CENTER FOR DIGITAL DEMOCRACY

1875 K Street, NW
4th floor
Washington, DC 20036
202-986-2220
www.democraticmedia.org

November 9, 2017

Comment by the Center for Digital Democracy

Advance NPRM on Internet Disclaimer Notices\REG 2011-02

The Center for Digital Democracy (CDD)[1] respectfully calls on the Federal Election Commission (FEC) to hold hearings examining the role that the Internet and related digital data applications now play in federal political campaigns. The public needs a better understanding of how contemporary digital practices in the "Big Data" era affect our electoral system. CDD also urges the FEC to begin a rulemaking to revise its regulations concerning disclaimers so the public has appropriate access to information regarding the operations of online ads and related content.

In the 2016 election cycle, political campaigns for president and other federal offices used a wide range of digital and data applications that were originally developed by the commercial online marketing sector. These include data processes that are designed to build robust profiles of individuals and groups of online users, and include information related to their use of mobile phones, personal computers, set-top boxes and other

[1] The Center for Digital Democracy is a nonprofit organization located in Washington, DC, that is recognized as one of the leading consumer protection and privacy organizations in the United States. Since its founding in 2001 (and prior to that through its predecessor organization, the Center for Media Education), CDD has been at the forefront of research, public education, and advocacy protecting consumers in the digital age.

devices (known as cross-device data onboarding). Leading platforms such as Facebook, Google and many other digital media services now provide an array of additional data and marketing services—including through so-called "marketing data clouds"—that are used to enhance profiles for micro- and group-targeting purposes. These profiles can include information on individuals' financial status, health concerns, racial and ethnic status, their interests and spending (online and offline), as well as their geolocation (including in real-time). Such commercial data profiles are now routinely merged with voter profiles in order to target the electorate, a process that is invisible to the public.

In 2016, the U.S. witnessed the widespread use of "machine-driven" (or "programmatic") advertising for political campaigns, where potential voters' attention is bought and sold in milliseconds—using algorithms and robust data profiles—for targeting across platforms, publishers, and devices. "Lookalike" modeling, in which potential voter targets are "cloned" according to an analysis of profile data from other individuals, was also used in the last cycle. So was "native" advertising, which purposefully blurs the distinctions between editorial content and advertising. Both Google and Facebook also played important roles in 2016, providing insights and other services on data and device targeting of voters. We also witnessed the use of political data-driven targeting for voter suppression purposes, to dissuade turnout and undermine potential support of particular candidates.

The use of classifying and predictive Big Data analytics and advanced advertising and marketing practices in political campaigns is now common, just as they are already routinely used with a high level of sophistication to target and influence consumers for commercial purposes. The practices have evolved so much that updating disclosure requirements alone is no longer sufficient to preserve the integrity of the electoral process.

Among the questions FEC hearings should address are the following:

- How have these new campaigns techniques **influenced** the public via highly personalized micro-targeting, which can be tailored to exacerbate voters' fears, concerns, and subconscious behavioral biases?

- Can these practices affect the voting population unequally, resulting in **digital voter suppression and exclusion** of certain groups and individuals from deliberation and debate?

- What kinds of commercial **data sources**, such as those from data brokers, digital ad companies, and mobile providers, are being merged with voter files?

- How can **transparency and trust** in the electoral process be improved through more effective disclosures and limits on the most egregious attempts at voter influence?

- What additional **safeguards**, if any, are available so Americans can determine whether political data about them derived from commercial sources ought to be used by political campaigns?

We urge you to hold hearings examining the role that the Internet and related digital data applications now play in federal political campaigns, and to begin the rulemaking to revise your regulations concerning disclaimers on certain Internet communications.

Jeffrey Chester, Executive Director
Katharina Kopp, Policy Director