

**Federal Election Commission
11 SFR Part 110 [Notice 2012-12]
Internet Communication Disclaimers; Reopening of
Comment Period**

Comments by Spot-On

Spot-On is responding to the Federal Election Commission's request for comment appearing in the Federal Register Volume 82, No. 194 on October 10, 2017.

Based in San Francisco, CA, Spot-On is a cloud-based ad buying service specializing in political and advocacy efforts. Our firm has been in business since 2008. We specialize in buying directly from media outlets with an emphasis on high impact visually 'rich' media placements on well-read local news outlets.

We also have extensive experience buying and placing ads on multiple platforms: audio, video, mobile and desktop. We maintain strong business relationships with most popular vendors and third-party resellers and buying platforms. Our customers run the gamut of those involved in political speech at all levels of political activity: Local, state, regional and federal.

Like many American companies, we are extremely concerned about the online activity that occurred during last year's election. We write today to share our experience in this market with some suggestions for what we believe will be an improved, less fraud-ridden playing field.

The open and easy communications access provided by the Internet opened a door to 2016 election interference by non-U.S. residents and foreign governments. It's clear to us that the dangers to our democratic process highlighted by this shadowy behavior aren't limited to interference by foreign governments or actors. Under the current system, interference by a campaign opponent or interested third party, using the tactics and strategies deployed in

2016 is entirely possible, even likely without better oversight over election advertising.

Our overriding concern is that individual online platforms – those that do business directly with the public and those that provide services for businesses – will enact their own rules and regulations for political speech without regard for traditional standard and practices that most political actors rely on in the “analog” or “real” world. Just to give on recent, high profile example: President Trump’s Twitter account was suspended by a disgruntled employee. Imagine if that person – on his own or at the suggestion of a political rival – decided to make similar decisions about ad placement, distribution or rating.

We concur with the sentiments expressed by members of Congress last week when they asked three of the largest ‘platforms’ about their lack of involvement or even responsibility in deciding what is said on their online real estate. The use of the word ‘platform’ as a way to avoid responsibility for material that appears on a website or page strikes us as a convenient way to shrug off what has been the historic responsibility of companies that are in the business of facilitating public discourse, namely newspapers, radio and television stations.

The issue in front of the commission is not just a question of disclosure. It will not be solved by requirements that more information kept by “public-facing” platforms with large audiences. Or by corporate-imposed ‘icons’ or badges. With multiple paths and platforms available to all ad buyers – including many that do not do business directly with consumers – Spot-On sees the best solutions as those that call on campaigns and the intermediaries that dominate the political ad buying world to be as transparent as they are with radio and TV buying. The technology that allows campaigns to reach voters easily and effectively can simultaneously provide effective and easily accomplished reporting and review.

We would not suggest that our clients take on more recordkeeping. However, given the borderless nature of the

Internet, Internet-based platforms and news outlets, we believe that U.S. entities should keep records for U.S. voters. It is not certain that American companies or individuals will always manage or own controlling interests in online communication pathways. We think that giving campaigns and candidates responsibility for these disclosures now, as these issues are coming to the forefront of our understanding of the nexus of elections and digital communication, provide the clearest way forward.

How Online Ads are Bought

To fully appreciate the online political ad environment and how to best solve the problems of attribution, disclosure and transparency, it's necessary to take a few minutes to understand the overall ad buying environment. It's a mess.

We begin with an understatement: Automated or 'programmatic' ad buying is fraud-ridden. To expect these companies - buying and selling exchanges - to police themselves for political advertising is foolhardy. Consider these following two, highest profile examples.

- A group of hackers known as "Methbot" stole an estimated \$5 billion a day in ad revenue in the fall of 2016. It was either ignored or, worse, unnoticed by many resellers and buying platforms ([New York Times Dec. 20, 2016](#)).

- Both Procter and Gamble and Chase Bank have reduced their 'programmatic' (automated) ad buying and seen no visible change in their marketing results ([WSJ, July 27, 2017](#) and [New York Times, March 29, 2017](#)).

And almost all political ad buying flows through these the third party ad buying platforms, without any review for accuracy or legally required disclosures.

Most of these bidding platforms do not enforce the law because few know or care about it. They frequently apply arbitrary and

confusing ‘standards’ for what they believe is the good of their readers and viewers – in other words, their business and their brand comes first. These actions – in absence of clear rules – can amount to a chilling effect on free speech.

Last year, our firm was told a client’s ads had been reviewed by an ad platform audit team in India – a standard practice – and, as result, had been labeled ‘negative’. The ads weren’t reviewed for disclaimers; we weren’t asked if the charges were true or if we had substantiation – questions we would have had to answer for a TV or radio placement – our clients’ speech was seen as negative by someone living in a foreign country and marked accordingly. Until Spot-On repeatedly questioned why the ads we purchased weren’t running as we anticipated, we didn’t know about this characterization. Our client’s speech was labeled before it had a chance to reach voters by non-U.S. citizens in a country with very different laws about political speech and libel.

Placing ads directly with more easily identifiable outlets – the publishers Spot-On deals with regularly – is still confusing. Spot-On has been asked to insert disclosures for Congressional races that apply to state elections. We are told that advocacy efforts addressing federal level office-holders are subject to FEC rules governing election campaigns. One platform uses the disclosure requirements that apply in its home state elections for all states and all races where they do business. None of this is accurate or required by law and it’s both confusing and chilling to have wildly different – and sometimes arbitrarily enforced rules – for political advertising.

While Spot-On understands and appreciates that the commission can only set rules for federal elections, our firm feels strongly that statements and guidance issued by the FEC would go a long way to making it clear what sort of disclosures and disclaimers are acceptable at all levels of political discourse.

