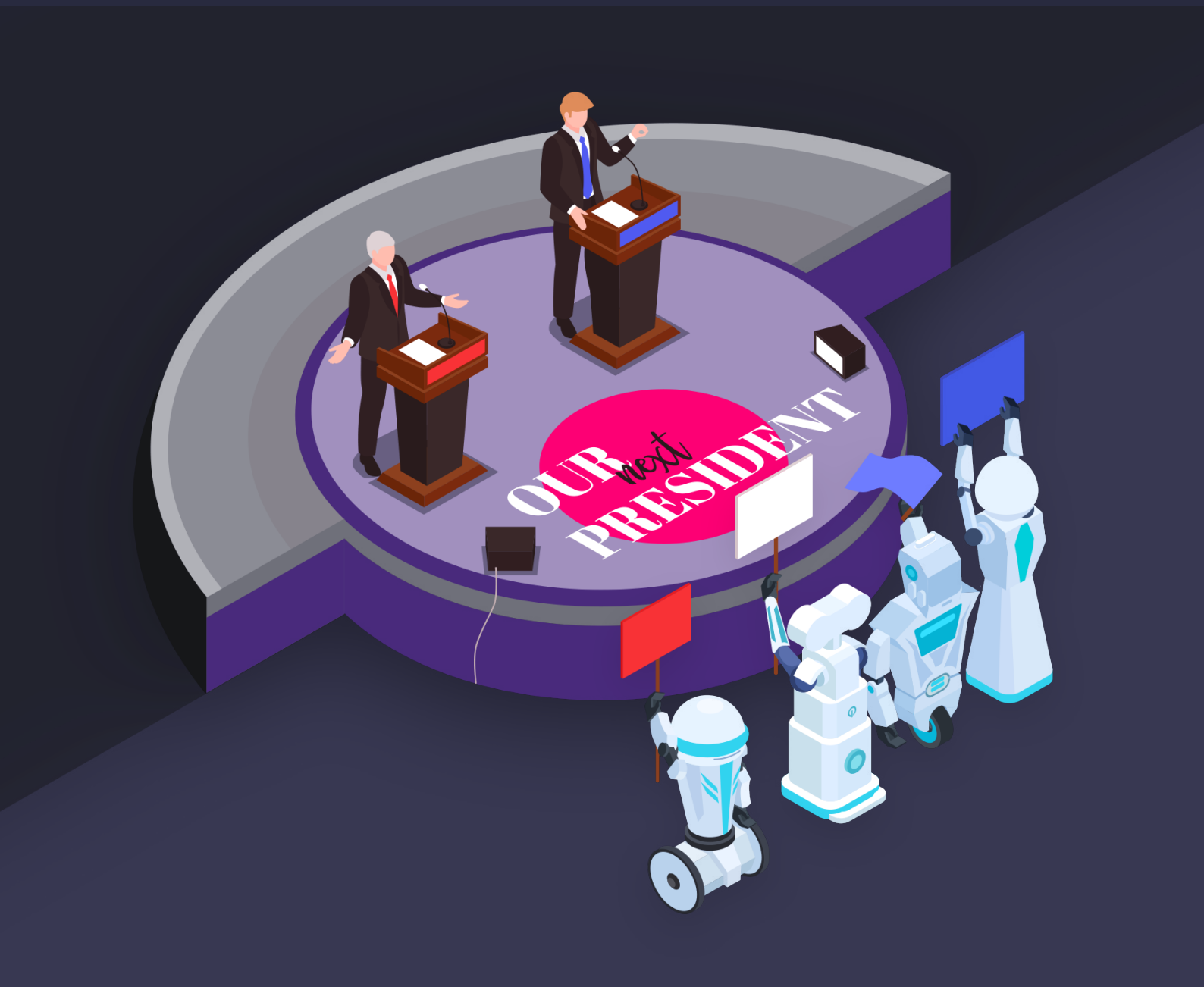
BOTS AND AD FRAUD IN THE US PRESIDENTIAL ELECTION 2020



UNIVERSITY OF BALTIMORE

CHEQ

INTRODUCTION

13% OF 2020 DIGITAL CAMPAIGN SPEND SET TO BE HIJACKED BY AD FRAUD

In this report, we show that 13% of US digital campaign spend will be lost to ad fraud. The high levels of ad fraud mean in effect that millions of digital political messages aimed at voters are being consumed by bots (that cannot vote). This will see at least $377 million of digital campaign spend lost to ad fraud in the 2020 Presidential election.

