admonsters

PLAYBOOK

Navigating Political Ads for the 2024 Election Season

An AdMonsters Playbook
November 2023

Sponsored by:

geoedge
Add Integrity

What's a Playbook?

A playbook is an extension of what the AdMonsters community has been doing at our conferences for 20 years. A playbook solidifies what has made our events "must-attend" for many digital strategists. By bringing people together to share learnings and best practices in a focused way, people can create a plan and avoid hours—if not days—of doing research on their own.

The AdMonsters playbook concept takes existing AdMonsters content (from conferences and AdMonsters.com) and, with the help of the AdMonsters community, "crowdsources" a document that outlines best practices on a particular topic. Our belief is that this will allow for a free exchange of ideas with the benefit of curation for accuracy. This document does not get into specifics about individual solution providers intentionally.

Great effort has gone into writing the playbook in a fashion that applies to as many publishers as possible without becoming too general. In a technology-driven industry like digital advertising, information quickly becomes obsolete. The intention is that, based on the feedback of the AdMonsters community, the next playbook will start to take shape and, with additional contributors, grow in both depth and breadth.

TABLE OF CONTENTS

INTRODUCTION

A staggering $10 billion will pour into the political advertising arena with the goal of swaying American voters during the 2024 Election cycle. While $10 billion is a boon for digital media stakeholders, that money comes with severe risks. Navigating **misinformation** and **disinformation** will be a key challenge of this election cycle, driven by the widespread availability of sophisticated AI tools. Digital publishers and CTV stakeholders face direct and negative effects on their business, from drops in user engagement to broader societal mistrust.

The proliferation of generative AI, deepfakes, and sophisticated malvertising tactics have empowered fraudsters and foreign governments to distribute deceptive ads via programmatic channels. This alarming trend has forced digital media entities into a rapid and rigorous process of establishing, overhauling, and strictly enforcing political ad quality policies.

Ultimately it falls to publishers to serve as the final bastion of defense for their audiences. Publishers must undertake the critical task of determining whether specific advertisers and promoters of sensitive, hot-button issues can be permitted to run ads on their sites and under which conditions, while simultaneously ensuring malicious actors are kept at bay.

This Playbook provides a robust framework for an ad quality strategy, essential for setting up robust election advertising guidelines. It delves into the tools available to publishers for increased visibility and control, shedding light on challenges in the upcoming election cycle. The Playbook's goal is to empower publishers to guarantee that political ads on their platforms are informative and accurate and enhance both user experience and their own reputation.

1. CLASSIFYING ELECTION ADVERTISING RISKS

The purpose of every political ad is to influence actions, such as donating to a candidate, smearing other candidates and political parties, and swaying public opinion. Political ads are generally not subject to the Federal Trade Commission's truth in advertising regulations due to First Amendment protections. The types of ads that are of particular concern to publishers are **clickbait ads**, **deepfakes**, and those that spread **misinformation** and **disinformation**.

Clickbait Ads

Clickbait ads, known for their aggressive tactics, lure consumers away from a publisher's site. Their goal is either to directly scam or to harvest users' personal information for subsequent sale. This revenue-hijacking form of advertising becomes increasingly prevalent during election cycles.

***76%** of publishers say users have encountered clickbait ads on their sites.*

Decoding Clickbait Attacks

Here is a typical scenario of how malicious clickbait ads work:

1. Users were lured by an ad with a sensational, alarming headline.
2. A menacing pop-up then appeared, falsely alerting them that their computer had been compromised.
3. In a state of panic, they were directed to call an emergency hotline for help.
4. Once on the call, users were intensely coerced into disclosing their credit card information to "resolve" the fictitious hack.

Generative AI: A Political Super-Weapon

Election experts are deeply concerned about the potential of generative AI to spread advertising disinformation, with some calling it a "**political super-weapon**."

Source

GeoEdge CEO Amnon Siev suggests **"Publishers' credibility is on the line as they are judged on their capacity to filter out AI advertising disinformation."**

We've already witnessed global instances of information wars fueled by AI. These images have ranged from deepfake videos that depict Ukrainian President Volodymyr Zelensky surrendering to Russia, to AI-generated campaign videos of former President Trump hugging Dr. Anthony Fauci.

The Times Group requires AI disclosure within advertiser contracts. "At The Times Group, we take a proactive approach to address concerns regarding generative AI-generated political ads," said Samantha Hoffnagle, VP North America & Canada Sales, Times Group. "We have established a specific contractual agreement with political advertisers that mandates the pre-campaign sharing of their ads with us. This practice ensures transparency and accountability in political advertising on our platform.

