack of adequate law has no clear philosophical, legal, or practical basis. Certainly, based on our empirical findings, anonymous groups might still find ways to conceal their true identities. However, adequate regulatory policies including disclosure and disclaimer requirements would, at the very least, provide the basis for public monitoring, research, and investigation.[36]

By the same token, we also suggest that digital platforms at least offer some guidelines and policies that promote transparency in political campaigns. This requires, however, a better understanding of the differences between commercial and political advertising, as well as the differential motivations and incentives behind digital advertising. For example, we found that Facebook's Right Column ad policy, which at that time did not require an advertiser's (brand) name placed in their ads, had no impact on commercial ads since, in general, businesses aim to promote brand awareness. The same policy, however, inadvertently facilitated anonymous groups' sensational, misleading, headline-style negative campaigning. When Sponsored Feeds only required a Facebook Page as a link and algorithmically promoted engagement with news feeds or Pages among friends' networks, yet did not require an external landing page, political groups created Pages with generic names concealing true identities and still utilized the algorithmic features as amplifiers for false information and polarizing the public, as exemplified with Russians' ads.[37]

The current digital political advertising practices certainly pose significant methodological challenges to political communication researchers as well. As explained in this paper previously, it is incredibly difficult to track groups who run ads on digital media. It is nearly impossible to understand microtargeting patterns. Just the sheer volume of ads generated in real time by just a few clicks makes it impossible to track and monitor the content. For example, it was reported that Trump's digital campaign team ran 175,000 variations of an ad on a day just as an experiment (Lapowsky, *WIRED*, September 20, 2017). Although our unique methodological approach enabled us to overcome such problems, when anonymous groups took advantage of the regulatory loopholes on digital media at every level, neither machine learning nor name matching generated valid results. We had no choice but to remove those cases from analysis in the present

research. Future research should strive to overcome such limitations.

Despite the limitations, however, the present research illuminates important normative issues. The proliferation of anonymous groups and dark money campaigns raises questions of not only the transparency and accountability of governing systems, but also the significance of political parties in contemporary democracy. Gerken (2014) maintains that a deeper problem that underlies anonymous campaigns is that groups behind these campaigns become "shadow parties." These groups are outside of the political party system, yet have begun functioning as political parties in that they raise money, push issue policies and candidates, and house the party leadership. This shifts the balance of power between party leadership and members and that of political elites and voters. In a similar vein, Skocpol and Hertel-Fernandex (2016) argue that shadow parties have supplanted the role of traditional parties, exerting a great deal of influence on political elites and rendering ideologically extreme policy decisions. This contention follows previous political science scholarship that has demonstrated that the decline of traditional party organizations, relative to non-party entities, increases ideological polarization (La Raja & Schaffner, 2015).

Political elites' strategic polarization is furthered by microtargeting. With ubiquitous data and analytics that profile voters in as much detail as possible, and with digital media able to reach narrowly defined voters with customized content, political elites now widely adopt microtargeting strategies for communicating policy issues to their constituents. Catering to a fragmented, niche-issue interest rather than the broad public, political elites' microtargeted communication, however, bypasses public and forecloses a wide range of public policy discussion (Hillygus & Shields, 2009).

Simulation research (Glaeser, Ponzetto, & Shapiro, 2008) also demonstrated that as campaigns obtain more information about voters and provide customized messages to narrower segments of the population, candidates take more extreme positions on policy issues. Hillygus and Shields (2009) found that compared to television advertising, direct mail focuses on wedge issues, targeting narrow segments of persuadable voters who hold strong attitudes toward those issues. This suggests that microtargeting further moves political elites to extreme policy positions, and the electorate is sharply divided within a wide range of conflicting policy options.

Cynics might still argue that political elites, as well as outgroups, have always looked for back channels, dark money campaigns, and "silent" messages in various ways. Is the digital media the only tool for a stealth campaign? Perhaps not. However, it is worth noting that the behind-the-scenes information operation on digital media is above and beyond any other operation we have ever seen in the past in terms of its scale, speed, and most importantly, its capacity to amplify information.

With the continuing decline in broadcast media and the exponential increase in data-driven, algorithm-based, globally networked digital platforms, we must ask what anonymous groups' stealth political campaigns on the digital media means for the functioning of democracy. Further, the question of how to address the problems we recently witnessed— such as election campaign intervention by a foreign entity— warrants considerably more public debate.

Appendices/Examples: https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/04/Supplemental-Materials.Appendices.Ad-Samples.pdf

[1] We define outside groups as any type of organized interest that exists outside of formal political leadership. In the context of election campaigns, outside groups are independent of, and not coordinated with, candidate committees. Outside groups typically refer to interests groups (or pressure groups), nonprofits, astroturf/movement groups, or the like, and formal or informal organizations.