This report sets out the challenge of ad fraud in the 2020 Presidential election, using the latest economic analysis, data from campaigns, and interviews with campaign experts.

THE RISE OF US DIGITAL CAMPAIGN SPENDING REACHES $2.9 BILLION IN 2020

The motivation for fraudsters to use bots to hijack digital campaign spending comes as online campaigns reaches record levels. In short, fraudsters follow the money. Spend on digital ads in the US election will reach a record level in 2020, estimated between $1.3 billion and $2.9 billion[1]. This is up from $0.4 billion in the 2016 election. It marks the continuing rise of digital as central to US political campaigns, since President Obama's campaign manager, David Plouffe heralded digital as the deciding factor in the election 12 years ago.

The impact of digital advertising is decisive. It has been demonstrated that 65% of U.S. adults turn to digital channels to gather information about the election. Political science has shown that political advertising, whether conveying emotional or information content, contributes to "more informed, more engaged, and more participatory citizenry."[2] Moreover, "exposure to campaign advertising produces citizens who are more interested in the election, have more to say about the candidates, are more familiar with who is running, and ultimately are more likely to vote."[3]

[1] Borrell Associates Inc., a consulting firm, cited in https://www.wsj.com/articles/as-political-ad-spending-balloons-online-consensus-on-regulation-is-elusive-11573813803

[2] American Journal of Political Science, Vol. 48, No. 4, October 2004, Pp. 723–741

[3] Ibid.

THE IMPACT OF AD FRAUD

BOTS HIJACKING DIGITAL AD SPEND

However, this campaign spending is increasingly being targeted by ad fraud. Ad fraud is the practice of fraudulently representing online advertising impressions, clicks, conversion or data events in order to generate revenue. Money spent reaching bots rather than voters can damage the fabric and potentially the outcome of the election. The impact on digital ad spend has grown as ad fraudsters have become more sophisticated. For the majority of fraudsters, the automation tools used to commit fraud are evolving without them having to do anything about it – fraudsters just have to hide and rewrite certain elements in order to evade more and more tests.

Bot-makers create millions of headless browsers, that can simulate all human-like actions such as mouse movement, page scrolling, and clicks, to load webpages and cause ad impressions, that appear entirely human. In many campaigns analyzed across CHEQ we see 789 bots return 1323 times to click on ads. This is not uncommon. Today, malicious SDKs for advanced and AI-powered click injection are sold in the Dark Web on sale to the public for a fairly low price to perpetrate ad fraud, offering the opportunity in the words of the suppliers to "emulate ad clicks and hijack clicks including Google, Facebook and organic clicks."

ONE IN FIVE INVALID CLICKS NOT FROM US VOTERS

In addition, one in five click fraud cases involve VPNs or proxies – disguising the fact that the user clicking on a campaign ad is actually located in countries other than the US – and therefore almost certainly not eligible to vote. These readily accessible tools involve creating a unique new IP address every time the VPN is activated. Using the VPN and the new IP address, fraudsters choose how your location is presented online. For instance, Indian users may use a VPN to show their location as the USA.

REFUNDS FOR INVALID CLICKS

Even when refunds are provided by digital platforms, damage is done to the performance and strategy of campaigns. Laura Edelson, of the NYU Tandon Online Transparency Project has been monitoring the 2020 US election spend. Her team at NYU often see in transparency reports on political digital ad spend by platforms that suggests a regular refunding of money by platforms to digital political campaigns due to invalid clicks.

"Campaign spend is known to only go up over time, but we have seen 450 daily drops of more than a $1000 in spend back to campaigns. The only thing we can attribute it to is the refund due to invalid clicks. Ad fraud makes the spend calculations very difficult." Even if refunds do not see campaigns out of pocket (as platforms are refunding invalid clicks that have been served to bots) it nevertheless this diminishes the impact of targeting and planned activity that campaigns cannot get back.

