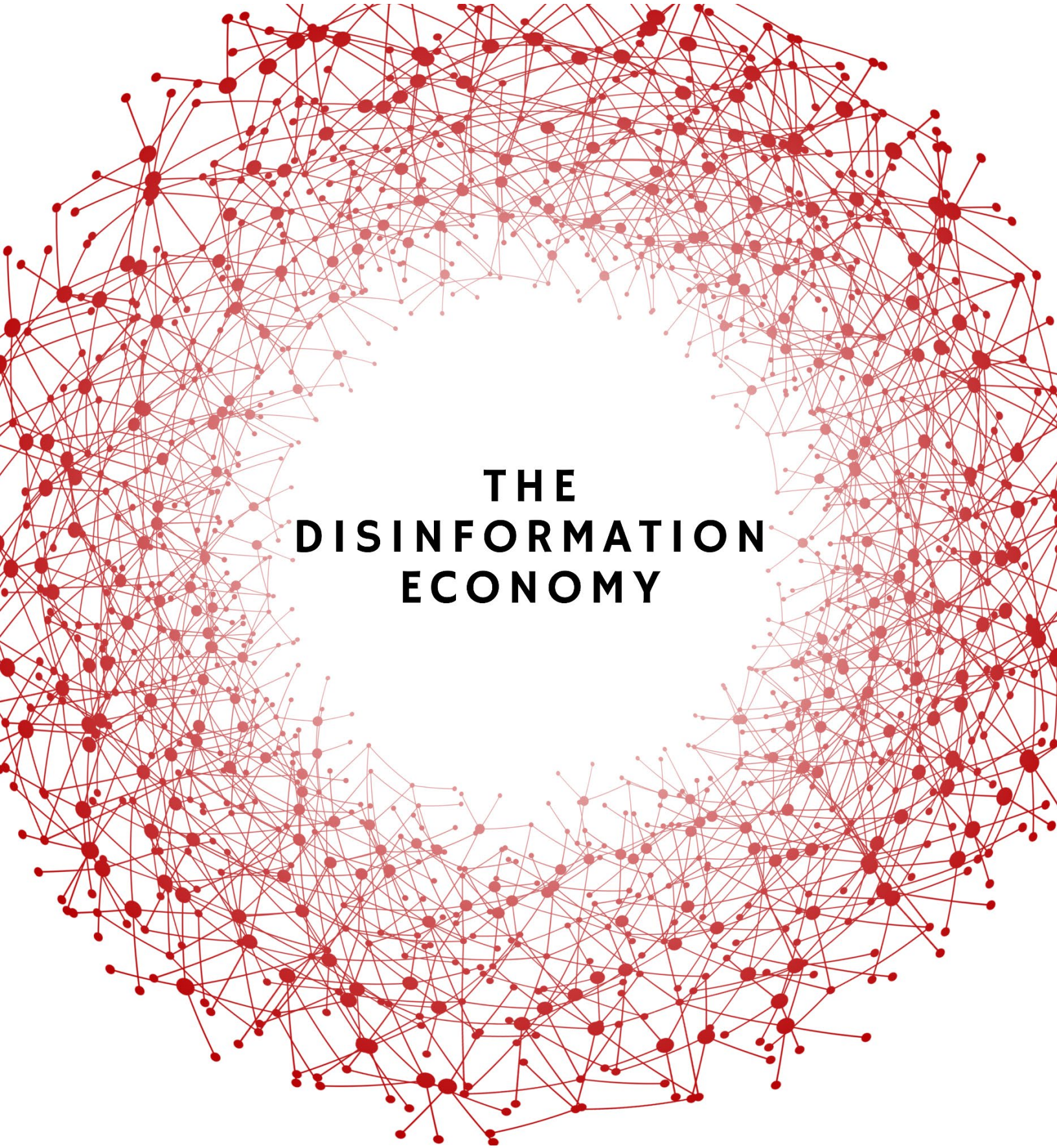


THE DISINFORMATION ECONOMY

THE CARTER CENTER

MICHAEL SCHOLTENS, PEDRO PIZANO
MAX KARPAWICH, GUTHRIE KUCKES

MCCAIN INSTITUTE

This report was made possible by generous support by the Craig Newmark Philanthropies. We would also like to acknowledge support from Michael Baldassaro, Paul Fagan, Dan Richardson, and Dr. Anthony DeMattee.

Craig Newmark Philanthropies

I. EXECUTIVE SUMMARY

Ahead of the 2016 US Elections, teenagers in Macedonian created pop-up websites with fabricated stories about the upcoming elections to generate ad revenue.[1] The political fallout from these sites helped introduce the term "fake news" into the popular lexicon. However, the teenagers that ran these sites were not political ideologues, but, instead, understood how to exploit the virality of misinformation on social media platforms to generate clicks and monetize sensational political content. These fake news sites didn't generate the same traffic as established media sites, but they garnered global media attention, and provided a blueprint for converting clicks on social media into advertising revenue. This was the birth of The Disinformation Economy.

During 2020 US Elections, The Carter Center highlighted how election fraud narratives were spread and amplified by sites known to repeatedly publish false and misleading information.[2] Between Election Day and Inauguration Day, content from known disinformation sources spiked 156% on Facebook as 10 of the top 15 sources in Facebook groups where election misinformation metastasized were known sources of disinformation, outperforming, and drowning out, mainstream news sources. On Facebook, the 20 most shared links about election fraud from disinformation publishers were shared 283,000 times with a potential audience of 31.2 million users.

The revenue generated from social media clicks through to disinformation sites is what sustains websites that publish disinformation and incentivizes them to produce more. In 2018, a study by MIT found that false and misleading political content travels six times faster and reaches wider audiences than other forms of social media content.[3] A 2019 Global Disinformation Index (GDI) report examining technology that automatically serves ads on high traffic sites found that sites that publish disinformation rake in an estimated $235 million annually in ad revenue[4]; in 2022, GDI estimated that the 40 US websites responsible for most election disinformation generate $42.7 million in annual ad revenue.[5]

The Disinformation Economy is abetted by an opaque and complex online advertising ecosystem. In abstract terms, the system includes thousands of advertising technology ("ad tech") systems that function as brokers between companies looking to advertise ("advertisers") and websites ("publishers") with ad space to sell. To quickly match advertisers and publishers, ad tech systems maintain direct

[1] How Teens in The Balkans Are Duping Trump Supporters with Fake News
[2] The Big Lie and Big Tech: Misinformation Repeat Offenders and Social Media in the 2020 U.S. Election
[3] The Spread of True and False News Online, pg. 2
[4] The Quarter Billion Dollar Question: How is Disinformation Gaming Ad Tech?
[5] Ad-funded Elections Integrity Disinformation

relationships with publishers. In addition to the publishers that are directly selling their ad space through these ad tech systems, there are also numerous resellers that buy and sell ad space as intermediaries. This often results in ad space being sold and resold, before an advertiser actually places an ad. With this complexity and an industry focus on user data over contextual data about ad placements, advertisers are often unaware of all the locations where their ads run online.[6] This means that ad tech systems themselves are best placed to prevent ad placements on known sources of disinformation by removing them from the marketplace.

The Carter Center and The McCain Institute have investigated the online advertising ecosystem, using NewGuard media ratings, web traffic estimations, and open-source information. Among the key findings:

- Disinformation sources benefit extensively from online advertising revenue. 81.47% of estimated traffic to known sources of disinformation have direct access to online programmatic advertising.
- Disinformation sources are not a core component of ad tech systems' business models. As of the end of 2022, only 35% of ad tech systems evaluated in this report have a disinformation publisher as a direct client. The average proportion of traffic from disinformation publishers compared to all other NewsGuard rated sites is 2.9%.
- Advertisers are likely unaware of where their ads are running. In 2022, well-known advertisers such as Amazon, Hewlett Packard, Bing, and Verizon had their ads run on sites that publish election disinformation, health disinformation, and conspiracy theories. However, the complexity of the online advertising marketplace means that they may never have been aware of these ad placements.
- Credible media sites have direct relationships with ad tech systems that work with disinformation sites. The New York Times and Wall Street Journal have direct relationships with several ad tech systems that work with known disinformation publishers. Given the opacity of the marketplace, it is unlikely that credible media sites are aware they share platforms with disinformation sites.
- Google is the dominant force in the programmatic advertising space and any effective industrial action to demonetize disinformation must include their ad tech platforms. A policy change by Google could have a devastating effect on disinformation online. A GDI report from 2022 found that Google facilitated an estimated 26.9% of revenue to 40 sites known to spread disinformation

[6] Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes, and the Business of Journalism, pg. 16

about U.S. elections, more than double the percentage of any other ad tech platform.[7] However, Google does not conform to industry norms concerning the disclosure of publishers that are active on their platforms. More than 72% of their sellers.json file (a record of active sellers of ad space on an ad tech platform) are listed as classified and contain no information about the owners of the accounts. This is in stark contrast to the industry average of 0.5% of records being classified. Without this transparency it is impossible to independently verify the extent to which Google has direct business relationships with known sources of disinformation.

