CENTER FOR DIGITAL DEMOCRACY

24 May 2018

The Center for Digital Democracy (CDD) respectfully urges the Federal Election Commission (FEC) to adopt regulations to ensure that voters will have meaningful transparency and control over the digital data and marketing practices used in elections today. The FEC must boldly act and use its legal authority and leadership position to enact—as well as recommend—much-needed safeguards. We call on the FEC to tell campaigns that they must refrain from using digital tactics that promote "voter suppression." It should also urge federal candidates not to use viral and other forms of stealth communications to influence voters through misinformation—including "fake news." The FEC should go on record saying that political campaigns should not deploy digital marketing tactics that have not been publicly assessed for their impact on the integrity of the voting process—such as the use of predictive artificial intelligence products (including bots) and applications designed to bypass conscious decision-making (through the use of neuromarketing and emotionally based psychometrics).

The Cambridge Analytica/Facebook incident should serve as a wake-up call for the FEC, which needs to update its policies and practices to address the realities of 21st century political marketing. Rather than an aberration, Cambridge Analytica/Facebook's work together largely reflects how digital marketing routinely operates with political and other campaigns—in the U.S. and globally. Today's election campaigns are fought using all of our devices—known as omnichannel marketing. An individual's mobile phone, tablet, PC and digital TV are increasingly linked together (via a unique number) so candidates can continually send ads that follow a voter from place to place via the most appropriate device (mobile while in the street; PC at office or school, TV at home, etc.). An array of "Big Data" services gather, store, sell and make available an array of personal information to be used for voter targeting, such as from Data Management Platforms (DMPs), Data Marketing Clouds, and cross-device identification companies. Ad formats and messages are tested and honed and made more effective regardless of device, using multivariate and biometric testing. Highly personal and granular information is harnessed to allow for more effective micro-targeting, using individuals' real-time geo-location as well as data regarding their race, ethnicity, finances, health and political interests. Groups of voters are targeted as well through "look-alike" modeling and other practices. Political campaigns also use the most popular formats originally developed to sell consumer goods, including native, mobile, influencer and social ads. Data on individuals, communities and other groups are analyzed and used to fuel microsecond decision-making ad-targeting platforms—so called programmatic marketing. Interactive marketing messages to voters can be dynamically changed in

nearly real-time, based on their prior reactions and what device they may be using at a particular time.

In other words, political advertising via the Internet and digital platforms is not the same as such advertising on traditional radio and television. We are now faced with "smart" ads that know a person (or a group), can shadow them wherever they go, and "learn" about their interests, fears and concerns to take better advantage on a continuous basis.

There has been an explosion of companies helping create and deliver online political marketing, including giant ad and content platforms Google and Facebook; phone and cable Internet Service Providers, including Verizon/AOL and Comcast; and marketing services companies like WPP and Nielsen. There is also growing consolidation in the political marketing sphere, giving candidates and campaigns one-stop shopping for an array of powerful tools to reach and influence the public.

Public Communication: The FEC's definition of "Public Communication" should include "service," so it covers all "internet-enabled devices, applications and services." This would help address the growing distribution of digital political ads on television, including on cable, broadband and streaming (OTT), where there may not be an Internet-enabled end device. Public Communication should also reflect all the methods used by political campaigns to distribute ads and messaging in the current digital media system. This should include purposefully viral content promoted initially by what are known as "influencers." In other words, even if no funds were used beyond the initial paid sponsorship to have someone distribute the content, disclosure rules should be required when other people subsequently post the message. A similar rule is required for "native" ads (which are disguised as content) and where the goal is to have people repost without also including any initial disclaimer regarding its paid status. In other words, the FEC should adopt a rule that reflects an understanding of how so-called "free media" is generated today for political marketing purposes. The FEC should specifically reference Internet of Things, Virtual Reality, Algorithmic analysis and Artificial Intelligence as part of "Internet Public Communication" to reflect how these techniques are already part of the political marketing paradigm. Given that both radio and television are being delivered in ways designed to generate targeted digital advertising (via programmatic methods), it is important to include both audio and video Internet services under the definition.

Disclaimers: The FEC must require disclaimers to be tested and measured using the same methods relied on by every digital marketer—usability testing (UX). Ads are routinely designed to make sure they are truly visible, convey the desired information, and have a real impact. Through trade groups such as the IAB, ad formats are tested and standardized to make sure marketing content is effectively conveyed across devices and applications. The FEC should insist, for example, that the same effort that goes into ensuring various mobile ad formats are effective be applied to the development of political disclaimers. Unless disclaimers are tested to

ensure their efficacy, they may be deliberately crafted so they are purposefully ignored—buried in digital fine print. The testing and measurement techniques that demonstrate "viewability" and comprehension should also be made publicly available.

We believe that such testing must be required in order for the FEC even to consider whether it is appropriate to allow campaigns to place disclosures via links away from the ads themselves. Political advertisers and ad services such as Google and Facebook must first demonstrate to the FEC, via objective testing, that placement of complete or partial disclosure data outside the confines of the ad is necessary. As the commission knows, digital marketing is a very creative field and has made tremendous strides promoting information using very small screens and with highly limited space for copy. The same innovative effort should be required to ensure meaningful disclaimers. That is one reason why it is premature to permit "safe harbors."

Political Campaigns must be required to fully disclose their data and marketing practices: In response to the public outcry over Cambridge Analytica, including congressional hearings, several companies (Facebook and Twitter, for example) have voluntarily adopted a number of new corporate policies to promote transparency and disclosure. But such self-regulation, while a positive development, is insufficient when it comes to ensuring the voting public enjoys comprehensive safeguards for political digital ads. The FEC should adopt rules that require political advertisers to make publicly available complete information on how prospective voters are targeted. That includes identifying all the targeting techniques used (such as look-alike modeling, geolocation tracking, programmatic delivery, cross-device, etc.). Disclosure should also identify all the data sources used, including those from data brokers, ad platforms, marketing clouds and political parties. This information should reveal whether race, ethnicity, financial, health and other sensitive or psychometric data were used. Given the serial and real-time nature of digital ad campaigns, disclosures should also address how the data generated from an ad were subsequently utilized (for targeting on Facebook, digital TV, mobile devices, etc.).

The FEC must speak out on what is needed to protect the integrity of the electoral system regarding the role of advertising and voter decision-making in the digital era. It should adopt regulations that take advantage of already developed applications created by the digital ad industry designed to ensure a marketer's goals are met. It is in everyone's interests to make paramount requirements that ensure fair elections, foster an informed electorate, and reflect the priorities of our democracy.