$377 MILLION LOSSES DUE TO AD FRAUD

Based on data gathered and campaign insiders we conservatively place the ad fraud levels of digital campaign spend in the US election at 13%. This is higher than the average for other sectors were ad fraud accounts for an average of 10.5% digital spend. This equates to $377 million lost from the $2.9 billion in total digital spend in the US Presidential election. The reasons for the higher susceptibility of digital political campaigns to sophisticated ad fraud are set out below.

FAST SPEND: LESS ACCOUNTABILITY

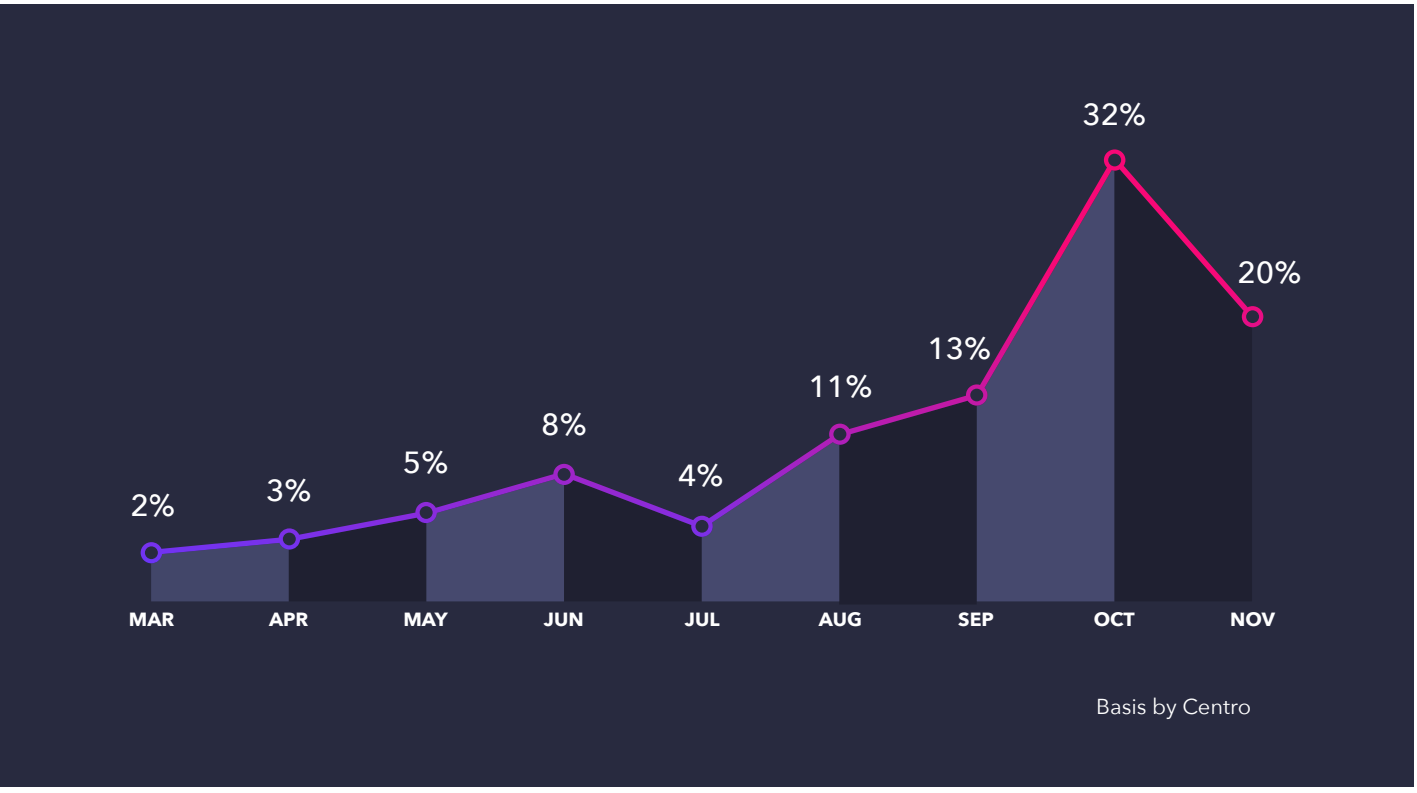
Higher ad fraud rates arise due to an issue – almost entirely unique in political races – the need to spend within the fixed deadline (of the election date). In the words of Cam Cameron, digital political consultant at Strategic Partners & Media: "How effective your campaign has been, comes down to the result you wake up to on November 4".

This fast and potentially loose spending can harm accountability and see spend wasted on bots, rather than voters. Zach Edwards, who worked on the online digital campaigns for President Obama and Mayor Bloomberg, says: "There is no ad fraud department in most of these buying teams that can be spending "$30,000 to 50,000 a day".

Large digital spend is often required at the last minute to bring out the vote, making checks and balances less likely. In general, 56% of Google political spend occurs in the last month of the election race.[4] Spend is even more free flowing in the last stretch, with 21% of ad dollars pumped out in the final 10 days.[5]

Edwards adds: "In a business ad buy you have an ROI, you have people checking it for months afterwards, and if it didn't pan out you may ask for a refund, whereas in political buying the only day that matters is election day. So, **you are spending money as fast as you possibly can**. Because the political campaigns are so short, there is no accountability for ad fraud. But because the campaigns dissolve, no one ever checks that, and no-one ever asks for refunds."

TIMING OF 2018 POLITICAL AD SPEND



[4] Tech For Campaigns Political Digital Advertising report (2019) based on an analysis of 57 political campaigns in 2018.

[5] Centro data: Will 2018 U.S. Mid-Term Ad Tech MVPs Deliver in 2020 Politics?

LACK OF TRANSPARENCY

The need to spend is coupled with the fact that online digital advertising is noted for its lack of transparency. Tech For Campaigns which analyzed digital ad spend across 57 US political campaigns in 2018: "While much has been made of digital media's role in political persuasion over the course of running different analyses, our understanding that the entire political space is wrought with severe data transparency issues has been reinforced".[6] Online advertising is an ecosystem in which the situation and interests of more than 20 parties are not aligned, and there is little to disincentivize fraudsters.
Indeed in 2020, the ISBA and PwC in a study, involving brands including HSBC, Walt Disney, and Unilever (each with 300 distinct supply chains), found that 15% of advertiser spend is completely unattributable, creating a markedly opaque supply chain.[7] This is even more pronounced in digital political campaigns. Tara McGowan CEO of the liberal nonprofit group Acronym said that campaigns are "working against the tide of bad actors to reach voters with the facts."

DIMINISHED INVENTORY FOR LATE CAMPAIGN SPENDING

With large spending occurring at the end of campaigns, strategists will find a diminished portion of "legitimate digital inventory" - exacerbating the conditions for ad fraud to thrive. Due to concerns over misinformation (bot traffic manipulating online political conversations) almost all of the main digital advertising platforms have imposed some limits on political ad buys in 2020. The lack of available inventory opens the door for less effective or fraud-filled spend. For example, Adobe, a large player in facilitating online ad buying. In August 2020, Adobe prohibited clients from purchasing political advertisements, such as those featuring a candidate or political issue, on its Advertising Cloud product. They joined Twitter, Spotify and Pinterest who announced similar measures. As a result, campaign cash has been diverted to programmatic display ad spend – which is more susceptible to fraud. Rates of fraud can reach up to 30% in display. In a GOTV push (Get out the vote campaign) at least 70% of digital political spend is programmatic.

Cameron says: "There is definitely a too good to be true feeling when I am being pitched by new partners, new websites where they are coming at me telling me they are getting so much traffic - a local news blog will come at you and I will do the math on their area and it does not make sense. They want to look like they have the most traffic possible so they can look like they have the highest CPM or flat rate. A lot of times I have had these conversations with my clients because newspapers will call up the guy running for Congress and they will say I can get you this really great CPM at a great price. They will send a screenshot of Google Analytics showing this traffic, but I have a lot of questions to ask them, starting with, 'How can you prove you do not have bots and that is not a large proportion of your views or clicks?'"
However, the announcements by Google and Facebook further limiting certain political ad spend further diminishes destinations for ad spend, creating more opportunies for ad fraud.

[6] Tech For Campaigns Political Digital Advertising report (2019)

[7] ISBA/PWC Programmatic Supply Chain Transparency Study (2020)

AD FRAUD-PRONE TRAFFIC RISES

Decisions by Google and Facebook, considered relatively safe ad buys, has allowed more ad fraud-prone traffic to take center stage. Firstly, Google, which overall represents 18.2% of political digital spend, announced the limiting of re-marketing ads for political campaigns. This occurs for instance when someone visits a site – perhaps half-filling a donation form, and then gets "retargeted" to be convinced to return to the site. Lindsay Jacobs, executive director of Majority Money, and an expert in political fundraising, says: "We then can't go after them to recapture that information and hopefully persuade them and take them through the whole acquisition phase — that's going to be where we see the biggest changes". Republican digital consultant Carter Kidd also noted how persuasion ads will suffer: "You can come up with a lot of ways to work around it for acquisition when you're looking for new email

Facebook, which accounts for 59% of digital political spend, has been a major success for campaigns. The platform's reach, targeting capabilities and ease of use and has been a powerhouse in raising money in the early stages of campaigns. However, Facebook announced limits on any new political adverts 10 days before the election. As has been seen, this is a significant challenge for campaigns which tend to spend biggest at this final stage. Cameron argues that many second-choice options to persuade voters – such as mail programs (still vital in US elections) cannot be turned around in 10 days, while there is a constantly limited inventory of television buys. This leaves the path open for free flowing spend on less accountable channels by the endgame.
For instance, in races such as Georgia, North Carolina, Ohio, Michigan, Minnesota, where Trump and Biden are going head to head, it remains challenging to buy television because of limited inventory.

OTHER TYPES OF AD FRAUD IN DIGITAL POLITICAL ADVERTISING

OTT/STREAMING SPEND

Promising new channels of digital political spend is hijacked by sophisticated fraudsters. Over the top (OTT) inventory digital-video ads have been used by political campaigns to connect with the nation's cord-cutters. Political-ad buyers often use streaming services and devices' personalization capabilities to target voters based on household income, education level, number of children or veteran status. The Washington Post (February 2020 showed that all candidates including Donald Trump spent to advertise on Hulu, Roku and other streaming services . Hulu's Brooklyn Nine-Nine opened with a 30-second spot from President Trump for instance to reach these targeted viewers, while earlier Sen. Elizabeth Warren (D-Mass.) spent at least $326,000 on political ads on Hulu between Nov. 1 and Dec. 31.

However, the emergent OTT option faces specific challenges with ad fraud. Fraud rates on OTT inventory stand at 17%, according to almost all estimates. Several OTT ad fraud cases has been discovered in 2020. Joe Barone, managing partner for brand safety in the Americas at GroupM, the world's largest media investment company responsible for more than $50B in annual media investment, said of the rise of OTT ad fraud: "Right now, we're looking at a big bucket of invalid traffic. It's not just fraud. There's content that's emanating from outside of U.S., redirects to user-generated content, and straight fraud like spoofing. … There are a number of different things adding up to [problems] we don't want to

COMPETITOR CLICKS

Perhaps the least sophisticated type of attack, competitor click fraud is nonetheless frighteningly effective. This involves opposition campaigns clicking on ads of their competitors to drain ad spend. With pay per click on political keywords costing up to $10 per keyword, this sneaky ad fraud prevents ads from being seen by the intended electorate. This is despite such click fraud being illegal violating the federal Computer Fraud and Abuse Act (CFAA). Under this law, you can go to prison for up to 10 years. Such competitor click fraud has seen a rapid increase during COVID-19 particularly in white collar sectors such as real estate and law firms. Click fraud is perpetrated to deplete advertisers' budget in an attempt to remove the ad from the search engine results, and damage digital campaign data.

CONCLUSION

The challenge of ad fraud represents a threat to political campaigns, seeing their digital ad strategies manipulated by bad actors. In the US election, 13% of ad messages will reach bots rather than real voters costing campaigns $377 million. In comparison to social media misinformation campaigns, ad fraud is a more agnostic crime, but neverthless essentially part of the same core playbook used by bad actors.

Bots don't vote, however large sums of campaign spending in 2020 will be spent in reaching them, rather than real voters. In reality, few campaigns think about carrying out post-mortems in digital spend after a campaign. However seeking answers on whether campaigns reached voters, or bots, represents a crucial analysis to ensure greater efficiency in future political races.