[2] It must not be confused with an issue ad, a narrower legal term in election law (see below). Issue campaigns can take all of the following three types of ads defined in election law: First, *express advocacy*. It refers to ads that expressively advocate the election or defeat of a clearly identified candidate by using expressive phrases (namely, magic words, "vote for" or "vote against"); Second, *electioneering communications* refers to ads including a clearly identified candidate for federal office, but the message is subject to interpretation. Thus, unlike express advocacy, electioneering communications do not contain expressive phrases. However, campaigns that are a) run on "airwaves"—broadcast, cable, or satellites communications; b) made within 60 days before the general election or 30 days before a primary— the so-called FEC window; and c) publicly distributed to the electorate qualify as electioneering communications. Third, *issue ads* include campaigns designed to further or detail a political issue, legislative proposal, or public policy but do not contain express advocacy phrases or do not qualify as electioneering communications fall under issue ads.

[3] Such phrases, called magic words, include "vote for," "vote against," "support," "oppose," "elect," "defeat." Campaigns that contain expressive advocacy words and phrases fall under expressive advocacy.

[4] However, ads concerning policy issues that are run during the "FEC window," i.e., within 60 days before the general election and 30 days before a primary, do not qualify as issue ads. The ads this paper empirically examines indeed fall within the FEC window.

[5] Those groups include tax-exempt nonprofits—that is, groups with IRS tax code 501c3 (religious, scientific, and educational charitable organizations, e.g., NAACP), 501c4 (social welfare groups, e.g., National Rifle Association, Planned Parenthood), 501c5 (labor unions, agricultural groups), 501c6 (trade associations), and the like.

[6] Independent expenditure-only Political Action Committee. As guided by *Citizens United*, Speechnow.org v. Federal Election Commission lifted a limit on contributions by Super PACs.

[7] However, exactly what activity constitutes the promotion of public education or common goods, but not political is, at best, unclear.

[8] In layperson's terms, native advertising is used more broadly to refer to any organic promotional tactic such as word-of-mouth or viral marketing. However, our definition of native advertising refers to an advertising strategy for *paid* content.

[9] Facebook's own investigation revealed that by taking advantage of the native advertising capacity of Facebook, disinformation campaigns (including Russian operations) used a false news style

that purported to be factual but contained intentional misstatements of fact with the intention to arouse passions, attract viewership, or deceive users. A "fake news" phenomenon thus can be a purposeful operation (Weedon, Nuland & Stamos, Facebook, April 2017).

[10] On Twitter, on the other hand, much of disinformation and misinformation was amplified by automated, algorithm-based, computational bots that simulate the message sharing by human beings (Kollanyi, Howard, & Wooley, 2017).

[11] Hillygus and Shields (2008) further specify the most persuadable issue publics as those who consider a particular issue important, yet their issue position is not consistent with their own party's issue position, such as a pro-gun Democrat or an LGBT Republican.

[12] The empirical research presented in this article (Study 1 and Study 2) is part of a larger scale research project, EScope, which tracks and analyzes digital campaign content, sponsors/sources, and targets with a reverse engineering. The project collected 87 million digital promotional messages exposed to more than 17,000 volunteers who used a reverse engineering app, EScope. The data collection was conducted between February 15 and May 3, 2016 (the 2016 Primary Election Study) and between September 22 and November 9, 2016 (the 2016 General Election Study).

[13] We randomly drew 520,882 messages and hand-labeled whether an ad was a political campaign message or not.
The number of political messages indeed varied by type of platform. Across platforms, however, an average of 23.7% of promotional messages turned out to be political campaigns. We define a political digital campaign as any organized digital operation that is designed for a political purpose including persuasion, Get-Out-The-Vote (GOTV), donation/kick-back, solicitation of volunteers, petitioning, polling, event organization (e.g., Meet Ivanka), or the like.

[14] Even few notable research of digital political advertising (e.g., Ballard, Hillygus, & Konitzer, 2016) has been limited to an analysis of non-interactive simple web display ads by *previously known actors* (e.g., major presidential candidates) that were placed on *publicly accessible websites only* and anecdotally scraped by a third-party company. A non-interactive simple web display ad is similar to an ad in print media and fundamentally differs from the majority of digital ads as it does not have the capacity for individual-level targeting such as behavioral targeting, geographical targeting, or algorithm-based targeting.

[15] Our reverse-engineering approach is similar to crowd-sourced algorithm auditing. It significantly advances the existing approach, however, by participants' explicit consent process; unobtrusive data collection and automated data transfer; and integration of comprehensive user surveys. Most importantly, our approach includes more comprehensive, real-time, longitudinal observation that enables us to better predict who was targeted, for what reason, and how.

[16] Partnered with multiple online research firms, GfK runs the largest online participants pool in the United States.