Spot-On's Experience in California

As a California-based company, Spot-On has had to comply with state law in regard to digital advertising for almost 10 years. We have found that the regulations the state's Fair Political Practices Commission have put in place to be effective and not terribly intrusive. As such we're including some observations that we think maybe helpful to the commission because they have flavored our observations and the recommendations below.

All ads appearing in California for state races must carry a "Paid for by [candidate or committee]" disclaimer for audio, video, static and animated banners.

These disclaimers, as written by campaign attorneys, can become unduly cumbersome. Spot-On would prefer shorter disclaimers - a simply line suffices - alerting viewers to the ads' purpose and pretty much saying "political ad" to any reasonable viewer or user.

Unlike mail, TV or outdoor advertising, the online experience is multi-dimensional; all online ads link to a website. Viewers can know more with a click regardless of the ad format they're looking at - mobile or desktop video, audio or banner ads - doing away with the need for a one-shot, lengthy disclosures.

If the commission's preference is for longer, fuller disclaimers - which we don't believe are necessary - a technological solution is easily available. Ads can be constructed so that a 'mouse over' insert that appears as a viewer touches or 'mouses over' an ad. The lengthy disclaimer can appear then disappear to display the full ad.

California permits third-party entities - independent expenditure committees - to link to candidate sites. If the FEC were to promulgate a similar rule - and we think it's acceptable - a technological solution for disclosure is also at hand. Ads that endorse or support a candidate or cause should be 'mapped' so that a section for the ads carrying the brief "paid for...." disclaimer clicks through to a site with more information about the endorsing

entity. The bulk of the ad clicks through to the candidate or cause being promoted. This solution is also easily incorporated as the ads are created.

California campaigns are also required to list sub-vendors with FPPC on a regular basis. For example, if Spot-On were to spend \$100,000 on LATimes.com, our client would report that activity to the FPPC. We think this rule can be applied more universally. Having said that, we have strong objections to the haphazard way the law is currently enforced.

Campaigns that buy ads from third party bidding platforms are able to simply list the name of that firm as their sub-vendor. Unlike direct buyers - Spot-On - they do not have to list the actual websites where their ads appeared. These sub-vendors are the same third parties described above, the ones who are lax about enforcement and placements with reviews conducted - if they're conducted at all - in foreign countries. And make no mistake, these platforms are wildly popular with political resellers because they provide targeting and data management services as well as one-stop ad buying. Spot-On must list individual publishers as sub-vendors when it places ads for candidates and causes. We think the ad platforms and their reselling partners should be required to list specific websites where political ads run just as we are.

Given our experience with ad buying and selling platforms, Spot-On is reluctant to join a movement to label political advertising with special "icons" or badges. We think this could easily create a 21st Century Scarlet Letter for political speech, encouraging publishers to shunt political ads aside to less visible position or to reject them out-of-hand. Furthermore, it seems that the political "icon" would be appended by the same faceless entities currently rating the political advertising we send through various exchanges. It's easy for Spot-On to see how this marking could be deliberately misused to flag advertising or speech that the initial reviewer finds objectionable or injurious to his or her political point-of-view or favored candidate.

U.S. politics is moving to a world where non-public facing entities – perhaps entities owned by residents of other nations – have a powerful impact on where ads appear online. It is incumbent on the FEC to determine how these entities should produce reports and manage ad traffic. This is not chilling free speech. On the contrary, we have seen that the open, free-for-all nature of online ad buying can create an environment where speech is derailed by faceless, nameless operators which poorly defined – even nefarious – interests. More troubling, this behavior is rewarded since it allows campaigns to cloak their activity.

The current ‘black box’ approach using a fraud-ridden and poorly policed system also wastes campaigns’ money on ads that aren’t seen and don’t reach voters. As an additional protection, the commission might consider asking the resellers who deploy these services for political campaigns to supply the locations where the ads ran either by latitude/longitude for mobile and some social media applications, zip code or I/P address for desktop and mobile devices. This would give a clear picture of what ads are running, where they’re running and what their intended impact and target.

Recommendations

As a result of our experience, Spot-On proposes that the FEC consider five concrete actions:

- Promulgate and enforce ‘know your customer’ rules similar to the due diligence that financial institutions have to protect themselves from allegations of fraud and illicit behavior for ad buying and selling platforms taking election-related political ads.
 - o These rules should be used by all online outlets - consumer- and voter-facing platforms as well as third part ad resellers who do not deal directly with the public – and should, at a minimum include a physical location for the campaign and links to appropriate information filed at the FEC or state agencies

regarding campaign registration and/or funding to assure legitimacy.

- Set rules for minimal disclosures on ads and require those ads to link to campaign websites.
- Require third-party bidding and buying platforms to provide a list of sites where political ads have appeared and the physical targets for the ads.
 - o Disclosure could also include information about the campaign's use of targeting, in much the same way that the EU requires a "cookie" disclaimer on websites operating in Europe.
- Set rules for website disclosure, life expectancy and search optimization for candidate and campaign websites so that election records are easy to find and review – even after the election.
 - o Information listed should include the "know your customer" requirements listed above as defined by the commission. And since all ads link to some sort of web page or presence, this would do away with arguments about 'size' of ads and disclaimer length.
- Critical ads should be required to link to webpages providing substantiation, much like that demanded by TV and radio. Those sites should provide "know your customer" information as described above.