With these findings, The Carter Center and the McCain Institute have discovered that disinformation publishers benefit greatly from access to advertising revenue using the same advertising marketplace as legitimate media sources. However, social media platforms, ad tech systems, publishers, and advertisers can take concrete action to limit this revenue and reduce the appeal of publishing disinformation online. To accomplish this goal, The Carter Center and the McCain Institute offer the following recommendations:

For Social Media Platforms

1. **Limit the sharing of posts containing links to known sources of disinformation from a single user.** Restricting sharing of posts links to known sources of disinformation reduces the virality of the post and reduces the number of clicks the link receives. WhatsApp already limits the number of direct message forwards to five to curb viral misinformation spread. When Twitter has barred direct retweets of false information, it has found a 29% decrease in content sharing.[8]

For Advertisers:

2. **Use Exclusion/Inclusion lists that consider the harm of disinformation sites when setting up your ad campaign with your demand side platform (DSP).** Exclusion/Inclusion lists reduce the threat of your ads appearing on sites that could harm the brand image. They also reduce the demand for impressions from sites excluded from your campaign and lower their revenue. While there may be other options, NewsGuard for Advertising provides up-to-date information about known sources of mis- and disinformation that can be used to create exclusion/inclusion lists to protect your brand.
3. **Check your DSP's policy on mis- and disinformation**. Some DSPs have policies prohibiting known sources of disinformation from appearing on their platforms. If you work with a DSP that does not have such a policy, contact your account

[7] Ad-funded Elections Integrity Disinformation
[8] An update on our work around the 2020 US Elections

representative and express the importance of not having your ads run on known sources of disinformation.

For Ad Tech Systems:

4. **Prohibit known sources of disinformation from opening accounts with your platform.** Known sources of disinformation represent a small portion of revenue for ad tech systems and a large threat to the brand security of advertisers. It is in the interest of the industry to prohibit these publishers from accessing the programmatic advertising system to protect advertisers and maintain credibility as responsible actors in the programmatic advertising ecosystem.
5. **Offer brand security tools that incorporate misinformation prevention.** Offering preset exclusion/inclusion lists for advertisers that exclude known sources of disinformation reduces the burden on advertisers to identify harmful sites for custom exclusion/inclusion lists and produces better ad campaigns that meet the expectations of advertisers that wish to avoid disinformation publishers.

For Google:

6. **Make public sellers.json records the default option.** Google currently requires publishers to opt in to sharing their details in their sellers.json file. This results in 72.9% of the records in their sellers.json file being classified, making it impossible for ad tech systems and advertisers to verify if most Google accounts in ads.txt files are accurate. The default classification of records undermines efforts to prevent fraud and makes it easier for disinformation sites to monetize their traffic.

For Publishers:

7. **Opt-in to sharing seller details on Google's sellers.json file.** If you use Google to sell ad inventory, opt to share details of your account to lower the rate of classified records on Google's sellers.json file. The high rate of classified records in Google's sellers.json file allows disinformation sites to appear less conspicuous in hiding their details by hiding in a sea of classified records instead of the 0.5% of classified records for the rest of the industry.

II. INTRODUCTION

Online misinformation has presented a challenge to governance around the globe. False narratives about election fraud, public health measures, and political leaders are now commonplace in our political discourse and play a pivotal role in efforts to destabilize democratic institutions.[9] How these narratives begin, evolve, and spread is often difficult to identify, but one popular mechanism is through fake new websites that intentionally produce misinformation. These sites often masquerade as legitimate news sites with content designed to diminish the reader's skepticism by mimicking the format of traditional online news outlets. While these sites regularly espouse a political ideology, the motivation for the creation of this content is also driven by economic incentives, as the vast majority of traffic on these sites can be monetized by online display advertising.[10] We define this opportunity to monetize the consumption of misinformation as what we call *The Disinformation Economy*.

The Carter Center illustrated the role of these sites in spreading misinformation in our report, *The Big Lie and Big Tech*, showing that the genesis of misinformation narratives is often not a result of discourse on large social media platforms, such as Facebook, Instagram, or X, but from individual content creators on third-party websites. From August 17, 2020, to January 20, 2021, The Carter Center collected 2.93 million posts from 883 public Facebook groups that engaged in political content during the presidential election cycle. Of these posts, nearly 1 million of them linked to an external site, with more than 350,000 originating from sites rated as untrustworthy by NewsGuard, an independent fact-checking organization that employs trained journalists to investigate and rate media sites. With users from social media sharing these links, the traffic directed to these sites is then monetized through online advertising and supports the creation of more misinformation in the future.

While The Disinformation Economy incentivizes websites to produce harmful content, it also presents an opportunity to take concrete steps to curb the spread of misinformation. If the online advertising industry and ad buyers restrict the sale of ads on these sites, the loss of revenue will dramatically reduce the appeal of misinformation as a business model. In this report, we investigate the scope of The Disinformation Economy based on extensive data collection and provide a set of recommendations for reducing the production of disinformation.

III. THE ONLINE ADVERTISING SYSTEM

[9] Disinformation as a Threat to Deliberative Democracy, pg.2

[10] Using web traffic estimation data from Similarweb, NewsGuard ratings, and information from ads.txt files we can estimate that more than 80% of traffic on disinformation sites has the potential to be monetized using online display advertising.

The online advertising economy is a complex network of buyers, sellers, and intermediaries that facilitate the placement of ads on websites and social media platforms. Advertisements displayed on websites are predominantly served by ***advertising systems***, which function as middlemen between the ***advertisers*** (e.g., Coca-Cola, Home Depot, etc.) that want to place their ad on a website and the ***publishers*** (e.g., New York Times, Wall Street Journal, etc.) that have ad space to sell.

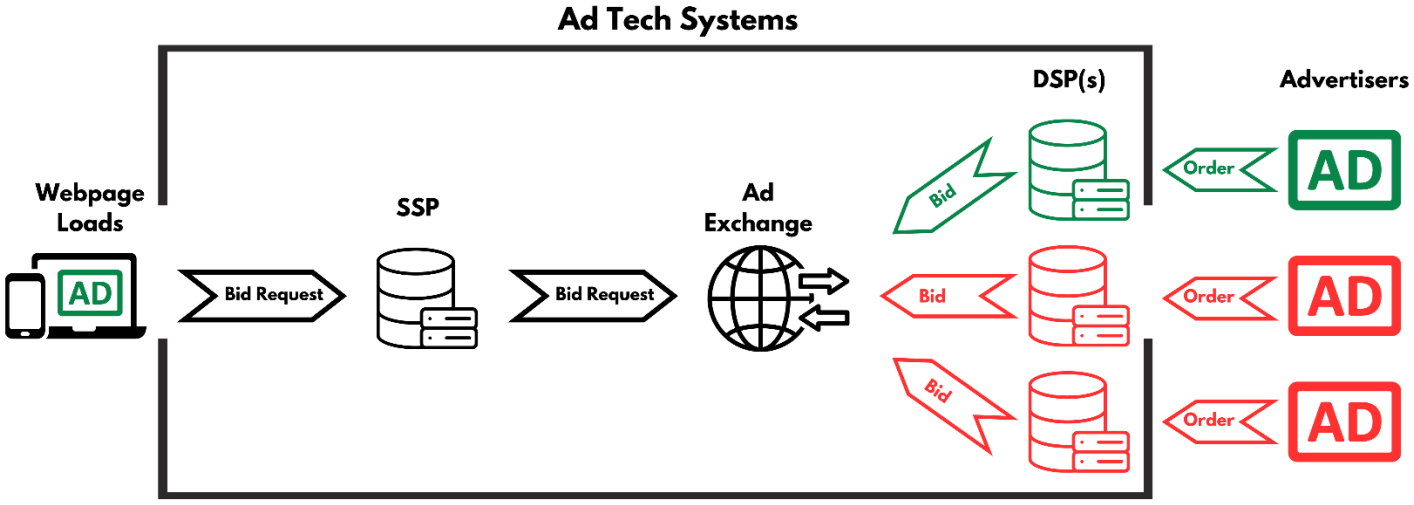
In the online advertising industry, the opportunity to sell an ad is called an ***impression***. An impression occurs when a user loads a webpage that has ad space to sell.[11] Unlike billboards on the side of the road, online display ads are rarely permanent fixtures on a webpage but are sold and displayed every time a user navigates to the page. While there are several ways to value an ad space, advertisers often bid for ads by the impression with the prices for ads listed by the metric ***Cost Per Mille (CPM)***, or the cost per 1000 impressions. This cost is determined by several factors, including the number of bidders (e.g., advertisers), the demographic of users targeted, and the subject of the ad.[12] Despite the wide variability in pricing, impressions are the primary unit of sale in online advertising.

