NYU TANDON SCHOOL OF ENGINEERING

PRESS OFFICE • 1 MetroTech Center, 19th Floor, Brooklyn, NY 11201

CONTACT • Kathleen Hamilton
646.997.3792 / mobile 347.843.9782
kathleen.hamilton@nyu.edu

Images at https://nyutandon.photoshelter.com/galleries/C0000DKT3j1lAvpA/G0000jKxM9ixg_VI/Transparency-Project
EMBARGO: FRIDAY, MARCH 6, 202007:30 a.m. EDT

Researchers report widespread disclosure violations

in political advertising on Facebook

NYU Tandon School of Engineering study tallies the cost of inauthentic ads and makes a case for independent monitors

BROOKLYN, New York, Friday, March 6, 2020 – A new study by data scientists revealed systemic flaws in Facebook's political ad monitoring and enforcement processes, which allow foreign entities or shady businesses to continue to advertise despite long-term violations.

The researchers at New York University Tandon School of Engineering revealed numerous examples of advertisers employing disinformation tactics and discovered $37 million in advertising – representing 55 percent of all pages with political ads during the study period – that failed to identify the funding source, in violation of Facebook policy.

The NYU Tandon researchers noted failures of Facebook to enforce its own policies and called for outside monitoring of its political ad library, to increase transparency for voters. They pointed to the data the NYU Tandon team collected, by means of both machine learning algorithms and manual investigation, as evidence that independent monitoring is effective.

The researchers meanwhile credited Facebook for being the only digital advertising platform to provide a level of transparency sufficient for them to detect disinformation campaigns.

Their study, which will be presented in May at the IEEE Symposium on Security and Privacy, the leading research conference in the field, also reported:

- Sixteen ad clusters were placed by likely inauthentic advertisers, often using disinformation tactics similar to those employed by the Russian-backed Internet Research Agency. These tactics included targeting readers by race, gender, union membership, or veteran status – identity markers well known to be highly effective in organically spreading messages. They identified 19,526 ads, worth at least $3.86 million, placed by these inauthentic communities. Once people engage, their data is often collected for future political micro-targeting.

- It took Facebook an average of 210 days to shut down such inauthentic groups – longer than digital ads typically run.

- Dubious commercial operations promoting, for example, “TrumpCare,” “Christian Health Plans,” or “Heroes Home Buyers Program” – none registered legal entities – used similar micro-targeting tactics and violated Facebook disclosure policies. These were most prevalent in the Midwest and Rust Belt. Others used “astroturfing” techniques – pretending to be independent people instead of companies – to secretly promote their interests. The researchers pointed out that such questionable commercial practices likely extend far beyond the political advertising that comprised their study.

- The largest category of inauthentic ad clusters fell into the clickbait category and often employed political or seemingly apolitical influencers who didn’t report their funding. In one example, a Lithuanian entertainment company placed ads on 116 pages, ranging from “Homestead & Survival” to “Drunk Texts.” New pages kept popping up as old ones were shut down – none ever disclosing the source of the advertising. By the end of the study, clickbait communities had disappeared – probably because of aggressive action by Facebook, the authors wrote. Facebook’s recent decision to allow influencers to forego disclosure of their financial backers will further harm transparency, the researchers warned.

- During the study period, Facebook did not check the accuracy of the citations of those who bought political ads, nor, with few exceptions, did it prevent inaccurate disclosure, according to the researchers. It also did not penalize repeat offenders or take down ads that were clones to non-compliant ones that it previously took down. After the study, Facebook changed its policy and will now write the disclosure strings for certain large political advertisers, but the researchers pointed to prior instances when Facebook did not enforce its policies and said it is unclear whether enforcement will change.

- They cited the case of China Xinhua News, the state-run press agency recently designated by the U.S. State Department as a foreign government functionary rather than a news agency. Despite China Xinhua News repeatedly being caught failing to disclose political ads, the researchers found no instance of meaningful long-term enforcement. This was despite Facebook’s policy banning advertising by foreign entities.

- The importance of outside monitoring was illustrated by the fact that Facebook restored some 46,000 ads, worth at least $7.37 million, when the NYU Tandon researchers reported them missing from the archive. They had been unintentionally excluded. Facebook had promised to keep all political ads in its library for seven years but when it changes its advertising policy, it applies the new rules retroactively, thereby removing once-banned ads from the archive shared with certain researchers and news organizations.

The study suggests methods for reducing honest errors, but the researchers also called for a strict “trust but verify” security policy to replace the current one, in which advertisers self-certify they are the source for ads.

The study evolved from the team's Online Political Ads Transparency Project, the first security analysis of Facebook's U.S. Ad Library API. That Facebook tool allows authorized outsiders to monitor election interference. The latest NYU Tandon study is the first to propose an auditing framework – particularly important in light of the shortcomings revealed by the team's own audit. But even their new algorithm developed to reveal dubious advertising will be insufficient to thwart adversaries intent upon spreading disinformation, researchers warned.

"This study shows large-scale disclosure issues. We recommend that Facebook take on a more active role in improving its Ad Library security so that fewer political advertisers are able to avoid accurate disclosure and transparency," said NYU Tandon Assistant Professor of Computer Science and Engineering Damon McCoy, who leads the Online Transparency Project. "Facebook appears to be taking steps in the right direction, and it has made the most political ads transparent, enabling us to identify election interference techniques. On the other hand, we found several limitations, such as not providing ad targeting information, which hindered transparency. However, we thank the team at Facebook for creating a transparency library that was the only one that provided enough data to meaningfully study. Google doesn't include issue advertising, and Twitter's transparency center lists only a few hundred advertisers, compared to 126,000 pages with transparent political ads provided by Facebook."

The clustering algorithm to reveal undisclosed coordinated advertising, developed by McCoy and NYU doctoral student Laura Edelson, will be shared with other researchers studying Facebook's political advertising.

The study, "A Security Analysis of the Facebook Ad Library," was conducted on data covering one year beginning May 2018. It is available at http://damonmccoy.com/papers/ad_library2020sp.pdf. A National Science Foundation grant helped support the research, and the Online Transparency Project receives funding for its research on Canadian election advertising from the Digital Ecosystem Research Challenge.

About the New York University Tandon School of Engineering
The NYU Tandon School of Engineering dates to 1854, the founding date for both the New York University School of Civil Engineering and Architecture and the Brooklyn Collegiate and Polytechnic Institute (widely known as Brooklyn Poly). A January 2014 merger created a comprehensive school of education and research in engineering and applied sciences, rooted in a tradition of invention and entrepreneurship and dedicated to furthering technology in service to society. In addition to its main location in Brooklyn, NYU Tandon collaborates with other schools within NYU, one of the country's foremost private research universities, and is closely connected to engineering programs at NYU Abu Dhabi and NYU Shanghai. It operates Future Labs focused on start-up businesses in Brooklyn and an award-winning online graduate program. For more information, visit engineering.nyu.edu.

About the NYU Center for Cyber Security
The NYU Center for Cybersecurity (CCS) is an interdisciplinary research institute dedicated to training the current and future generations of cybersecurity professionals and to shaping the public discourse and policy, legal, and technological landscape on issues of cybersecurity. NYU CCS is a collaboration between NYU School of Law, NYU Tandon School of Engineering, and other NYU schools and departments. For more information, visit cyber.nyu.edu.

###

Key words: online advertising, political advertising, election advertising, clickbait, astroturfing, Facebook, Instagram, cybersecurity, security analysis, advertising disclosure, misinformation, social media

www.facebook.com/nyutandon @NYUTandon