[17] In recruitment, GfK used the demographic profiles (gender, race/ethnicity, household income, education, age, region/state) of the Current Population Survey (March Supplement, 2016) of the Census as the benchmark. For the projection of registered voters in the general population, GfK used GfK's Knowledge Panel survey responses after the full panel was weighted to the demographic benchmark from the Current Population Survey.

[18] Compared to the Census (female 52% vs.-male 48%), the GfK online pool (female 59% vs. male 41%) as well as our sample (female 64% vs. male 35%) included more females than males. However, the difference was not significant (Cramer-V = .27). The sample also included more registered voters (94%) than the GfK's general population estimates (85%), but the difference was not significant (Cramer-V = .23). In terms of age, however, the sample (median = 37) is closer to the online population (voting age only online population, median = 33), but slightly different than the voting age population (median=45). See Appendix 1 for the comparison between the Census (the 2016 American Community Survey, voting age only), the online population (GfK 2016, voting age only), and our sample.

[19] The app was developed by the research team in consultation with Moat, a leading digital advertising analytics firm. If added to a browser, it works on mobile devices as well.

[20] At the time of recruitment, volunteers for the 2016 General Election Study were asked to install EScope and fill out our baseline survey. The baseline survey appeared as a pop-up window once the app was installed. There was no time lag between the recruitment, installation, and administration of the baseline survey. The recruitment site was open between September 22 and October 3, 2016. The majority of users (8,587, 88% of the sample) were recruited by September 28, 2016; thus we included the ad data from September 28 to November 8, 2016 for data analysis.

[21] Based on the hand-labeling of random sample ads, we estimated that approximately 1.6 million of the Facebook campaigns (23.7%) would be political campaigns (see Note13). When we focused on Sponsored Feeds and Right Columns only, we found approximately 12% of Sponsored Feeds (~163,451) and 2% of Right Columns (~747,476) are paid political ads, yielding a total of 1 million paid political campaigns. The estimate is generally consistent when employing a "dictionary approach." The research team developed a "political ad dictionary (v.1.2)" based on initial content analysis that contained 358 keywords associated with the issue campaigns of 17 policy-relevant issues, several candidate scandals (e.g., Access Hollywood; Hillary's email-server; Clinton Foundation, etc.), standard candidate endorsement ads, fundraising, and GOTV ads. The word-matching keyword search yielded a total of 1,034,063.

[22] The sample ads illustrate how a typical Sponsored Feed and Right Column ad looked at the time of our data collection period. Recently, Facebook changed their Right Column formats and expanded its size and engagement capacity.

[23] The issue keywords were taken from our political ad dictionary (v.1.2), which was designed to capture political ads (see Note 20).

[24] We define a political ad broadly as any content of political campaigns (Note #13 for definition of a political campaign). The content has direct or indirect policy implications including current affairs; nationally or internationally important agenda or collective action; election relevant agenda (including any issues ever mentioned by federal candidates) or party platform issues; mentions of candidates (any levels of elections); or mentions of parties. At an operational level, trained coders employed two-step coding. Trained coders first excluded obvious commercial ads, defining the rest as political ads. Next, trained coders classified political ads into two types: (a) political, yet with no direct policy implication or with no election relevance (public education only; 0.1% of the sample Sponsor Feeds; 0.4% of the Right Side sample) (b) political ads with election relevance.

[25] If the sponsor was clearly identified as a candidate committee with a full disclaimer ("paid for by") and the name of the disclaimer was exactly matched and verified with the FEC data, we excluded the ads because the focus of this study was tracking the ads by outside groups. With our conservative approach, however, only three candidate committees (out of 1,038 registered candidate committees) turned out to use the registered name on Facebook ads.

[26] For instance, a group that did not identify itself conducted a campaign "syrianrefugeethreats.com" and ran petition ads to stop the entry of Syrian Refugees into the U.S. (and Europe). The original campaign Facebook page was not found and the landing page was not accessible. Similarly, groups called Trump Insurrection, Trump Nation Now, and other groups with similar names all ran the same campaign, "Support the 2nd Amendment? Click LIKE to tell Hillary to Keep Her Hands Off Your Guns". Their Facebook pages, however, were taken down, we were unable to

track them further. We did not find any information about those groups in the FEC-data, NCCS or Guide Star. The ads run by Trump Nation Now indicated the sponsor as Trump Nation in the ad text (even though the landing page directed us to Trump Nation Now). However, no sufficient information existed to establish the link between the two groups, Trump Nation Now and Trump Nation. In regard to Trump Insurrection, the only information we found that might be related to the group was an archived website trumpinsurrection.com (available through Wayback Machine). Even the archived website, however, did not contain any information about the group.