Looking At Future Elections

As new platforms and services arise and set their own rules about allowable speech, the troubling problems outlined here in Spot-On's comments will continue to plague the political ad environment – at all levels. It is inevitable that these problems will spill over into editorial speech. The over-arching question before the commission today isn't just about disclosure, which only covers the material on an ad. It's about how political communication will

be handled by each platform as we move into a world where a faceless third-party entity, potentially located outside the U.S., can decide what readers, viewers and listeners learn about American elections and campaigns.

With careful action, the FEC can send a clear signal that transparency and disclosure are necessary for credible participants and that people who want to speak freely should and can make their actions clear. It can establish a set of benchmarks to help online outlets set standards and practices for political ad placements to help focus and define our national ideas about credibility. These actions would enhance voters' ability to understand the messages and the sources of various online claims and counter-claims without being burdensome or inhibiting free speech.

We have appended four documents to this submission: three copies of the news stories referenced above about ad fraud and a copy of our Best Practices White Paper which we use to orient customers to the online environment.

Thank you for your time and attention. Spot-On is happy to respond to any detailed questions members of the commission may have. Please contact us at your convenience.

Chris Nolan
Founder/CEO
Spot-On
350 Townsend Street
Suite 302
San Francisco CA 94109

cnolan@spot-on.com
415-771-7133

TECHNOLOGY

Russian Cyberforgers Steal Millions a Day With Fake Sites

By VINDU GOEL DEC. 20, 2016

SAN FRANCISCO — In a twist on the peddling of fake news to real people, researchers say a Russian cyberforgery ring has created more than half a million fake internet users and 250,000 fake websites to trick advertisers into collectively paying as much as \$5 million a day for video ads that are never watched.

The fraud, which began in September and is still going on, represents a new level of sophistication among criminals who seek to profit by using bots — computer programs that pretend to be people — to cheat advertisers.

“We think that nothing has approached this operation in terms of profitability,” said Michael Tiffany, a founder and the chief executive of White Ops, the ad-focused computer security firm that publicly disclosed the fraud in a report on Tuesday. “Our adversaries are bringing whole new levels of innovation to ad fraud.”

The thieves impersonated more than 6,100 news and content publishers, stealing advertising revenue that marketers intended to run on those sites, White Ops said.

The scheme exploited known flaws in the system of digital advertising, including the lack of a consistent, reliable method for tracking ads and ensuring

that they are shown to the promised audience.

The spoofed outlets include a who's who of the web: video-laden sites like Fox News and CBS Sports, large news organizations like The New York Times and The Wall Street Journal, major content platforms like Facebook and Yahoo, and niche sites like Allrecipes.com and AccuWeather. Although the main targets were in the United States, news organizations in other countries were also affected.

“It will be a big shock to all of these publishers that someone was selling inventory supposedly on their sites,” Mr. Tiffany said in an interview on Monday, before the report's release. White Ops and an advertising industry organization, the Trustworthy Accountability Group, held a conference call with about 170 advertisers, ad networks and content publishers on Tuesday morning to brief them on their findings.

Mr. Tiffany said White Ops had traced the fraud to Russia and believed that the organization behind it was a criminal enterprise out to make money. There was no evidence of a connection between the fraud and the politically motivated hacking during the United States election that American intelligence agencies and President Obama have linked to the Russian government.

The Methbot scheme — named after the word “meth,” which shows up in its software code — was carefully designed to evade the antifraud mechanisms the advertising industry has put in place in recent years. Digital ad fraud was projected to cost marketers more than \$7 billion in 2016, according to a study by the Association of National Advertisers and White Ops.

To carry out the operation:

The Methbot forgers first took numeric internet addresses they controlled and falsely registered them in the names of well-known internet service providers.

Among those were Comcast, AT&T and Cox, as well as fake companies like AmOL. This allowed the thieves to make it look as if the web traffic from Methbot's servers in Dallas and Amsterdam were really coming from individual users of those internet providers.

The forgers then associated the addresses with 571,904 bots designed to mimic human web surfers.

Embedded in the bots' web browsers were fake geographic locations, a fake history of other sites visited and fake logins to social networks like Facebook. "The bots would start and stop video just like people do and move the mouse and click," Mr. Tiffany said.

The perpetrators connected the bots to the automated advertising networks that sell unsold ad space for thousands of websites.

A bot would pretend to visit a website like CNN.com, and the ad networks would conduct a microsecond bidding war against one another to show a brand's video ad. But instead of going to the real CNN, the bot's web browser would go to a fake site that nobody could see, and the ad would play there.

Finally, the system would report fake data to the ad networks and advertisers to convince them that humans had watched the ad on the real content site.

"It would send just the right kind of metrics back to look like real live audiences that were logged into Facebook and watching videos all day," Mr. Tiffany said. The thieves then collected payment for the ads.

The report did not name the advertisers tricked by the fraud.

David Hahn, the executive vice president of strategy at Integral Ad Science, an advertising security firm that competes with White Ops, said the Methbot fraud affected just a tiny portion of the ad traffic of his own clients.

"There are new bots and new ways in which the bad guys are trying to figure out ways around our technology all the time," he said.

The automated ad networks that buy and sell access to ad space on popular websites operate in a murky, fast-paced world, and it's often unclear to advertisers who such middlemen truly represent.

“As a buyer, how do you check that those other companies are authorized sellers of the ad inventory?” said Neal Richter, who until recently was the chief technology officer for Rubicon Project, a major exchange for automated ad sales. “You need to know who you’re doing business with.”

Trustworthy Accountability Group, which is a joint effort of the ad industry’s major trade groups, is already blacklisting the internet addresses used by Methbot’s bots, adding them to a master list used by many in the industry to screen out fraud.