Commonly, there are multiple ad tech systems involved in the sale of an impression. Advertisers often deal with ad tech systems called ***demand-side platforms (DSP),*** and publishers list their available impressions through an ad tech system called a ***supply-side platform (SSP)***. DSPs and SSPs then work to connect interested advertisers and publishers by participating in online auctions for these impressions. Publishers initiate these auctions by sending a request for bids on an impression through their SSP to another type of ad tech system called an ***ad exchange***. The ad exchange then facilitates an auction for the impression, where DSPs will then bid on behalf of advertisers for the opportunity to show ads to the user who loaded the webpage. A simplified version of this process is outlined below.

[11] Interactive Audience Measurement and Advertising Campaign Reporting and Audit Guidelines

[12] 8 factors that influence your CPM

Figure 1



In this illustration, the process is initiated on the left when a user loads a web page with ads. The website publisher then sends a request for bids to their SSP(s), and the SSP(s) sends that request to an ad exchange. At the exchange, the impression is auctioned, where DSP(s) working on behalf of advertisers place bids based on orders for impressions. The winning bid results in that advertiser's ad being placed on the page and shown to the user, as seen by the green ad above. The impression may also be purchased by intermediary ad tech systems such as resellers or ad networks and sold again through another ad exchange or other mechanism.

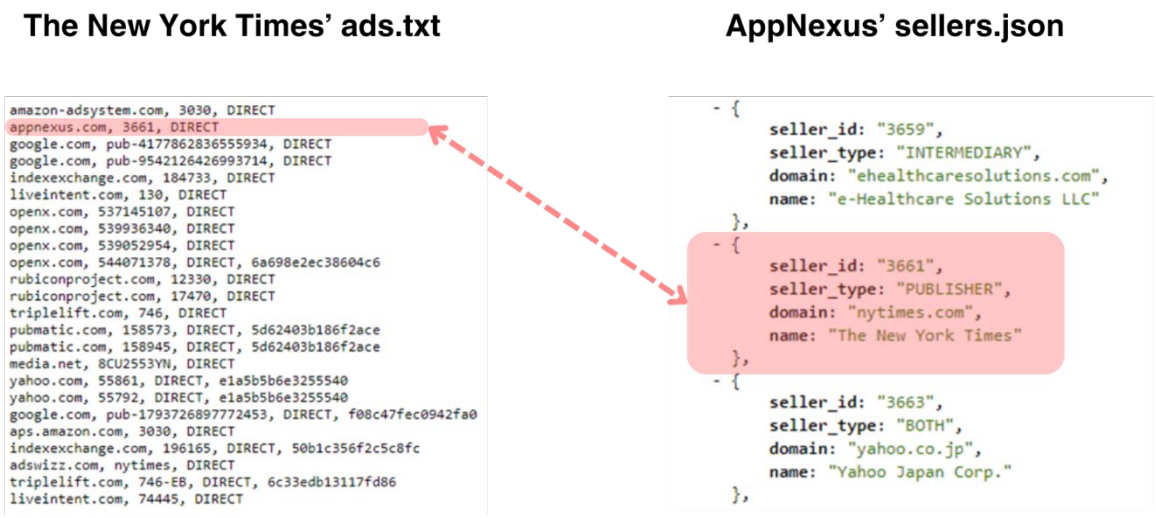
To accomplish personalized ad placements, the system is highly automated and is often referred to as ***programmatic advertising***. In this report, we have focused on programmatic display advertising, which includes the automated sale of ads such as banners and pop-ups. In 2022, Advertisers spent $63.5 billion on display advertising, accounting for 30.3% of all internet advertising spending.[13] The focus on programmatic display advertising in this report is due to the prevalence of these types of ads in the monetization of websites, like those that spread mis- and disinformation. Programmatic advertising also made up 87.3% of online display advertising in 2022 compared to static advertisements and other methods of placing display ads.

To allow for ads to be placed in the milliseconds it takes to load a webpage, the programmatic ads system relies on a set of documents shared by publishers and ad tech systems on their websites. In 2017, the Interactive Advertising Bureau (IAB)

[13] Internet Advertising Revenue Report 2022, pg.15

proposed the creation of these documents, called ads.txt and sellers.json, in an effort to prevent fraud in online advertising auctions. These documents take the form of machine-readable files hosted on each site in the online advertising marketplace. In the case of ads.txt, the file is hosted by website publishers and lists each of the ad tech systems that are authorized to sell impressions from their site. For sellers.json, the file is hosted by the ad tech system and lists all of the publishers that have authorized them to sell impressions on their behalf. Together, the ads.txt and sellers.json files form a ledger to verify the authenticity of impressions and prevent fraud in online advertising purchases. The two files below illustrate how the system works. The file on the left is The New York Times' ads.txt file found at www.nytimes.com/ads.txt. The file on the right shows the corresponding entry in the sellers.json file found at www.appnexus.com/sellers.json, a major ad tech system.

Figure 2



As a prospective advertiser, these two files show that AppNexus and The New York Times have an agreement to sell impressions, so they could be confident that if they purchased an impression from nytimes.com through one of their SSPs, AppNexus, it would not be a fraudulent purchase and that their ad would appear on the intended webpage. Normally, these documents are checked programmatically by the ad tech systems involved in the transaction. However, they are available for review by all entities in the system as well as outside observers and offer a glimpse into the opaque world of online advertising.

Unfortunately, the files do not provide complete information for all market transactions. In particular, the files do not tell how many transactions have occurred between an ad exchange and a publisher, the monetary value of those exchanges, or which organization is paying to advertise its brand on the publisher's site.

IV. DATA COLLECTION METHODOLOGY

To adequately evaluate the scale of *The Disinformation Economy*, The Carter Center and McCain Institute collected and combined multiple data sources to substantiate our analysis. This included data collected from ads.txt and sellers.json files, online media ratings data from NewsGuard, as well as web traffic estimation and advertisement data from SimilarWeb. Together, these data streams offer a view into the opaque world of online advertising and provide actionable insights to limit the monetization of disinformation.

To determine what is considered a source of disinformation, we relied on NewsGuard ratings data to evaluate the information profile of news media publishers. These ratings provide a credible and thorough review of online media in the United States, and according to NewsGuard, sites they have rated make up approximately 95% of engagement with online media in the United States.[14] NewsGuard ratings divide online media into four categories: Trustworthy (e.g., credible news sources), Not Trustworthy (i.e., not credible news sources), Satire, and Platform (i.e., social media platforms). As part of the evaluation process, there are further assessments of each site's behavior, including whether the site repeatedly fails to remove or publish retractions for stories that have been fact-checked and proven false.[15] NewsGuard asserts that there is a high bar for sites to be identified as "repeatedly publishing false content."[16] Consequently, this status separates sites that may consistently share misinformation unwittingly from those that are likely to maliciously publish misinformation. This report discusses the first set of sites as 'known sources of misinformation' and the second set of sites as 'known sources of disinformation.'

To determine the possibility of these sites monetizing their traffic with programmatic advertising, The Center collected information from ads.txt files hosted by publishers that have a NewsGuard rating and the sellers.json files of the ad tech systems listed in the ads.txt files. This produced a set of publishers that have been evaluated for misinformation and a set of ad tech systems that were reported to work with these publishers to sell ads. One challenge with analysis involving ads.txt and sellers.json files is that participation in the system is voluntary, and there is no comprehensive list of publishers and ad tech systems that host ads.txt and sellers.json files. However, as NewsGuard-rated websites account for an estimated 95% of engagement with online news media in the United States,[17] our analysis uses NewsGuard-rated sites to define the scope of our data collection.