[27] The NCCS archives
all active organizations that have registered for tax-exempt status with the IRS and compiles IRS Business Master Files (BMF).

[28] Similar to the NCCS, GuideStar archives all financial and business information of registered nonprofits.

[29] As of January 13, 2017, the FEC data included 4,555 groups.

[30] Even though these ads tend to implicitly support or attack a particular candidate, only a few of them included the FEC-defined "magic words" that explicitly advocate for support or the defeat a candidate. Among the ads analyzed in Study 1 (36,961 ads). Only 3258 ads (adjusted after taking into account false positive rates) contained the magic words (8.8%). 9,105 ads (24.6%) included presidential candidates' names.

[31] Among the randomly drawn sample of Right Column ads (16,616), only 45.9% of political groups identified their names in the ads.

[32] Howard and his colleagues' data memo (Howard et al., 2017) on the concentration of junk news in swing states uses a functionally similar index, the ratio of ratios although three differences must be noted. First, is the unit of analysis. Howard and his colleagues count the number of junk news items (tweets) which, if adopted to this study, the unit of analysis would be an ad. The unit of analysis adopted to calculate our index in Study 2 is a unique individual user. Second, while the ratio of ratios uses a conditional probability without providing the baseline population information, our index uses a conditional probability *and* a marginal probability to provide baseline information about the population obtained from the Census data. Third, is the balance point of the index. Howard and his colleagues' ratio of ratios uses a log transformation, a conventional normalization for skewed sample with 0 being the balance point. Our unit of analysis in Study 2 is a unique individual user, and as our index includes conditional and marginal probability, we multiply the probability by 100, with 100 being the balance point.

[33] Even though our sample generally mirrors the Census, one might argue that our Facebook users might be different than the population. Given the lack of information about the Facebook user population, we are unable to examine systematic differences between our Facebook users and the Facebook population. Therefore, for each segment, we created three types of indices by considering three different baseline denominators (i.e., when calculating P (Y =1)), a) the voting age population (the 2016 ACS, the Census); b) our survey sample; and c) our Facebook sample. Then, we take a targeting index *only if all three indices are higher than 115*.

[34] While ACS Census used the three income categories (Low income: <$35,000; Middle income: $35,000~$100,000; High income: > $100,000), our survey used five categories. We collapsed our categories into three to make the survey and the Facebook baselines best comparable to the voting age population baseline obtained from the ACS Census.

[35] The immigration indices: "Other" racial/ethnic group appears to be targeted with the immigration issue when only reading indices (indices > 115 Figure 2.2B). However, the percentage of the immigration ads targeted to the "other" racial/ethnic group was indeed significantly lower than the average when an equal probability is assumed. Therefore, the "other" racial/ethnic group should not be considered a high issue target; the index bars thus were indicated with lighter shades.

[36] During our study, a bicameral, bipartisan bill, the Honest Ads Act, was introduced and sponsored by Senators Amy Klobuchar (D), Mark Warner (D), and John McCain (R) to close the loopholes (Klobuchar, A., S.1989 Honest Ads Act; 115th Congress, 2017-2018). The bill would a) expand the definition of electioneering communications that mention federal candidates to include paid digital ads and therefore subject them to disclaimer and disclosure requirements; b) require digital platforms (with 50 million or more unique monthly visitors for a majority of months) to maintain a complete record of political advertisements of the sponsor whose total spending exceeds $500; c) require digital platforms to make reasonable efforts for foreign entities not to purchase political ads. It is certainly a very welcoming and encouraging policymaking move that would provide an important basis for regulatory policies and guidelines. Still, however, given that it is confined by the current definition of electioneering communications, the disclaimer and disclosure requirements are only limited to the ads that mention candidate names (Note 30: Only 24.6% of the ads we analyzed contained presidential candidate names).

[37] In response to Congressional investigations, Facebook promised to adopt new policies to increase the transparency of digital political ads on their platform. For instance, in the U.S. federal races, "advertisers may be required to identify that they are running election-related advertising and verify both their entity and location" (Goldman, *Facebook*, October 2017). It is, however, unclear about what "election-related advertising" constitutes and how verification is processed. It must be guided by clear and consistent regulatory policies. Facebook also announced a new system that would weigh down users' engagement with Facebook pages in their engagement matrices. Notably, however, while this change will greatly decrease non-paid content promotion, it will *not* be applied to paid promotions including Sponsored News Feeds (Hern, *the Guardian*, October 23, 2017).

Addendum: Since the completion of the data analysis, we discovered that one of the suspicious groups (that ran 15 ads, total) did file a report to the FEC. To have the most up-to-date information, on April 17, 2018, we reclassified the group into the FEC-group and revised Table 1 accordingly. However, the patterns found in this research---the proportion of group types and ads, and targeting--- remain the same as those of the earlier version.