Mike Zaneis, the chief executive of the organization, said his group began a certification program last week to verify that ad exchanges truly represent the buyers and sellers they are claiming to represent. Under the system, payment for an ad flows directly to the website publisher, which would make it more difficult for forgers like the Methbot crew to get paid for their deception.

Several news organizations whose websites were faked by Methbot, including The Times, said Tuesday they were still evaluating the fraud case.

White Ops said the thieves received high prices for the fake ad views, garnering an average price of \$13 per 1,000 video views. Over all, the botnet delivered 200 million to 300 million fake ad views per day and brought in \$3 million to \$5 million in daily revenue, according to the company’s analysis.

White Ops released the full list of fake internet addresses and impersonated websites so that fraud-detection services and ad networks can block them. The company has also shared its findings with United States law enforcement authorities and is working with them to further investigate the fraud.

Mr. Tiffany said the use of bots to steal ad revenue is not new in the industry, but it “has never happened at this scale before.”

He continued, “It all adds up to the most profitable bot operation we’ve ever seen.”

Sapna Maheshwari contributed reporting from New York.

A version of this article appears in print on December 21, 2016, on Page B1 of the New York edition with the headline: Selling Ads on Fake Sites, Russian Ring Steals Up to \$5 Million Daily.

whitelisting, this month after The New York Times showed it an ad for Chase's private client services on a site called Hillary 4 Prison. It was under a headline claiming that the actor Elijah Wood had revealed "the horrifying truth about the Satanic liberal perverts who run Hollywood."

Of the 400,000 web addresses JPMorgan's ads showed up on in a recent 30-day period, said Ms. Lemkau, only 12,000, or 3 percent, led to activity beyond an impression. An intern then manually clicked on each of those addresses to ensure that the websites were ones the company wanted to advertise on. About 7,000 of them were not, winnowing the group to 5,000. The shift has been easier to execute than expected, Ms. Lemkau said, even as some in the industry warned the company that it risked missing out on audience "reach" and efficiency.

JPMorgan had already decided last year to oversee its own programmatic buying operation, and it works with Google and AppNexus to show its ads, she said. It was not a difficult decision to extend whitelisting to YouTube, given that Chase was already making that shift across its display advertising, she said.

"Before the YouTube thing happened, we were just looking at programmatic," she said. "Now the question is, what else is out there that we should be looking at whitelisting?"

She added, "At some point, a human is going to take a look."

Follow Sapna Maheshwari on Twitter at @sapna.

A version of this article appears in print on March 30, 2017, on Page B1 of the New York edition with the headline: A Bank Had Ads on 400,000 Sites. Then Just 5,000. Same Results.

MEDIA

Chase Had Ads on 400,000 Sites. Then on Just 5,000. Same Results.

By SAPNA MAHESHWARI MARCH 29, 2017

As of a few weeks ago, advertisements for JPMorgan Chase were appearing on about 400,000 websites a month. It is the sort of eye-popping number that has become the norm these days for big companies that use automated tools to reach consumers online.

Now, as more and more brands find their ads popping up next to toxic content like fake news sites or offensive YouTube videos, JPMorgan has limited its display ads to about 5,000 websites it has preapproved, said Kristin Lemkau, the bank's chief marketing officer. Surprisingly, the company is seeing little change in the cost of impressions or the visibility of its ads on the internet, she said. An impression is generally counted each time an ad is shown.

The change illustrates the new skepticism with which major marketers are approaching online ad platforms and the automated technology placing their brands on millions of websites. In recent years, advertisers have increasingly shunned buying ads on individual sites in favor of cheaply targeting groups of people across the web based on their browsing habits, a process known as programmatic advertising — enabling, say, a Gerber ad to show up on a local mother's blog, or a purse in an online shopping cart to follow a person around the internet for weeks.

But as the risks around the far reaches of the web have been cast into stark relief, some advertisers are questioning the value of showing up on hundreds of thousands of unknown sites, and wondering whether millions of appearances actually translate into more sales.

“It’s only been a few days, but we haven’t seen any deterioration on our performance metrics,” Ms. Lemkau said in an interview on Tuesday. She added that the company had also pulled ads from YouTube in the past week after reports showed other major advertisers like Verizon unintentionally appearing on videos promoting hate speech and terrorism. JPMorgan aims to restrict its ads on the platform to a “human-checked” list of 1,000 YouTube channels, which it expects to be able to do by the week of April 10, she said.

Much of the promise of online advertising hinges on the vast reach of the web, and the ability to reach people on niche sites at low prices. Index Exchange, an ad exchange, has estimated that the titles owned by the top 50 traditional media companies account for 5 percent or fewer of the trillions of ad impressions available for sale each day. Google’s display network alone includes more than two million websites. YouTube has more than three million ad-supported channels, according to the analytics company OpenSlate, which says the average \$100,000 campaign on the platform runs on more than 7,000 channels.

If more advertisers follow JPMorgan’s lead and see similar results, it could hurt the operators of smaller sites that make up the so-called long tail of the internet, as well as the advertising technology companies that profit from funneling trillions of ad impressions from brands to consumers through systems that mimic a stock exchange, according to Eric Franchi, co-founder of the ad technology firm Undertone.

“If you charge a percentage of all of the ads that run through your platform, then the prospects can be pretty dim if all of a sudden your volume has been cut by 95 percent,” Mr. Franchi said. “So many of these companies, and some of them are public, tout the number of ads they deliver per second, per day. If you start seeing more marketers move in this direction, it will be pretty interesting. What are the metrics then that those companies start to report?”

JPMorgan started looking into preapproving sites, a strategy known as

whitelisting, this month after The New York Times showed it an ad for Chase’s private client services on a site called Hillary 4 Prison. It was under a headline claiming that the actor Elijah Wood had revealed “the horrifying truth about the Satanic liberal perverts who run Hollywood.”

Of the 400,000 web addresses JPMorgan’s ads showed up on in a recent 30-day period, said Ms. Lemkau, only 12,000, or 3 percent, led to activity beyond an impression. An intern then manually clicked on each of those addresses to ensure that the websites were ones the company wanted to advertise on. About 7,000 of them were not, winnowing the group to 5,000. The shift has been easier to execute than expected, Ms. Lemkau said, even as some in the industry warned the company that it risked missing out on audience “reach” and efficiency.

JPMorgan had already decided last year to oversee its own programmatic buying operation, and it works with Google and AppNexus to show its ads, she said. It was not a difficult decision to extend whitelisting to YouTube, given that Chase was already making that shift across its display advertising, she said.

“Before the YouTube thing happened, we were just looking at programmatic,” she said. “Now the question is, what else is out there that we should be looking at whitelisting?”

She added, “At some point, a human is going to take a look.”

Follow Sapna Maheshwari on Twitter at @sapna.

A version of this article appears in print on March 30, 2017, on Page B1 of the New York edition with the headline: A Bank Had Ads on 400,000 Sites. Then Just 5,000. Same Results.

THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<https://www.wsj.com/articles/p-g-cuts-more-than-100-million-in-largely-ineffective-digital-ads-1501191104>

BUSINESS | MEDIA & MARKETING | CMO

P&G Cuts More Than \$100 Million in ‘Largely Ineffective’ Digital Ads

Consumer product giant steers clear of ‘bot’ traffic and objectionable content



P&G owns consumer brands, including Bounty, Crest, Tide and Pampers. PHOTO: REUTERS

By Alexandra Bruell and Sharon Terlep

July 27, 2017 5:31 p.m. ET

Procter & Gamble Co. [PG 0.64% ▲](#) said that its move to cut more than \$100 million in digital marketing spend in the June quarter had little impact on its business, proving that those digital ads were largely ineffective.

Almost all of the consumer product giant’s advertising cuts in the period came from digital, finance chief Jon Moeller said on its earnings call Thursday. The company targeted ads that could wind up on sites with fake traffic from software known as “bots,” or those with objectionable content.

“What it reflected was a choice to cut spending from a digital standpoint where it was ineffective, where either we were serving bots as opposed to human beings or where the placement of ads was not facilitating the equity of our brands,” he said.

Chief Executive David Taylor said in an interview that the digital spending cuts are part of a bigger push by the company to more quickly halt spending on items -- from ad campaigns to product development programs -- that aren’t working.

“We got some data that said either it was in a bad place or it was not effective,” Mr. Taylor said of the digital cuts. “And we shut it down and said, ‘We’re not going to follow a formula of how much you spend or share of voice. We want every dollar to add value for the consumer or add value for our stakeholders.’”

After cutting back on certain digital ads, “we didn’t see a reduction in the growth rate,” said Mr. Moeller during the call. “What that tells me is that the spending we cut was largely ineffective.”

P&G also said it reduced overhead, agency fee and ad-production costs in the quarter.

P&G, whose brands include Bounty, Crest, Tide and Pampers, spent \$2.45 billion on U.S. advertising, not including spending on some digital platforms, according to Kantar Media. Long the biggest advertiser in the world, its pronouncements on trends in ad spending are watched closely.

The company about a year ago said that it would move away from ads on Facebook that target specific consumers, after finding that ultra-niche targeting compromises reach and has limited effectiveness. P&G indicated it wouldn't pull back on overall Facebook spending.

It's unclear whether P&G has shifted more spending to other media, including television, as it tweaks its digital spending approach. TV networks have been making an aggressive case that marketers have over-allocated budgets to the dark alleys of digital, and should move ad money back into TV.

The cuts echo marketing executives' mounting concerns around the efficacy of digital advertising and the growing perception that they are wasting money on digital ads that never reach their intended audience.

P&G, which is facing a proxy fight with activist investor Nelson Peltz, reported 2% increase in organic revenue in the quarter and full year ended June 30. The company posted a higher profit in the most recent quarter despite a slump in consumer spending.

Mr. Peltz's Trian Fund Management LP criticized P&G's cutback on digital spending. P&G's improved earnings "came as a result of reducing advertising, specifically digital, a tactic we believe will damage the value of the company's brands if continued in the long term," the firm said in a statement.

It's unclear what impact the digital cuts have on P&G's overall marketing spend.

P&G said it's committed to advertising that delivers tangible results for its brands.

Personal care brand Always, for example, saw "a significant increase" in awareness and equity scores since its "Like a Girl" campaign launched a few years ago, said Mr. Taylor on the call. The campaign shed a light on gender bias, challenging what it meant to do something "like a girl."

Mr. Taylor on the call talked about the importance of "having a superior product" that has "a point of view" as more consumers use social media to share their opinions.

Always is among the many brands that have taken on a larger social cause or purpose in their marketing in recent years.

P&G is among the packaged-goods giants tweaking their marketing spending and strategy as they face larger business challenges. Rival Unilever is also undergoing a marketing reorganization, including drastically cutting the number of agencies it works with.

Spending cuts are hurting the ad agencies that rely on business from the big consumer-goods spenders. Interpublic Group of Companies, which owns McCann Worldgroup and IPG Mediabrands, said during its latest earnings call this week that spending cuts by consumer packaged goods clients reduced its revenue in the second quarter by almost 1%.

SPOT-ON

POLITICAL ADS and ANALYTICS



The Modern Consultant's Guide to Online Political Advertising

Your 10-Step Roadmap for Navigating
a Changing Digital Environment

INTRODUCTION

2016: THE YEAR THAT CHANGED EVERYTHING

The 2016 election cycle delivered a harsh reality check across the entire political spectrum. President Trump's victory stunned many political consultants in both parties and changed many long-held ideas about digital advertising and political outreach. Some are saying the Trump victory validates the use of traditional outreach tools. Others say that digital is now more important than ever.

The market came down squarely on the side of digital outreach. Going into the 2016 election cycle, analysts estimated digital ad spending would eclipse \$1.5 billion in 2016. And, according to Borrell Associates, which has been measuring the political online ad market for more than 10 years, it did.

According to advertising research firm, Borrell Associates:

"Political was one ad category that remained stubbornly old-school when it came to how money was spent, with the vast majority of dollars going to TV for four solid decades. The 2016 presidential campaign proved, for the first time, that a candidate doesn't have to match or outspend an opponent in TV commercials -- or even in overall funds raised -- to win an election."

If that's true, then how did the digital advertising landscape change after this election?

While President Trump spent \$340 million less than Romney spent in 2012, the 2016 cycle still represented a new milestone for political advertising, topping just under \$10 billion.

For many digital shops, the bonanza did not translate into higher revenues - leading to some criticism of market estimates. However, a closer analysis shows that while the \$1.5 billion spend did materialize, a lion's share went to tech giants Facebook and Google. Both of those firms have multiple sales channels -- some of which can work around resellers.

The fall-out from the miscalculations made by many of these resellers - many of whom added little value to the large firms' initial product - will echo through this year as many close, consolidate or seek new business models.

Okay, so how should consultants and buyers plan their digital advertising strategies for the 2018 election cycle?

To help political consultants and media buyers plan ahead for the 2018 election cycle, Spot-On created this 10-step guide, which illuminates the road ahead and serves as a practical digital advertising framework. Our overriding advice: use this past election cycle as a healthy 'reality check' to reset your online advertising strategies for the years ahead.

BACKGROUND: What we learned. How it can help in 2018

During the two months immediately before the 2016 general election, Spot-On surveyed political ad buyers, campaign managers and media consultants from both parties. What emerged is a portrait of a market still adjusting to the use of digital and online technology.

Key findings from Spot-On's survey include:

- **Digital Spend is Growing.**

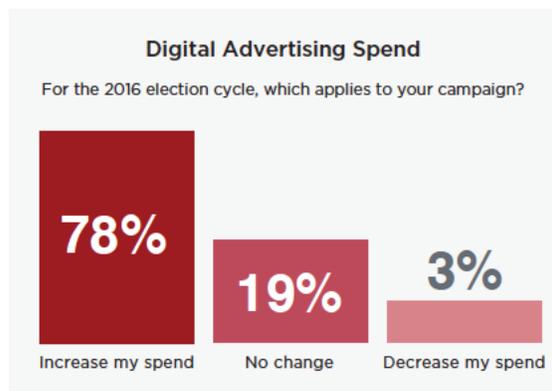
Regardless of their level of comfort with digital campaigning, 60 percent of those surveyed said that they maintained or increased their spending online in 2016. One in five said they were increasing budgets by 25 percent or more.

- **Young professionals use the digital space better.**

An overwhelming number – 93 percent – of consultants and campaign managers over 45 years of age described themselves as knowing “enough to be dangerous” or “novices.”

Younger professionals, 76 percent considered themselves as “dangerous” or “expert” in their use of digital technology.

While younger consultants and buyers are more enthusiastic about the use of online, we found that many are guided more by vendors they like and trust, rather than by technical savvy or familiarity.



- **Consultants use of media based on experience, not effectiveness.**

The use of technology also differed by age. The majority of younger respondents said digital advertising was better than TV or traditional media when it came to targeting voters. Older consultants were less inclined to rely on digital for reaching voters calling online efforts “an emerging channel.”

Targeting isn't the be-all and end-all of digital ad buying. While it's extremely useful for larger statewide or national campaigns, an over-reliance on targeting can lead to fraudulent ad placement.

- **Everyone thinks the other party's doing better. They're not.**

There was no difference across the political parties when it came to the use or deployment of digital advertising. Regardless of affiliation, those polled shared the same primary concerns about measuring the effectiveness of online campaigns. At the same time, these professionals struggle to understand the variety offerings available and how best to use them.

This confusion is across the board. And it's the main reason we've created this guide. Knowing what you're buying and what it's going to do for your campaigns is the first step in being savvy and well-informed customers.

Key findings from Spot-On's research include:

1. There is no "digital" silver bullet.

Over the past few years, every candidate, elected official and consultant has become enamored with a shiny new digital toy. In 2008 it was the "Google surge" where consultants thought they were buying "all of Google's inventory" on election day. Then came the race for "likes" on Facebook. In 2008 voter file matching came to the forefront.

The use of "big" data, analytics, automation and sophisticated segmentation, is real, yet it doesn't work at every campaign level.

As political consultants plan for 2018, they should not put all of their eggs into one "digital basket" or rely on one vendor to meet every online need. Before adopting any technology approach, consultants and candidates should first establish some tangible goals for their digital advertising program: Are you trying to boost awareness? Is your goal to build an accurate database of voters in your district? Are you targeting specific segments of the population? The answers to these questions are different for a Congressional race than they would be for a statewide ballot measure – regardless of budget.

No single solution exists that will meet the unique set of campaign requirements. With this understanding and a clear definition of goals, campaigns should leverage a mix of best of breed technologies, digital channels, data sources and best practices.

2. Digital will elbow into the linear TV landscape.

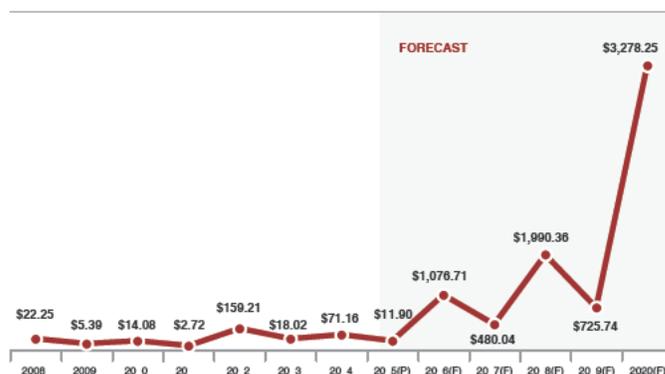
Targeting voters using programmatic ad buying platforms was an important driver of political ad spending during the 2016 cycle – with mixed results. The campaign that won the presidential race used its own – not 3rd party – data for its online targeting. And the campaign that lost used large databases drawn from years of party research and modeling.

According to Borrell Associates 2016 election post-mortem traditional broadcast TV spending fell nearly 20 percent this cycle compared with 2012, from \$5.45 billion to \$4.4 billion in 2016.

That said, television will remain an important channel – yet within a broader digital context. Specifically, video will be consumed cross-device (smartphones and other devices), including game consoles and traditional set-top boxes, all offering streaming services. This means all campaigns need a holistic strategy.

This is important as voters age. Younger voters will continue to push new online platforms (with Snapchat being eyed as the next shiny thing). Those younger voters aren't considered politically reliable and in 2016 many stayed home. But consider this: A first time voter in 2008 is now 26 and will be 30 for the next presidential election. That voter will be more familiar with streaming services than traditional TV 'stations.'

U.S. TOTAL ONLINE/ DIGITAL POLITICAL AD SPENDING, IN \$ MILLIONS, 2008-2020



Source: Borrell Associates, "2015 to 2016 Political Advertising Outlook"

3. Mobile technology and its promise.

In a multi-screen world, content is consumed on demand, everywhere and anywhere. The impact and visuals from digital video offers tremendous opportunities to the candidate or cause. In fact, video advertising garners much higher engagement rates compared to traditional display ads.

Mobile video has some challenges – several vendors want the aspect ratio for a vertical phone, not a horizontal TV set, and viewer engagement can vary wildly. A YouTube viewer will tolerate longer ads; those seeing ads in mobile apps want placements than can be easily skipped.

Mobile has also offered the opportunity to tightly target – or "geo-fence" ad placements. This can be a handy GOTV tool for polling places and other gatherings. But, as with many nascent technologies, the ability to directly reach individuals is over-sold and often over-promised. It can also raise the cost of ad placement and can diminish the "social pressure" aspect of an out-reach effort.

Also, let's be clear. We all know phones are mobile devices -- but so are iPads and tablets!

4. Design everything for the cross-connected viewer.

According to the Pew Research Center, 66 percent of voters are now viewing political content online. For candidates and campaigns, reaching voters where they are most engaged — via mobile and web — can only be accomplished with a highly focused multi-screen strategy.

In 2018, political consultants should produce ads that are fluid across devices since it's clear that the popular 're-purposing' of static mail pieces isn't as effective as it was when political ads were an online novelty back in 2008.

It's also a good idea to think about the intimacy of online viewing. Someone watching an ad on a bus with headphones is the only person seeing that ad — so producers can worry less about high quality production and more about message delivery that's compelling for that one-on-one interaction.

5. No more dumb banners! Rich media rules!

The move away from broadcast television means that online ads need to become as dynamic and engaging as a 30-second spot. So here's some good news. Those dramatic push-down video banners selling Apple computers that you see on the front page of USA Today and the New York Times? They can run on other outlets — same drama, same production values.

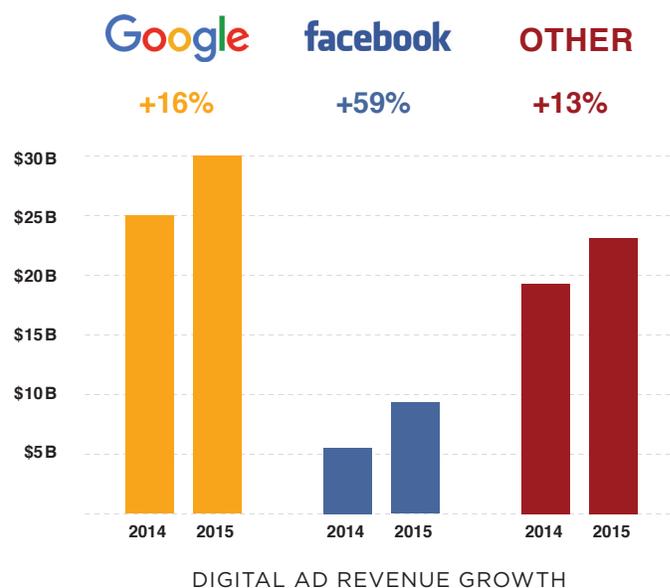
The cost for online placements like these varies greatly depending on the size of the audience. Which means that a 30-second TV ad can be cut down to a dramatic 10-seconds and run online on your local outlet of record. That same 30-seconds can also be used as a "pre-roll" placement on a cable news web page with the audio running on an Internet radio site (with or without banner ad support).

In other words, rich media offers a whole new way to engage voters — for a fraction of the cost that you may have assumed those big brand advertisers were paying.

There are some changes where consultants may need help with technical details: The death of flash banner ads means animated banners need special coding. And outlets can have different specs for different types of 'rich' media. But a professional placement firm should be able to handle these challenges seamlessly.

6. Facebook and Google will remain dominant.

During the 2016 election cycle, Facebook and Google were the clear digital winners. Facebook's ease of use, targeting tools and real-time feedback created a turnkey platform for campaigns to target its more than 162 million U.S. users. As a result, there is almost no reason to use an outside vendor for any Facebook effort. Those young persons who voted for the first time in 2008? They are now entry-level staffers and they're conversant with the buying platform and its implementation.



Source: KPBC Internet Trends 2016

Google has established dominance across the desktop and mobile platforms — not just with search and keyword ad buying long favored by political consultants — but with other channels like YouTube and its 'back end' purchasing platforms, AdX and DoubleClick Bid Manager. The YouTube channel has over 200 million US-based users that spend hundreds of millions hours a day watching video, mostly on mobile devices.

Given their broad reach and scale, the Facebook and Google duopoly will continue to consume a majority of digital advertising budgets. But that doesn't mean they're the only game in town.

7. Get social – and you can do it yourself.

For some politically insightful data points, social media can be your best friend, especially if it's used early in a campaign.

“Over 10 billion sharing and syndication events take place each month over social media”

A big data footprint is being created every minute through each like, comment and share. Political consultants and campaign managers are finding new ways to synthesize this data to provide voters with a seamless user experience as they move between channels and devices – spanning desktop computers, mobile devices or smart tablets.

According to *The Washington Post*, Senator Rob Portman was perhaps the 2016 poster child for creating a winning combination of a home-grown data warehouse and analytics to support targeted campaign ads and voter outreach. Building the right mix of data and analytics to support your digital advertising efforts does not happen overnight and requires a long-term vision – and sometimes multiple campaigns. Here too, the human element – experience and knowledge not just of a vendor but also a community or state – becomes extremely important to customize the right approach.

8. “Roll your own” data.

No two campaigns are created equal. As such, campaigns need to examine their data and targeting with an eye on the campaigns to come, not the ones from the past.

In 2018, each campaign should take a focused approach to building the right mix of data, demographics and other analytics for field, ad placement, GOTV and fundraising drives. Having the right data – and using that information for ad placement – can help deliver maximum impact from the paid advertising budget.

With the ubiquity of mobile, we are living in a “cookie-less” world, where “cookies” – online tagging methods that rely on voter registration information – are less useful. Cookies sit within the code that's used to display a desktop web browser. But more and more online access comes via tablets and phones which use a different kind of technology. Cookies can't work in that environment. They are not reliable and can lead to fraudulent ad placements.

9. Dramatic changes in Ad Tech will affect political resellers.

Over the past two years, brand advertisers have become increasingly frustrated with online ad performance. Why? Ad fraud. More than a half the time, ads saw fraudulent traffic created by people who make money by creating dummy IP addresses and “machine-generated” clicks, commonly referred to as “bots.”

Recently, brand advertisers have started to fight back and are demanding better reporting accountability and transparency. As a result, the ad tech industry has consolidated with fewer players and programmatic direct platforms emphasizing quality placements that are verifiable.

The rise of “fake news” content farms – sites set up to attract a specific kind of political viewer – is part of this trend. An ad targeted at a “likely” voter with a “voter-match cookie” is more likely to show up on a “fake news” site than it is on a legitimate outlet that attracts regular voters.

“In a Private Exchange vs. Programmatic world, the human element will still remain an essential component across the digital value chain”

So, for political ads in particular, the human element will still remain an essential component. With the continuation of fake news and click-baiting, one-on-one relationships combined with direct buys will protect advertisers while ensuring the ability to secure the best inventory.

10. Hacking isn't going away. Security of ALL data is going to become more important.

This past year, hackers exposed the vulnerabilities common in almost every organization that eschews basic tech security. If you're not taking steps to protect the data that fuels your campaign, you're asking for trouble.

This is basic stuff: Make everyone use passwords; change them periodically. Put sensitive information behind firewalls – on your computers but also your office Wi-Fi routers and storage devices. If a vendor offers an extra layer of security, use it.

All the best laid plans will go up in smoke if a hack exposes campaign strategies, denigrates the quality digital campaign data or compromises important information.

ON your mark....

During this off-year election hiatus, every political consultant should brush up on their digital skills – using the time to bolster digital aptitude will pay tremendous dividends down the road. Those that prefer to stick their head in the sand and wistfully yearn for “the good old days of broadcast television advertising” will be sorely disappointed.

Consultants should become digitally versant in the following four areas:

1. Know your vendors:

Their strengths and weaknesses. Vendors with complementary strengths can and should work well together.

2. Ask questions:

Candidates and consultants need to hold their vendor partners accountable for managing their digital advertising spend with measurable results. Getting the brush off? Ask yourself “why?”

3. Be discrete using “data”:

Not all data has to come off the shelf. Voter lists can be handy for field and mail but not useful for small online campaigns.

4. Look at Rich Media:

Think about using video in all placements. The cost isn't prohibitive; the pay-off is huge.

ABOUT SPOT-ON

Spot-On is a cloud-based political ad buying platform based in San Francisco. The firm's clients are all over the country and include advocacy and lobbying efforts as well as candidates and campaigns.

Spot-On Contact: Chris Nolan cnolan@spot-on.com