---

[14] Misinformation White Paper: Independent Research Shows Human-Curated News Reliability Ratings Work to Mitigate False News

[15] For more detail and description of NewsGuard's rating system, you can find more information on their website.

[16] Website Rating Process and Criteria

[17] Website Reliability Ratings

For each NewsGuard-rated site, we checked for an ads.txt file listing authorized sellers of advertising for the publisher. If there was at least one valid authorized seller (i.e., an ad tech system that appeared in the ads.txt file and was confirmed by the matching sellers.json file, as shown in Figure 2), we determined that the site was prepared to sell ads. While the presence of an ads.txt file does not guarantee that any ads were run on the publisher's domain, it does show the intent of the publisher to monetize traffic on their site and successful integration into the programmatic advertising marketplace.

While the presence of known sources of mis- and disinformation in sellers.json files evidences the potential for monetization, it does not provide an indication of the potential revenue. To determine the number of potential impressions available for sale from these publishers, we sourced web traffic estimation data from Similarweb to determine the number of visits each site received from October 1, 2021, to September 30, 2022. Web traffic estimation is not a replacement for actual web traffic data. Independent testing of Similarweb's data has shown that while the estimated number of visits is often incorrect when compared to actual visits[18], the error is consistent across sites, so the estimated traffic numbers still provide insight when comparing the sites to one another. To further reduce the effect of random errors, this report discusses the estimated traffic in aggregations based on the NewsGuard rating and not based on individual site estimations.

Similarweb also offers data on the placement of advertisements on websites based on real traffic data shared by users and websites. The identities of the advertisers are determined by where users are redirected when they click on an ad. This means that only ads on which users click are reported by Similarweb, so these data skew toward ads with higher engagement and not necessarily higher frequency of appearance. For this reason, these data do not offer a complete picture of all advertisements that run on each webpage, but it does confirm some of the ads that have appeared on known sources of disinformation. This report uses these data to show the threat of disinformation to established brands if these publishers are allowed to participate in the programmatic advertising system.

We also independently evaluated each site to determine the number of ads that appear on each publisher's home page. To do this, we programmatically navigated to each site and used the EasyList advertising filter that is used by many ad-blocking applications to identify advertisements on the page. To ensure that ads that rely on JavaScript were not excluded, we used Selenium to load each page and render JavaScript elements. As the EasyList is dynamically updated and adds elements on a given page, it may not display an ad for myriad reasons. We do not discuss the number

[18] How Accurate Is Similarweb Data (by Traffic, Keywords, Referrals)?

of ads on a single page but discuss the average number of ads per NewsGuard rating category to reduce random error.

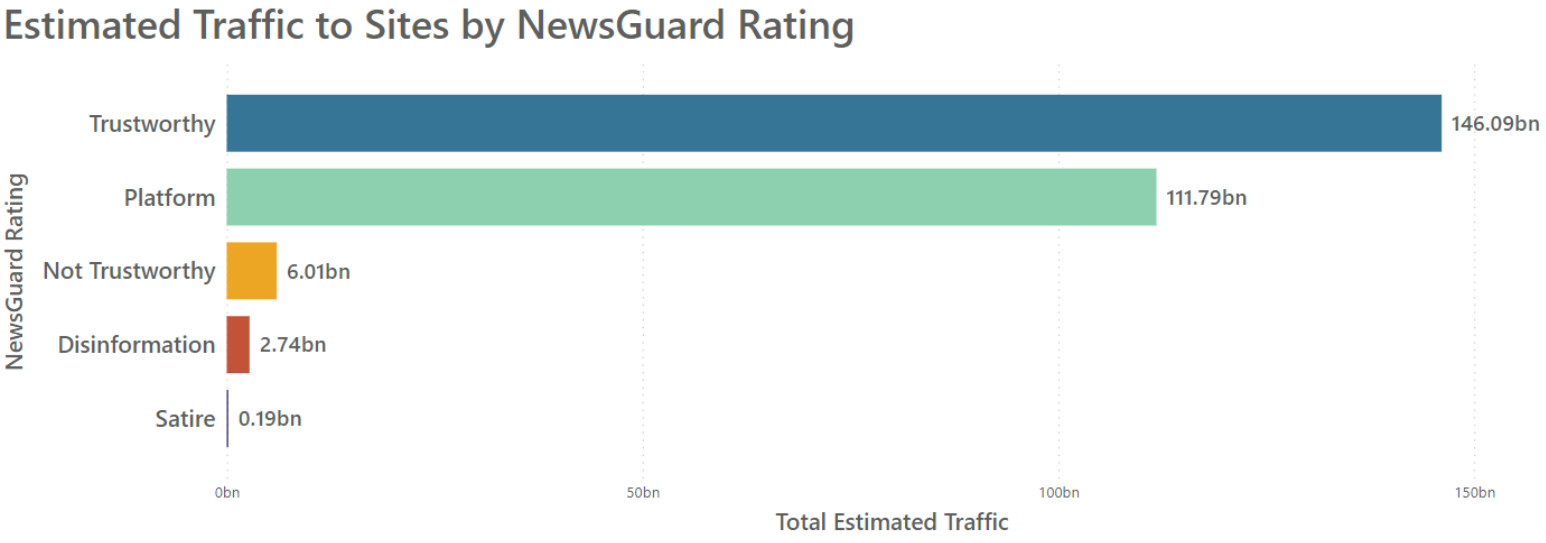
By combining data from ads.txt/sellers.json files, NewGuard ratings, web traffic estimation data, and reported advertising, this report offers the clearest picture of the opaque online programmatic advertising system possible without access to privileged data available only to the ad tech systems and publishers themselves.

V. FINDINGS

Presence of disinformation in the Online Advertising Ecosystem

While the monetization of disinformation through advertising is concerning, the magnitude and specific mode of monetization have been difficult to define due to a lack of transparency in the world of online advertising. In a report released by NewsGuard and ComScore, the advertising spending on misinformation globally is estimated to be approximately $2.6 billion dollars a year.[19] However, this estimate accounts for all known sources of misinformation sites compared to just known sources of disinformation. While this report evaluates the presence of known sources of misinformation in the marketplace, the primary focus of this analysis is on known sources of disinformation. By concentrating on sites with an intention to deceive, this report aims to build an easier consensus for collective action from advertisers, publishers, and ad tech systems to demonetize sources of disinformation and reduce the appeal of disinformation as a business model.

Figure 3



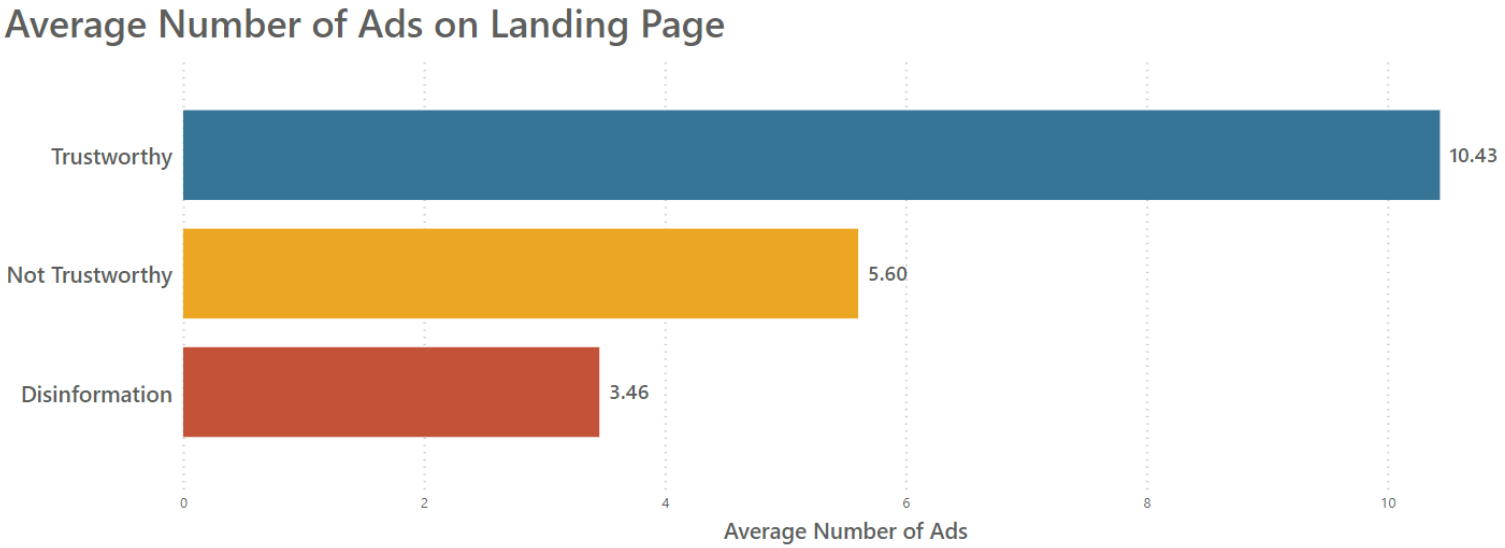
In 2022, the total traffic to disinformation sites accounted for only 1.03% of all traffic to NewsGuard rated websites. Traffic to Trustworthy sites stands at more than 146

[19] Special Report: Top brands are sending $2.6 billion to misinformation websites each year

billion, dwarfing traffic to misinformation, disinformation, and Satire sites.[20] Traffic is an important metric in understanding the advertising ecosystem because visits to a site, or impressions, are the unit of sale for online ads, so traffic serves as a proxy for the number of possible impressions sold by a publisher.

In addition to traffic, when comparing the number of ads that appear on the landing page of each site, it is clear that disinformation publishers host fewer ads on their landing pages than sites of higher information quality. Trustworthy sites host an average of 10.43 ads, Not Trustworthy sites host an average of 5.60 ads, and disinformation sites host an average of only 3.46.

Figure 4



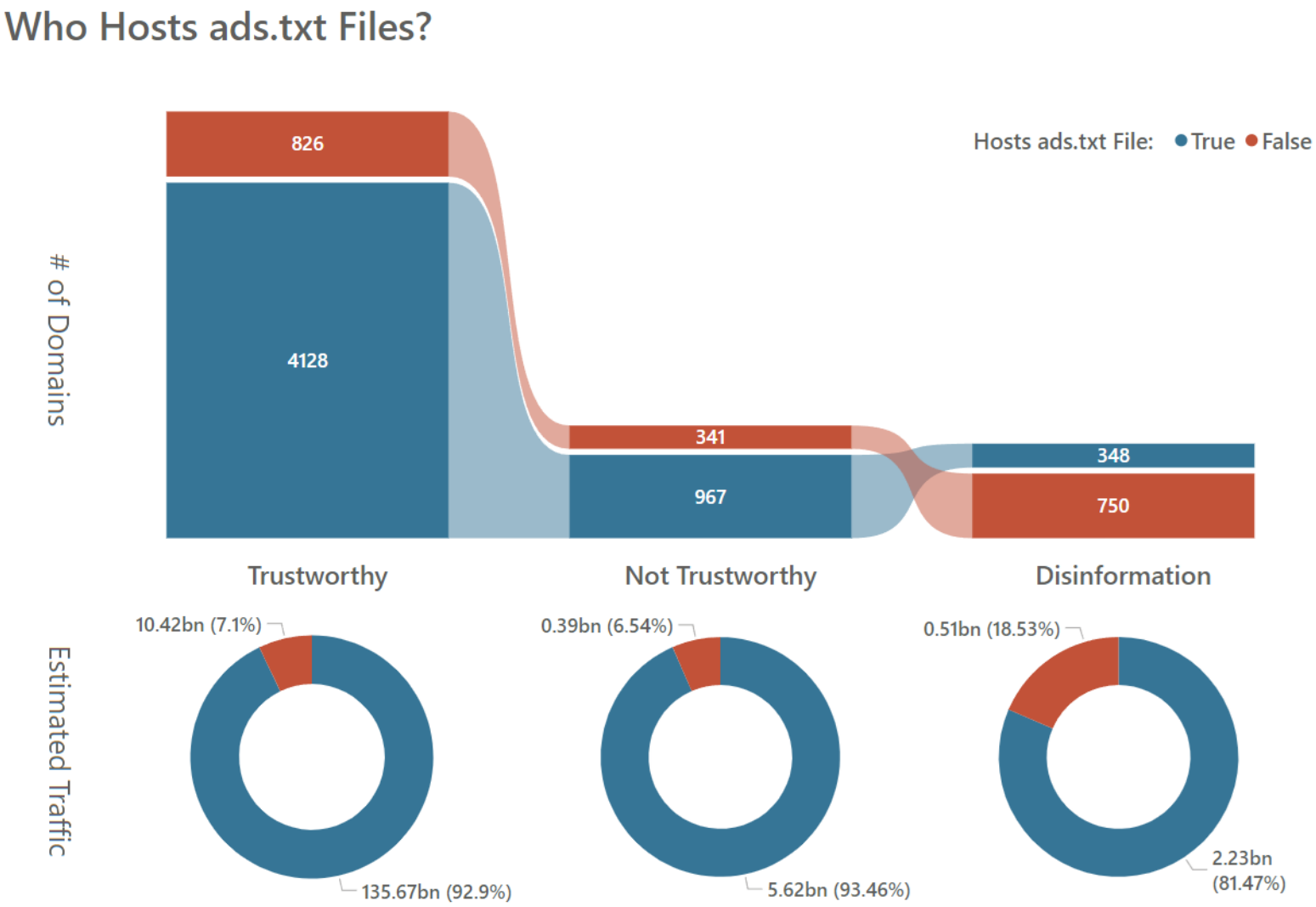
While disinformation sites only constitute a small portion of the traffic to online news sites, a large portion of this traffic can be monetized using programmatic advertising. Of the 1098 known sources of disinformation that have web traffic estimations through Similarweb, only 348, or 31.69%, host ads.txt files. However, these sites boasted more than 2 billion estimated visits during the past 12 months, equating to 81.47% of traffic to all disinformation news sites.[21] Ultimately, this means that the vast majority of traffic to disinformation publishers is, or is ready to be, monetized through the sale of programmatic ads.

---

[20] Platform traffic in this analysis only applies to platforms that use the ads.txt system to facilitate ad sales on their site. Site like Facebook.com and youtube.com rely on their own ad sales systems and are excluded from this statistic.

[21] 81.47% is an approximation, as there are 379 disinformation publishers that have estimated web traffic less than 5,000 visits per year. Due to the methodology used by Similarweb to estimate traffic, these sites do not have a confident web traffic estimation. However, the total web traffic estimation for the other 1098 disinformation sites is 2.74 billion visits per year, so the possible effect of the traffic from the other 379 sites on this statistic in negligible.

Figure 5



Advertisers in The Disinformation Economy

Despite the decrease in the volume of ad sales as the information quality of the website decreases, major advertisers continue to appear on websites that are known sources of disinformation. When comparing the top 100 advertisers that have appeared on trustworthy sites in the last 12 months and the top 100 advertisers to appear on disinformation publishers, 23 appeared on both sets of sites. This cross-over is impossible to attribute to a single cause, as some advertisers may intentionally advertise on disinformation sites. However, the lack of consistent audit transparency in ad placements makes it possible that many advertisers may not know that their ads ran on these sites.

As described in the previous section, the sale of an impression involves at least one ad tech system serving as an intermediary. However, there are often many

intermediaries between the advertiser and publisher, potentially obscuring the final location of the ad. Often, this results in the advertisers not receiving information, or receiving incomplete information, about where their ads were placed.[22] This lack of consistent audit transparency is driven by the industry focus on user data over publisher data at the point of sale and is difficult to solve with so many ad tech systems and intermediaries participating in the ecosystem.[23] Given the lack of transparency, it is possible, and perhaps likely, that many of the 23 advertisers that had ads on both trustworthy and disinformation news sites are unaware or did not intentionally place the ads on disinformation publishers' sites, despite the risks to brand security and image.

Using the NewsGuard topic classifications for the disinformation sites where these 23 advertisers appeared, the table below illustrates the type of content that may have appeared adjacent to their ads.

[22] Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes, and the Business of Journalism, pg. 16
[23] Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes, and the Business of Journalism, pg. 16

Figure 6

Ad Adjacent Content

	Political Misinformation	Health Misinformation	Conspiracy Theories
amazon.com	X	X	X
bing.com	X	X	X
hp.com	X	X	X
verizon.com	X	X	X
temu.com	X	X	X
carfax.com	X	X	X
coachoutlet.com	X	X	X
thewalletguru.com	X	X	X
walletgenius.com	X	X	X
heraldweekly.com	X	X	X
moneymetals.com	X	X	X
go.reference.com	X	X	X
go.hellogenie.com	X	X	X
lightinthebox.com	X	X	X
saksfifthavenue.com	X	X	
wayfair.com	X		X
kohls.com	X		X
motortrend.com	X		X
belk.com	X		X
orthofeet.com	X		X
globaltinyworld.com	X		X
orthofeet.com	X		X

Advertisers and ad tech systems have already identified mis- and disinformation as a threat to brand security. In surveys conducted by ad verification companies Integral

Ad Science (IAS) and Double Verify, ads appearing alongside misinformation have a negative impact on brand perception. Integral Ad Science's survey states:

> *The majority of US consumers (81%) find it annoying when a brand appears next to low-quality content. Of those consumers, 52% feel less favorably toward a brand that does this. The most concerning issue though, is the discovery that 62% will stop using the brand altogether if its ads appear adjacent to low-quality content.*[24]

According to IAS, 'low-quality content' includes material that poses a 'moderate brand risk,' with 'fake news' used as an example of content that may be considered low-quality.[25] Double Verify's survey directly addresses the effect of misinformation by asking consumers how ad placement next to false content affects their perceptions of the advertising brand. Their findings state:

> *Over half (55%) of consumers say it would negatively impact future purchase decisions if they were to see a brand advertised next to false or misleading content.*[26]

The threat to brand security for advertisers has only increased as journalists and organizations like checkmyads.com have called out brands such as Warby Parker[27] and organizations such as Planned Parenthood[28] for running ads on disinformation sites. In both cases, the advertisers likely had no idea that their ads appeared on these sites.[29]

In response to the threat of mis- and disinformation to brand image, many ad tech systems offer brand security tools that allow advertisers to set their own limits on where they would like their ads to appear. These tools can take the form of exclusion lists that prohibit ad sales to sites on the list or inclusion lists that only permit ad sales to sites on the list. In the current system, advertisers are responsible for making use of these tools and often have the choice to use an exclusion list or inclusion list. Some of these tools, like NewsGuard for Advertising, prioritize the exclusion of sources of misinformation and the inclusion of quality news media, but this is more difficult with many lists provided by ad tech systems.

Role of Ad tech systems in the Monetization of Disinformation

---

[24] The Ripple Effect
[25] The Ripple Effect
[26] Four Fundamental Shifts in Media & Advertising During 2020
[27] Warby Parker Tweet
[28] Do-Gooders Doing Bad: How Nonprofit and Government Organizations Unintentionally Fund the Misinformation Machine
[29] Do-Gooders Doing Bad: How Nonprofit and Government Organizations Unintentionally Fund the Misinformation Machine

Behind the placement of nearly every ad online, ad tech systems play a fundamental role in connecting advertisers with publishers and monetizing digital media around the world. With each impression that is sold through ad exchanges, the ad tech systems involved in that transaction facilitate the flow of ad dollars from advertiser to publisher and profit from the sale. While this mechanism is well understood, determining the potential revenue for ad tech systems from the sale of ads to disinformation publishers is difficult, given the lack of transparency in the marketplace.

Without access to direct ad sales data, estimated traffic is the only proxy for the number of impressions available for sale in the programmatic display advertising marketplace. When combined with NewsGuard ratings and the information from each ad tech systems' sellers.json file, estimated traffic can be used to determine the potential monetization of disinformation for each of the 328 ad tech systems evaluated in this analysis. We have defined the potential monetization as the total traffic of the disinformation publishers found in each ad tech system's sellers.json file. While it is highly unlikely that any ad tech systems were involved in the sale of every impression from their clients, higher traffic represents a greater opportunity to sell impressions. Thus, higher traffic to clients that are disinformation publishers represents a greater opportunity for an ad tech system to profit from the monetization of disinformation.[30]

While advertisers can limit the monetization of disinformation by using brand security tools like inclusion/exclusion lists, some ad tech systems have already recognized the need to prevent sources of disinformation from using their platforms. Ad tech systems, like OpenX and Revcontent, have explicit policies against monetizing publishers who produce misinformation. However, despite these policies, our analysis shows that OpenX worked directly with 20 disinformation publishers with a combined estimated traffic of 854.3 million in 2022, and Revcontent worked with 29 disinformation publishers with a combined estimated traffic of 910.2 million in 2022.

[30] To reduce assumptions in our estimations, we have not multiplied traffic by the average number of ads observed in the previous section of this report and only assumed a single ad placement per visit despite the likelihood that there is often more than one ad placement.

Figure 7

AD SYSTEM	MISINFORMATION POLICY
REVCONTENT	REVCONTENT DOES NOT ALLOW ANY NON-SATIRICAL POLITICAL NEWS WHICH IS DEMONSTRABLY FALSE OR WHICH IS MEANT TO INTENTIONALLY DECEIVE A CONSUMER.
OpenX	IN ADDITION TO THE FOREGOING REQUIREMENTS, SITES WHOSE CORE FUNCTION IS TO INCENTIVIZE USERS TO VIEW ADS, SITES THAT ARE PROXY SITES, AND SITES FEATURING THE FOLLOWING MAY NOT PARTICIPATE IN OPENX AD EXCHANGE:... • A PATTERN OF FALSE OR MISLEADING INFORMATION OR NEWS;...

[31]

Although Revcontent and OpenX have the highest volume of potential impressions from disinformation sites in this analysis, this traffic is unlikely to be a fundamental part of either platform's business, as only 4.05% of and 2.45% of potential impressions from NewsGuard-rated sites come from disinformation publishers on each ad tech system respectively. There are several smaller ad tech systems where traffic to disinformation publishers constitutes a much larger share of their business. For these ad tech systems, potential impressions from disinformation sites are greater than those from all other NewsGuard-rated sites. However, these ad tech systems only work with a limited number of media sites and have far fewer total potential impressions than the average available impressions (11.15 billion) of ad tech systems studied in this analysis.

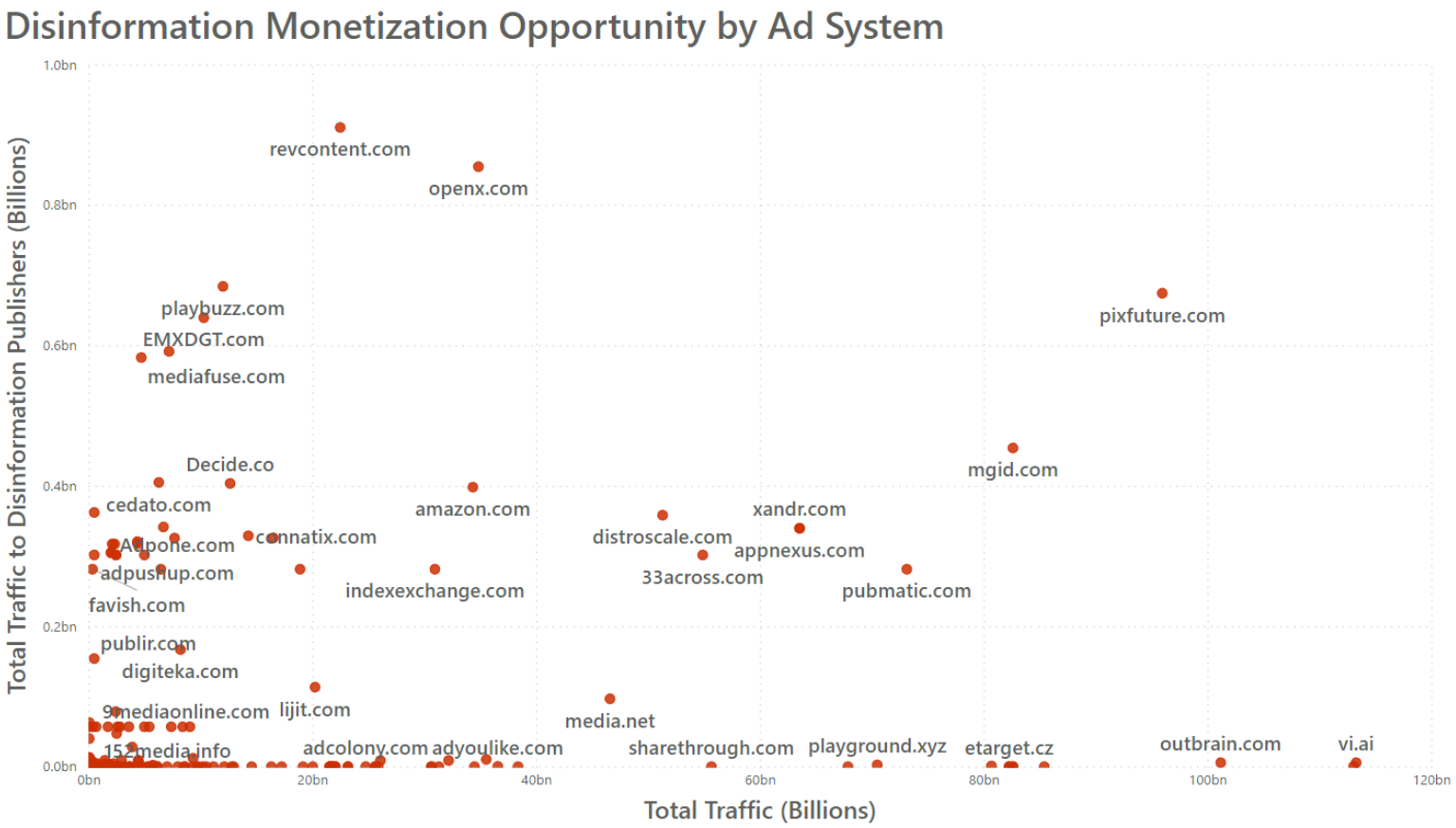
[31] Revcontent Policy, OpenX Policy

Figure 8

Ad System	Percent of Potential Impressions from Disinformation Publishers	Total Potential Impressions from NewsGuard Rated Sites (millions)
Stitchvideo.tv	100%	62.93
Vidillion.com	100%	56.73
Favish.com	80%	353
Fireflyengagement.com	71%	508.28
Marfeel.com	64%	61.94
Adpushup.com	59%	508.32

When plotting the traffic from disinformation sites against all other NewsGuard-rated sites for each ad tech system, Revcontent and OpenX are among the exceptions, as most ad tech systems have significantly fewer potential impressions from disinformation publishers. Across the entire marketplace, the average traffic to disinformation publishers on each ad tech system was only 67.1 million visits in 2022, with the vast majority of ad tech systems having no direct relationship with any known sources of disinformation. Only 35% of ad tech systems work directly with a disinformation publisher, and only 34 ad tech systems have disinformation publishers account for more than 5% of their potential impressions from NewsGuard-rated sites. When considering the total potential impressions available for sale across all 328 ad tech systems, disinformation publishers make up an average of only 2.9% of potential impressions on each ad tech system.

Figure 9



Despite the concerning and detrimental presence of disinformation publishers in the programmatic display advertising marketplace, the most important ad tech system in the world cannot be evaluated with the same level of scrutiny due to a lack of transparency. In 2019, the Competition and Markets Authority of the United Kingdom published a report on competition in programmatic display advertising in the UK, which found that Google was responsible for placing between 80-90% of display ads in the UK.[32] Reliable statistics for Google's market share of programmatic display advertising in the United States are not publicly available, but industry estimates place Google with a 39% global market share of digital advertising.[33] With this market share, Google's ad tech system is almost unavoidable for advertisers and publishers and is the most common ad tech system referenced in the ads.txt files of disinformation publishers. However, it is impossible to determine if these records are still active, as nearly 72.9% of all records in Google's sellers.json file are listed as 'classified' and have no information about the publisher associated with the account. This is in stark contrast to an average of 0.5% of records listed as classified by the other 328 ad tech systems evaluated in this analysis. The disparity between the rate of classified records in Google's sellers.json file and the industry average is the result

[32] Online platforms and digital advertising: Market study final report 2020, pg. 266
[33] Companies with largest share of digital advertising revenue worldwide in 2023

of Google's decision to classify records by default. Currently, Google requires publishers to 'opt in' to share their details, while most of the industry requires publishers to 'opt out'. Without access to the details of the publishers with valid accounts with Google, it is impossible to compare the potential impressions from disinformation sites available through Google to other ad tech systems.

VI. CONCLUSION AND RECOMMENDATIONS

The growth and monetization of online news media have helped traditional media outlets survive the decline of hardcopy. However, the programmatic advertising marketplace has also fueled the creation of a disinformation economy that incentivizes the creation of false narratives to generate revenue. Despite the industry's acknowledgment of the threat posed by this incentive structure, the existing tools and practices are insufficient to stem the tide of publishers willing to promote false narratives to turn a profit. Currently, publishers representing 81.47% of estimated traffic to known sources of disinformation have direct access to online programmatic advertising. Given the scale of the problem, more must be done to remove these publishers from the marketplace.

Advertisers are often unaware of all the locations where their ads are running, and the continued presence of disinformation publishers in the system represents a credible threat to their brands' security. In 2022, well-known advertisers such as Amazon, Hewlett Packard, Bing, and Verizon had their ads run on known sources of disinformation that publish stories about political misinformation, health misinformation, and conspiracy theories. While the current brand security tools offered by ad tech systems, such as exclusion/inclusion lists, give advertisers some tools to avoid their ads running on objectionable publishers, these tools do not always include disinformation publishers or require advertisers to identify objectionable publishers themselves. Without the ability to completely audit their ad placements, advertisers are forced to trust ad tech systems to help them avoid placing their ads adjacent to objectionable content.

Many ad tech systems already recognize their responsibility to exclude this content from their platforms, as evidenced by policies prohibiting publishers of disinformation from their platforms. As of the end of 2022, only 35% of ad tech systems evaluated in this report have a disinformation publisher as a direct client, and these publishers only represent an average of 2.9% of all potential impressions available to ad tech systems. Despite the relatively low cost of removing these publishers, known sources of disinformation continue to appear in their sellers.json files, and ads continue to appear on many of these sites.

While 81.47% of traffic to disinformation sites is available for sale in the programmatic advertising system, these sites only represent an average of 2.9% of available impressions for NewsGuard-rated publishers. Revenue for ad sales to disinformation publishers is also likely a smaller proportion than 2.9% of traffic due to the lower average number of ads run on disinformation sites (3.46 ads) compared to trustworthy publishers (10.43 ads).

Previous calls for the industry to remove these sites have stressed the importance of demonetizing the creation of disinformation.[34] However, effective collective action by industry requires the largest players in the marketplace to participate. Google has a dominant market share in the programmatic display advertising marketplace and is the most common ad tech system in the ads.txt files of disinformation publishers. For this reason, Google plays a pivotal role in demonetizing disinformation and must be a leader in restoring trust in the online advertising marketplace.

Disinformation is a threat to public health, democracy, and business, and it will require ongoing efforts from advertisers, ad tech systems, and publishers to undermine The Disinformation Economy. This report makes the case that the relative cost of removing disinformation from the marketplace is low in comparison to the added benefit to brand security for advertisers and confidence in the online advertising industry.

Based on the findings of this report, The Carter Center and The McCain Institute have the following recommendations:

For Social Media Platforms

1. **Limit the sharing of posts containing links to known sources of disinformation from a single user.** Restricting sharing of posts links to known sources of disinformation reduces the virality of the post and reduces the number of clicks the link receives. WhatsApp already limits the number of direct message forwards to five to curb viral misinformation spread. When Twitter has barred direct retweets of false information, it has found a 29% decrease in content sharing.[35]

For Advertisers:

2. **Use Exclusion/Inclusion lists that consider the harm of disinformation sites when setting up your ad campaign with your DSP.** Exclusion/Inclusion lists reduce the threat of your ads appearing on sites that could harm the brand image. They also reduce the demand for impressions from sites that are excluded from your campaign and lower the revenue for those sites. While there may be other options, NewsGuard for Advertising provides up-to-date information about known sources of mis- and

[34] Working to Stop Misinformation and False News
[35] An update on our work around the 2020 US Elections

disinformation that can be used to create exclusion/inclusion lists to protect your brand.

3. **Check your DSP's policy on mis- and disinformation**. Some DSPs have policies prohibiting known sources of disinformation from appearing on their platforms. If you work with a DSP that does not have such a policy, contact your account representative and express the importance of not having your ads run on known sources of disinformation.

For Ad tech systems:

4. **Prohibit known sources of disinformation from opening accounts with your platform.** Known sources of disinformation represent a small portion of revenue for ad tech systems and a large threat to the brand security of advertisers. It is in the interest of the industry to prohibit these publishers from accessing the programmatic advertising system to protect advertisers and maintain credibility as responsible actors in the programmatic advertising ecosystem.
5. **Offer brand security tools that incorporate misinformation prevention.** Offering preset exclusion/inclusion lists for advertisers that exclude known sources of disinformation reduces the burden on advertisers to identify harmful sites for custom exclusion/inclusion lists and produces better ad campaigns that meet the expectations of advertisers that wish to avoid disinformation publishers.

For Google:

6. **Make public sellers.json records the default option.** Google currently requires publishers to opt in to sharing their details in their sellers.json file. This results in 72.9% of the records in their sellers.json file being classified, making it impossible for ad tech systems and advertisers to verify if most Google accounts in ads.txt files are accurate. The default classification of records undermines efforts to prevent fraud and makes it easier for disinformation sites to monetize their traffic.

For Publishers:

7. **Opt-in to sharing seller details on Google's sellers.json file.** If you use Google to sell ad inventory, opt to share details of your account to lower the rate of classified records on Google's sellers.json file. The high rate of classified records in Google's sellers.json file allows disinformation sites to appear less conspicuous in hiding their details by hiding in a sea of classified records instead of the 0.5% of classified records for the rest of the industry.

List of Ad tech systems Evaluated in this Report:

1	152media.info
2	33across.com
3	4strokemedia.com
4	4wmarketplace.com
5	9dotsmedia.com
6	9mediaonline.com
7	ad-alliance.de
8	Ad.Plus
9	adagio.io
10	adalliance.nl
11	adapex.io
12	adasta.it
13	Adcolony.com
14	Adform.com
15	adipolo.com
16	Aditude.io
17	adkaora.com
18	admanmedia.com
19	admatic.com.tr
20	admetricspro.com
21	admonkey.mobi
22	adnimation.com
23	adnuro.com
24	adocean-global.com
25	adops.com
26	adplay.it
27	Adpone.com
28	adpushup.com
29	adsinteractive.hu
30	Adsolut.in
31	adsparc.com
32	adstanding.com
33	adswizz.com
34	adtarget.com.tr
35	adtelligent.com
36	adtrue.com
37	adverty.com
38	adview.com
39	adways.com
40	Adyoulike.com
41	affinity.com
42	algorix.co
43	alliancegravity.com
44	alpineinteractivegroup.com
45	amazon.com
46	amitydigital.io
47	ampliffy.com
48	amxrtb.com
49	Andbeyond.media
50	aniview.com
51	answermedia.com
52	AOL.com
53	App-stock.com
54	appads.in
55	applovin.com
56	appmonet.com
57	Appnexus.com
58	ardenodemedia.com
59	arkadium.com
60	ascendeum.com
61	atlas5.co
62	audience.media
63	audiencerun.com
64	audienciad.com
65	Beachfront.com
66	Behave.com
67	betweendigital.com
68	bidmachine.io
69	Blis.com
70	brightmountainmedia.com
71	buysellads.com
72	buzzfeed.com
73	catapultx.com
74	Cedato.com
75	chartboost.com
76	civicscience.com

77	cleanmedia.net
78	clickio.com
79	concept.dk
80	concert.io
81	Connatix.com
82	connectad.io
83	connekt.ai
84	consumable.com
85	contentignite.com
86	Conversantmedia.com
87	cpmstar.com
88	Criteo.com
89	dailymail.co.uk
90	datacygnal.io
91	datawrkz.com
92	dblks.net
93	Decide.co
94	dianomi.com
95	digitalbloom.it
96	digiteka.com
97	display.io
98	Disqus.com
99	distroscale.com
100	durationmedia.net
101	dynadmic.com
102	dyntrk.com
103	e-planning.net
104	e-volution.ai
105	elementaltv.io
106	EMXDGT.COM
107	engageya.com
108	entravision.com
109	Eskimi.com
110	etarget.cz
111	etarget.sk
112	evolutionadv.it
113	exmarketplace.com
114	ezoic.ai
115	ezoic.co.uk
116	factor-eleven.de
117	fatchillimedia.com
118	favish.com
119	feedad.com
120	Filmzie.com

121	fireflyengagement.com
122	firstimpression.io
123	flashb.id
124	forebase.com
125	foxpush.com
126	freegames66.com
127	gamoshi.io
128	getmediamx.com
129	gitberry.com
130	goodmove.media
131	gotchosen.com
132	groupm.com
133	grv.media
134	Gumgum.com
135	hbagency.it
136	headerlift.com
137	hoopladigital.co.uk
138	houseofpubs.com
139	hubvisor.io
140	impactify.io
141	Improvedigital.com
142	IndexExchange.com
143	Infolinks.com
144	Inmobi.com
145	innity.com
146	inskinmedia.com
147	Insticator.com
148	interdogmedia.com
149	invidi.com
150	ironsrc.com
151	italiaonline.it
152	itn-digital.com
153	justpremium.com
154	kargo.com
155	kiosked.com
156	kubient.com
157	kueez.com
158	lemmatechnologies.com
159	lgads.tv
160	lifestreet.com
161	Lijit.com
162	Limpid.tv
163	LiveIntent.com
164	lkqd.com

165	lkqd.net
166	longitudeads.com
167	luponmedia.com
168	madvertise.com
169	marfeel.com
170	mars.media
171	mcanvas.com
172	Media.Net
173	mediafuse.com
174	mediasquare.fr
175	mediatradecraft.com
176	mediavine.com
177	meitu.com
178	mgid.com
179	mintegral.com
180	minute.ly
181	Minutemedia.com
182	missena.com
183	mmpww.com
184	mobileapplied.com
185	mobilefuse.com
186	mobupps.com
187	movingup.it
188	mso-digital.de
189	Nativo.com
190	netlink.vn
191	netricsales.com
192	newormedia.com
193	Nextmillennium.io
194	nglcollective.com
195	nglmedia.com
196	nobid.io
197	novoroll.com
198	obox.group
199	oboxmedia.com
200	oko.uk
201	onetag.com
202	Onomagic.com
203	OpenX.com
204	opera.com
205	opinary.com
206	optad360.com
207	optidigital.com
208	optimanetwork.com
209	orangeclickmedia.com
210	orka.tv
211	Outbrain.com
212	Pangleglobal.com
213	pepsia.com
214	pixfuture.com
215	piximedia.com
216	playbuzz.com
217	playground.xyz
218	playwire.com
219	plista.com
220	pmc.com
221	pokkt.com
222	projectadv.it
223	proper.io
224	pubgalaxy.com
225	pubgenius.io
226	publift.com
227	Publir.com
228	publisher1st.com
229	publisherdesk.com
230	PubMatic.com
231	pubtech.ai
232	pubwise.io
233	purpleads.io
234	quantumdex.io
235	Qwarry.com
236	r2b2.io
237	reklamstore.com
238	relappro.com
239	resetdigital.co
240	revcontent.com
241	richaudience.com
242	roimediaconsultants.com
243	rtbsape.com
244	seedtag.com
245	selectmedia.asia
246	Sharethrough.com
247	shemedia.com
248	showheroes.com
249	Smaato.com
250	smartframe.io
251	SMARTSTREAM.TV
252	smrtb.com

253	sonictwist.media
254	sortable.com
255	spacefoot.com
256	Spot.IM
257	Spotxchange.com
258	sspx.tech
259	start.io
260	startapp.com
261	stitchvideo.tv
262	stnvideo.com
263	streambidmedia.com
264	Stroeer.com
265	stroeer.de
266	sunmedia.tv
267	symplr.de
268	Synacor.com
269	taboola.com
270	tagdeliver.com
271	talksmedia.it
272	tappx.com
273	target-video.com
274	Telaria.com
275	theglobeandmail.com
276	themediagrid.com
277	themediasense.com
278	themoneytizer.com
279	theplacetobid.fr
280	thisisdax.com
281	traffective.com
282	trioninteractive.com
283	triple13.io
284	Triplelift.com
285	tritondigital.com
286	trustx.org
287	truvid.com
288	tumblr.com
289	twiago.com
290	udmserve.net
291	undertone.com
292	united-internet-media.de
293	unity.com
294	unity3d.com
295	valuad.io
296	valueimpression.com
297	vdo.ai
298	venatus.com
299	venatusmedia.com
300	vi.ai
301	vidazoo.com
302	vidcrunch.com
303	vidillion.com
304	vidoomy.com
305	viewdeos.com
306	Viously.com
307	vitor.media
308	vlyby.com
309	Vrtcal.com
310	waardex.com
311	walletcircle.co
312	waytogrow.eu
313	webads.eu
314	welect.de
315	wemass.com
316	westseven.media
317	wideorbit.com
318	wunderkind.co
319	Xandr.com
320	xumo.tv
321	xymatic.com
322	Yahoo.com
323	yeahmobi.com
324	Yieldlab.net
325	yieldlove.com
326	yieldnexus.com
327	yobee.it
328	zeststack.com