"Under this agreement, any political campaign featured on our platform is subject to a strict policy that prohibits dynamic changes in the ads. This means that the content shared with us remains consistent throughout the campaign, eliminating the potential for last-minute alterations or manipulations using generative AI," — Samantha Hoffnagle, VP North America & Canada Sales Times Group.

2. THREATS BAD POLITICAL ADS POSE TO PUBLISHERS

Misinformation that is spread through digital advertising negatively affects public discourse, trust in media, as well as confidence in the democratic process and political institutions.

Political Ads and the Impact on Reader Expectations

Users are quick to leave a site or app if they encounter a bad ad, which we defined as an ad that is, "unpleasant, inappropriate, untruthful, or has some kind of computer virus associated with it." For this reason, it is critically important that publishers implement tools that can enforce the publishers ad quality measures.

PRO-TIP: *"Euronews does not accept Political advertising at all to maintain impartiality," explained Hassan Ramadan, Head of Digital Advertising for Euronews. "Aside from direct sales, we also monetise programmatically via direct PG deals and Google Adx OMP. We have blocked political ads via their controls and also apply additional blocking via GeoEdge to maintain our policy in this regard."*

Other publishers accept political ads, but limit the ad units in which they can appear. For instance, many publishers don't allow political ads to appear in native ad units, as they don't want them to appear as endorsements.

Impact of Bad Ads on Publisher's Reputation

Earlier this year, GeoEdge **released a study that measured the impact bad ads** have on readers' perception of publishers. The survey revealed that 77% of consumers felt that publishers that display bad ads care more about making money than they do about their readers' safety.

Over half (56%) reported leaving a site or app after seeing a bad ad, and 73% said they wouldn't recommend a site or app that had bad ads. The message is clear: Bad ads damage the publisher's reputation.

Malvertising and User Protection

Over the next 12 months, GeoEdge expects scams to take the form of asking users to help fund the campaigns of specific candidates. Others will use bait-and-switch tactics to lure consumers onto a landing page that contains malware or a social engineering scheme. Readers blame publishers when a scam originates from their sites.

PRO-TIP: *"We will not approve this type of advertising on our website and enable several technology tools like GeoEdge to monitor malicious behavior from sneaking into our inventory. That said, outside of our site, yes, IMO, the industry will see an uptick as fraudulent buyers become more sophisticated. We're already seeing reports on more sophisticated hackers from AI."*
— Katie Pillich, Senior Vice President, Revenue Operations, The Daily Beast.

3. ESTABLISHING AN ELECTION ADVERTISING POLICY

Deciding how best to deal with political advertising on a site is highly subjective; there is no one-size-fits-all strategy that's right for all online publications. Some may want to block all ads pertaining to any primary, caucus, or general election campaigns, while others may allow any or all ads submitted by a campaign, PAC, or candidate.

The difficulty lies in understanding the nuances and implementing them evenly across the site. To do that, publishers must first begin by articulating their policies towards political ads internally so that they can be uniformly enforced.

When deciding which ads to block or allow, publishers need to be meticulous in their approach. This includes applying their criteria to all aspects of political ads, such as ad creatives, landing pages, and content related to elections, political parties, policy positions, ballot initiatives, or sensitive keywords.

Managing Your Site's Political Ad Experience

Below are five strategies that online publishers can deploy for political advertising. These options can apply universally across an entire site or family of sites, or customized for specific publications.

Block all political ads while allowing specific political ads	This option blocks all political ads automatically while allowing only approved advertisers/brands to serve political ad campaigns on the site.
Allow all political ads while selectively barring some.	This option states that a publisher will accept any political ads, but selectively block ads/advertisers that do not meet the publisher's brand or audience expectations.
Spotcheck ads and associated landing pages and websites based on keywords	Publishers should create a list of sensitive keywords and proactively search political ads that contain those ads and are appearing on their sites. If one of those ads crosses the line, the publisher can opt to block it.
Automation of flagging based on keywords and their associated landing page or website	An option to consider is automated flagging of any ad that contains keywords that the publisher has blocked, or keywords that are suspicious. With this option, ads that may be problematic are flagged for review but not blocked until a brand suitability team member has reviewed it and made a determination.
Enable readers to flag political ads	All publishers should provide their users with the opportunity to report political ads they find offensive or inappropriate. The mechanism should enable flagging directly from the ad creative itself.

Crafting your Ad Quality Policy

Publishers crafting their ad quality policies should consider four key categories of political ads when identifying misinformation and disinformation:

- **Candidate-focused ads:** These are purchased by candidates to promote themselves and are well-suited for OTT/CTV, video, display, and geofencing.
- **Attack ads:** Typically launched by PACs to criticize opposing candidates, their placement is determined by platform guidelines, often extending beyond TV.
- **Fundraising ads:** Mainly used by candidates and support organizations, these ads include a call-to-action for direct donations.
- **Issue-based ads:** These address specific social issues, often sponsored by PACs in 2023, covering topics such as reproductive and voting rights, equality, the environment, and healthcare.

The next section provides a playbook for operationalizing decisions and policies across the publisher's sites to ensure compliance and minimize reputational risk.

4. GEOEDGE'S POLITICAL ADS PLAYBOOK FOR THE 2024 US ELECTIONS CYCLE

1. **Establish a Policy for Political Ad Content.** Establish a policy as described in section 4 (e.g. block all political ads but selectively allow some that meet key criteria, and so on). You'll need to first decide which ads you find acceptable (ads that cover a particular issue or are AI-generated), as well as how you will flag, review, block, or all political ads.

   When establishing a policy and communicating it to the team, be sure to be as specific as possible and include examples that help team members make decisions. This exercise will also help the editorial team explain to advertisers why their ads have been rejected, if necessary.

2. **Review the Creative's Entire Journey.** Some ads will appear innocuous enough, but the landing page or website on which they lead contains content your brand and readers will find offensive. For this reason, it's imperative that when considering the suitability of political ads, you check every aspect of it: message, images, associated landing page or website.

3. **Enable Keyword Searches of Ads.** It is imperative that publishers check for problematic ads that may contain barred or suspicious keywords. An offensive ad can damage your brand reputation quickly, which means you'll need a tool to find them and make a decision quickly and easily.

4. **Implement Strong Anti-Spam Detection & Mitigation Tools.** Fraudsters will use political ads to conduct social engineering scams to trick users into providing their email addresses, login credentials, and credit card information. Given the harm that malvertising can inflict on your readers and reputation, it is essential that you test for malvertising prior to it appearing in your ad.

   Traditional malware filters won't catch these social engineering scams. To protect your users, deploy a tool that can test the end-to-end ad delivery process ads — ad creative, text, and landing page — before allowing it on your site. Some tools leverage optical character recognition, image recognition, and context analysis to analyze campaigns on a real-time basis.

5. **Provide Mechanisms for User Reporting.** **Previous research found** that 77% of users say they would willingly report bad ads if publishers made it easy for them to do so. This political season, enable your readers to help you keep your site free of offensive and malicious ads. There are solutions available that generate reports directly from the ad itself. Establish a workflow that acknowledges the report, and follow-up with the steps you took as a result of receiving it.

The existence of a reporting tool and follow-up workflow will tell your readers that you are taking responsibility for the experience they have on your site, which is a critical step for re-establishing trust.

The global leader in strategic insight on the future of digital media and advertising technology. Through our conferences, website, and original research, we offer unparalleled in-person experiences and unique, highquality content focused on media operations, monetization, technology, strategy, platforms and trends. We provide a forum to share best practices, explore new technology platforms and build relationships.

AdMonsters has built its reputation on providing objective editorial leadership based on deep, real-world expertise. We have continued to evolve our editorial strategy to address the changing needs of the market and, as a result, AdMonsters has attracted a highly focused audience who are at the forefront of the industry, and leading marketing partners have found AdMonsters to be a powerful channel to reach these decision makers. Today, our portfolio of integrated media solutions includes industry-leading live events, our innovative Connect content solutions, email marketing programs, and more.

AdMonsters is part of the Access Intelligence family of companies.

For more info:
See **admonsters.com**
Follow us on Twitter: @AdMonsters
Facebook: facebook.com/admonsters

Media contact:
marketing@admonsters.com
Sponsorship contact:
sales@admonsters.com

GeoEdge's mission is to protect the integrity of the digital advertising ecosystem and to preserve a quality experience for users. GeoEdge's advanced security solutions ensure high ad quality and verify that sites/apps offer a clean, safe and engaging user experience, so publishers and app developers can focus on their business success.

App Developers and publishers around the world rely on GeoEdge to stop malicious and low-quality ads from reaching their audience. GeoEdge allows publishers to maximize their ad revenue without quality concerns, protect their brand reputation and increase their user loyalty. GeoEdge guards digital businesses against unwanted, malicious, offensive and inappropriate ads—without sacrificing revenue.

To learn more, visit: **www.geoedge.com**

sponsored by: