A Selection of Final Projects from the Stanford Internet Observatory’s Online Open Source Investigation Course

Stanford Internet Observatory
February 8, 2022
Contents

1 Introduction 2

2 TikTok on the clock: A call for increased urgency in researching the spread of misinformation and disinformation on TikTok 2
   2.1 Key findings 2
   2.2 Introduction 2
   2.3 Accounts with inauthentic attributes 3
   2.4 An absence of labeling on state-controlled media 6
   2.5 The spread of misinformation through sound 6
   2.6 The spread of misinformation during time-sensitive events 7
   2.7 Conclusion 8

3 A case study of misinformation on campus: Biden’s visit to Stanford 10
   3.1 Tracking the narrative 10
   3.2 Surveying students 13
   3.3 Areas of further research 15

4 Telegram analysis & immigration in Belarus 16
   4.1 Introduction 16
   4.2 Methods: Identifying channels 16
   4.3 Results 17
   4.4 Challenges and future work 19

5 Misleading health insurance offerings promoted through Google Paid Search 20
   5.1 Overview of findings 20
   5.2 Methods 20
   5.3 At least one current search result implicated in FTC lawsuits 21
   5.4 Bait-and-switch data grabs 25
   5.5 Challenges and conclusions 28

6 QAnon on Tumblr 29
   6.1 Key Findings 29
   6.2 Introduction 29
   6.3 #QAnon vs #wwg1wga 30
   6.4 Crossposting 31
   6.5 Connection to QAnon communities on other platforms 33
   6.6 Trends among QAnon Tumbrls 33
   6.7 Liberal QAnon in Spanish: Spainonymous 36
1 Introduction

In fall 2021, the Stanford Internet Observatory offered the fourth iteration of its Online Open Source Investigation course. The class covers strategies for investigating content on social media, cryptocurrency transactions, and more. Throughout the quarter students work on an open source investigation into the topic of their choosing. We periodically published projects from the course, including an investigation called “Who Are the President of Guinea’s Facebook Trolls? The Blurry Line Between Modern Campaigning and Coordinated Inauthentic Behavior” and a two-part investigation into inauthentic editing on Wikipedia (part 1; part 2). These investigations were covered in Bloomberg and Time Magazine respectively.

In this report we are publishing five student projects from the fall 2021 quarter. The projects investigate inauthentic behavior on TikTok; misinformation on Stanford’s campus; Telegram activity in Belarus; health insurance scams that run advertisements on Google; and QAnon content on Tumblr. Contact information for authors is at the bottom of each write-up.

2 TikTok on the clock: A call for increased urgency in researching the spread of misinformation and disinformation on TikTok

Lila Shroff and Kyla Guru

2.1 Key findings

• Unlike other social media platforms, TikTok does not label content affiliated with known state-backed media channels.

• TikTok's emphasis on remixing sound with media encourages the spread of misinformation through audio. This is unique from many of its peer platforms where text and image vectors are the primary means for misinformation spread.

• In our investigation, we discovered at least one group of inauthentic accounts posing as human users. While some of these inauthentic accounts have already been banned by TikTok, these accounts still contribute to a user’s follower and following counts.

2.2 Introduction

TikTok is one of the fastest-growing and most widely used social media platforms globally and its platform design creates an environment ripe for the spread of mis/disinformation. Users are served content from creators they do not follow or know in real life, content can go viral even when created by users with little credibility, and remixing and manipulation of media is inherent to the medium.
A user with no history on the platform may post an intentionally misleading video and reach millions of people in a matter of hours. Beyond viewing, liking, and sharing videos, as is done on other platforms, users may also “duet a video”—creating a video remix of an existing TikTok. The problem is further exacerbated by the sheer number of channels through which information is communicated (video, audio, comment, sound, etc.), and that some research suggests individuals are more likely to believe mis/disinformation that spreads through video than audio or text.

For our research, we set out with the goal of performing a holistic examination of the ways mis/disinformation is currently spreading on TikTok, primarily by using two methods for research. The first involved cross-platform examinations in which we found content and accounts that had already been flagged by platforms such as Facebook and Twitter, and searched for the presence of affiliated content or entities on TikTok. Our second research method involved deliberately training the recommendation algorithm of a new TikTok account created for this research project to suggest intentionally misleading and/or polarizing content.

In the following sections, we will outline with more specificity the areas of TikTok in which we found consistent issues and believe warrant further research, including:

1. Accounts with Inauthentic Attributes
2. An Absence of Labeling on State-Controlled Media
3. The Spread of Misinformation through Sound
4. The Spread of Misinformation during Time-Sensitive Events

2.3 Accounts with Inauthentic Attributes

In our investigation, we identified a set of suspicious accounts all following another account claiming to be linked to Russia Today (Image 1). There is reason to believe that these accounts appear to be impersonating human beings that do not exist.
Figure 1: Left: @russia_today_24 is a TikTok account with suspicious followers that demonstrate attributes of inauthentic accounts. While @russia_today_24 purports to be affiliated with RT, a Russian state-funded media channel, this is itself contestable, as the account has no currently posted content for verification and only a cryptic message in its bio. The accounts begin to share many similar attributes including date of creation, type of content posted, and username.

Many accounts following @russia_today_24 have usernames comprised of similar length alphanumeric strings (Figure 2). Of the suspicious accounts shown in Figure 2, there are two types. The first are accounts with no profile photos that have been banned by TikTok. The other accounts have profile photos and appear not to be banned. The profile photos either appear machine-generated or make repeated use of the same stock images. These accounts were all created around October 2020, post stock video content with seemingly unintelligible captions, have zero plays on most videos, follow between thirty to a few hundred similar accounts, have few (if any) followers themselves, and often have similar watermarks in the lower right-hand corner of videos.
Figure 2: Left: An account following @russia_today_24 that appears to be banned. The majority of the accounts following @russia_today_24 are also banned. Center: @disbio7forre is an account following @russia_today_24 that appears inauthentic and at the time of the investigation had not been banned. Barely any videos have been watched and the account has no followers and a seemingly nonsensical username. Right: @disbio7forre's profile photo appears machine-generated. The earrings on either side of the face are not symmetrical.

We suspect the majority of the accounts following @russia_today_24 were previously identified as being inauthentic and removed accordingly. However, as shown by the remaining accounts like @disbio7forre and the images of other accounts below, the removal was not comprehensive.

Figure 3: Note the visual similarities between the above four accounts, all of which follow @russia_today_24 and appear inauthentic. Left: @zhuravlovbf1975. Center left: @ryabovzjj1989 Center right: @shilovsrd1997. Right: @orehovadalvina.
TikTok removed many of these accounts, but the banning of follower accounts that violated community guidelines did not subtract from “followers”/“following” counts for the original @russia_today_24 account. For instance, @russia_today_-24 appears to be following ten accounts. However, if you click on their profiles, all ten of these accounts have been banned. We suggest TikTok update this count of “followers”/“following” totals to subtract banned accounts to provide audiences with an accurate estimation of the true reach of an account. Otherwise, these inauthentic accounts may continue to achieve goals of lending legitimacy to suspicious accounts, despite already having been banned.

2.4 An absence of labeling on state-controlled media

While Facebook, Twitter, and YouTube have made efforts to label accounts affiliated with partially or wholly state-controlled media channels, TikTok does not provide any form of labeling for state-controlled media on the platform. These inconsistencies in state-controlled media labeling were pointed out by University of Washington researchers in a comprehensive report preceding the 2020 US Presidential election. TikTok has not changed its policy since the report’s publication.

Research has shown these labels to be effective in counteracting foreign misinformation. The following images show a sample of how the same media channel appears on TikTok (unlabeled) vs. elsewhere (labeled).

![Figure 4: Left: @rt.news on TikTok. Center: TikTok content from @rt.news questioning Biden's ability to run for a second term. Right: An English language RT account on YouTube is labeled as state-affiliated.](image-url)

2.5 The spread of misinformation through sound

In addition to video creations, TikTok users are encouraged to create and customize their own audio bytes. In some instances, audio is intentionally layered
onto unrelated film footage to create misleading narratives.

In October 2021, a reporter mistakenly claimed that a NASCAR crowd was chanting “Let’s Go Brandon” in support of competitor Brandon Brown, when actually the audience was chanting “F*** Joe Biden.” The moment quickly turned into a meme and “Let’s Go Brandon” became code for insulting Biden. On TikTok, “F*** Joe Biden” audio from the NASCAR event was swiftly layered over footage of crowds at Dunkin Donuts, Disneyland, Hershey’s Park, and football games. The result is a set of misleading videos that imply large crowds nationwide are chanting insults at the President (these videos received 30K-140K likes).

![Figure 5:](image)

Figure 5: Left: The video posted by @notrub303 shows a crowd gathered at Disneyworld chanting “F*** Joe Biden.” Center: “F*** Joe Biden” audio is superimposed on a video of a crowd near Hershey’s Park. Right: Comments from the same video in the center image demonstrate crowdsourced fact-checking.

### 2.6 The spread of misinformation during time-sensitive events

The history of social media is a long narrative of digital interactions spilling out into the real world and the case of TikTok is no different. A timely example is the massive amount of COVID-19 related falsehoods that exist on the platform. It is worth noting that TikTok does label many videos containing vaccine mis/disinformation, though there are still many examples of content that evades this labeling.
Figure 6: Left: A post by @dross305fucwitit, purporting that the vaccine was developed by Bill Gates and is designed to “transform your DNA.” Center: A misleading article posted by @acusa1. Right: Video posted by @patriotwildflower1 appears to claim that an abandoned Walmart building is used by the government to administer these vaccines with some “ulterior motive.” (@dross305fucwitit and @patriotwildflower1 appear to have been removed by TikTok in the period between the research and publication of this piece. However, when these accounts are searched for on TikTok, affiliated, inflammatory content continues to surface). None of these posts carry TikTok’s misleading content label.

Other examples of TikTok being used to catalyze real-world action include the case of The Republican Hype House sharing incorrect election dates with young voters, and military officers in Myanmar using TikTok as an avenue to threaten individuals protesting the military coup.

2.7 Conclusion

This represents only a sliver of potentially problematic content and behavior on TikTok. Scrolling through our new TikTok account “For You Page” revealed, and continues to reveal, an overwhelming number of media and accounts that warrant exploration, and yet TikTok’s information ecosystem remains deeply under-researched. If you leave with one takeaway from reading this piece, let it be this: TikTok must prioritize misinformation and disinformation research with greater urgency and focus.

Improving the informational health of TikTok stands to benefit users and company alike. Individual users benefit from a better environment for communication, and the company, if proactive, may be able to avoid the fate of its peer platforms and the reputational damage they have faced in their devolutions into post-truthism.

Lila Shroff (lilashroff@stanford.edu, @lilashroff) is a first-year undergraduate Stanford student interested in creating a healthier internet and better understanding the forces that shape human behavior online. She is also passionate about creative
writing and spends much of her time dreaming up fictional worlds. Kyla Guru (kylaguru@stanford.edu, @GuruDetective) is a second-year undergraduate Stanford student excited about the nexus of cybersecurity, law, and international affairs. She is fueled by the idea of reforming our education system through social entrepreneurship and believes that there is a world where the Internet is a safe place of connection and community for everyone.
3 A case study of misinformation on campus: Biden's visit to Stanford

Lena Han and Frances Schroeder

On October 7, 2021, Stanford students were buzzing with excitement. Following a memorial for former Secretary of State George Shultz at Memorial Church, tweets circulated about President Biden's presence at the service, and people even shared pictures of the POTUS in Main Quad.

But – Biden was never on campus that day. What happened? What can this instance tell us about information networks on campus?

Through investigation of the Biden narrative on social media and administration of a survey, we identified key features of misinformation spread at Stanford. Our main findings are:

- Our open source investigation shows that the Biden narrative started on Twitter.
- We conducted a survey of 30 Stanford students, and found that the narrative reached 70% of students in the survey, despite just 27% of students using Twitter.
- The Biden narrative's plausibility and alignment with confusing activity on campus helped it spread far more consistently than most misinformation threads on campus.
- Debunking misinformation is difficult, and made even harder by social media. Online, commentary around false narratives is frequently presented as a joke, which is hard (and awkward) to fact-check.

3.1 Tracking the narrative

The Biden story began with one tweet that immediately got traction across the Stanford twittersphere.
The creator retracted the statement by replying “THIS WAS A JOKE…” to their initial tweet (without deleting the tweet) 90 minutes later, but the damage was already done.

To track the discourse, we used TweetDeck (combining location and time filters, as well as keyword searches like “Biden AND campus”), personal recollection, and manual investigation of retweets and replies. Additionally, we searched for similar activity on Buzz, an anonymous social media app developed by Stanford students popular among underclassmen. These posts were aggregated onto a spreadsheet to search for patterns, and three types of posts emerged.

First, many tweets, including one by a student who wrote “JOE BIDEN JS [sic] ON CAMPUS???” simply expressed surprise that Biden was on campus. While fact-checking was attempted by both individuals and The Stanford Daily, social media algorithms likely continued showing users the more popular initial misinformation posts without the retraction.

Second, many posts posed jokes and commentary about Biden’s visit. Because these posts were only tangentially related to the event, they reinforced the narrative but did not invite fact-checking. For example, it feels inappropriate to fact check a tweet by one student: “Biden and Harris on campus - anyone doing a gathering to let them know they’re not doing much to help anyone’s communities?”
A third category of posts circulated an alleged picture of Biden in Main Quad. This “photo evidence” was quickly disseminated through social media networks including Twitter, Buzz, Snapchat, and Instagram. In general, the quick spread of commentary from one platform to another limited the strength and reach of fact-checking efforts.
The narrative’s remarkable success was boosted by students’ observations of unusual activity on campus related to the high profile memorial service—for example, large barriers set up at the entrance to Memorial Church that disrupted many students’ bike commutes. Students were likely looking for any explanation for the strange activity. Furthermore, students could verify that other notable political figures attended the Shultz memorial, giving the narrative plausibility.

3.2 Surveying students

To validate and contextualize our social media observations, we surveyed a convenience sample of 30 undergraduate and graduate Stanford students about their social media activity and knowledge of Biden’s presence on campus before debriefing them on our project and misinformation. Some notable results are displayed below.
Figure 10: Despite most of our research taking place on Twitter, only 26.7% of respondents frequently use Twitter.

Figure 11

Figure 12: 62.5% of respondents heard of the narrative through word of mouth.
A primary limitation of our research is that our network as seniors on campus is restricted. This was reflected in our survey respondents, who were not representative of the entire student population.

Additionally, we could only access tweets of public accounts and private accounts we already followed, likely missing many private tweets.

### 3.3 Areas of further research

The Biden case study highlighted how being in a closed college campus network can exacerbate some issues with misinformation spread, as unreliable word of mouth accounts can mix with social media to propagate narratives. At the same time, in this smaller community, we each have greater ability to identify and influence false narratives. At the end of this project, several questions remain: what would be an effective strategy to combat misinformation on campus? How prevalent is misinformation on campus? What is our responsibility as students in situations of misinformation spread?

*Frances Schroeder (fschroe@stanford.edu, @franceschroe) is a senior at Stanford studying Symbolic Systems and International Relations. She is interested in the intersection of national security and technology. Lena Han (lahan@stanford.edu, @_lena_han) is a senior at Stanford studying Economics and Public Policy with a focus on urban policy.*
4 Telegram analysis & immigration in Belarus

Amy Dunphy and Kate Davidson

4.1 Introduction

Belarus has been the center of recent controversy, including fall 2020 protests against President Lukashenko's disputed reelection, and a 2021 migration and border crisis allegedly manufactured by Lukashenko in response to EU sanctions in which asylum-seekers crossed the Belarus-Poland EU border. Belarus’ government may be engaging in coordinated disinformation regarding political controversies. A Facebook takedown attributed many accounts that were generating criticism of Poland for its handling of the border crisis to the Belarusian KGB. A significant fraction of domestic conversations about these events occurs on Telegram, often referred to as the dominant platform in Belarus for political discussion.

We examined popular opposition and pro-government Belarusian channels and narratives in the 2021 immigration crisis, working to build out broadly applicable Telegram analytics tools.

- We identified and tested Telegram analysis tools, which we used to investigate keyword frequency and cluster groups based on interactions; these tools have the potential to be used for a more thorough analysis of information spread across the platform
- We found that top pro-government Telegram groups used a shared rhetoric about the 2021 migration crisis, emphasizing unexpected issues like international humanitarian law

4.1.1 Telegram

Telegram is structured as a set of discoverable channels into which a single user posts, and many users may view and comment. Information on users and trends is difficult to obtain. Countermeasures prevent web-scraping of potentially sensitive data (such as lists of posts in a channel by a user). Telegram resists moderation and has more lax policies than other similar social media platforms. As a result, illegal behavior, fringe viewpoints, disinformation, and conspiracy theories have proliferated across the site.

This makes Telegram interesting, though challenging, for social media research. We sought to visualize Telegram discussions in Belarus and elsewhere.

4.2 Methods: Identifying channels

We used collections of significant Belarusian Telegram groups assembled by the DFRLab to identify channels, verifying their continued prominence a year later. We then used TGStat.com in order to identify any other channels with current high
engagement in Belarus. We used **Telethon** to scrape all text or image messages posted in a particular channel over specified periods (Figure 14).

![Figure 14](image)

**Figure 14:** Automated message scraping with Telethon, using a Python script to read back the most recent message in a channel

### 4.3 Results

#### 4.3.1 Channel clustering

Channels frequently share messages from larger channels. We hypothesized that channels would mostly share from channels with similar viewpoints, and compiled an interactive network of popular Belarusian political channels (Figure 15).

![Figure 15](image)

**Figure 15:** Channel network plot, which draws a line between any two channels which have posted the same message in the last month. Different lines have different weights (i.e. numbers of shared messages).

As expected, channels mostly shared from channels with the same political slant (opposition in red, pro-regime in green). @zerkalo_io, shown in blue, represents a notable exception. With over 400,000 members, this independent news channel migrated to Telegram after the government decertified it during the 2020 protests.
4.3.2 Narratives

Pro-regime channels typically had more consistent narratives, likely because Lukashenko’s government is better positioned to spread a unified narrative.

Pro-regime channels focused on international law and criticizing the EU, alleging that the rights of asylum seekers were being violated and the position of Western countries was hypocritical (Figure 16). This rhetoric likely represents a response to Western criticism of Belarus over the suppression of pro-democracy protests, particularly the grounding of an international flight to arrest dissident journalist Roman Protasevich. These channels use the term “беженцы” (meaning refugees) over the term “мигранты” (migrants) which is more popular among anti-regime groups [Figure 6]. This emphasis on human rights is what initially interested us about pro-regime rhetoric. Given the historic antipathy towards immigration in Belarus, this narrative likely reflects intentional appropriation of Western narratives.

We examined the frequency of keywords across opposition and pro-regime channels (Figure 17). Opposition channels vary more than pro-regime channels. Some opposition channels, like NEXTA, are functionally news outlets. Others, like cpartisans, are more radical, less focused on the international angle, and more focused on violence and fringe narratives.
4.4 Challenges and future work

4.4.1 Attribution

We were unable to attribute anonymous groups or identify inauthentic behavior, largely due to the absence of transparency about admin accounts, account creation dates, and even admin locations.

@Zheltyeslivy is a highly prominent, unattributed Telegram channel that posts pro-regime messages and engages with other pro-regime channels. It voluntarily lists associated, non-Telegram accounts in the description of the channel, including a website, an email, and a TikTok (@zheltye_slivy). Though the phone number and email did not yield any hints, the connected social media accounts offer a possible avenue for further investigation.

4.4.2 Automation improvements

The ability to read images—for instance, by downloading images (easy through Telethon), feeding them through an image-to-text converter (such as google translate), and returning the text as message information—would significantly improve future investigations. Access to that data would significantly enhance the resolution of our analysis as many keywords are embedded in images, and more data would allow us to better understand trends.

Amy Dunphy (adunphy@stanford.edu) is a senior at Stanford studying Electrical Engineering, with a focus on dynamics of misinformation spread. Kate Davidson (kdavids@stanford.edu) is a master’s student at Stanford in Russian, East European, and Eurasian Studies.
5 Misleading health insurance offerings promoted through Google Paid Search

Leo Glikbarg, Eli MacKinnon, Eli Wald, and Songchen Yao

5.1 Overview of findings

We set out to investigate the prevalence and types of health insurance scams that rely on Google Paid Search ads to reach their victims. We discovered that businesses affiliated with known scammers have used Google Search ads as recently as November 2021.

Deceptive health insurance websites that ranked high in Google results tended to fall into two categories:

1. Lead generators for (junk insurance) “discount plans”: These sites act as magnets for identifying health insurance buyers who they then target with low-quality and expensive plans that are not compliant with the American Care Act (ACA).

2. Bait-and-switch data grabs: These companies publish web pages to produce “custom quotes” for health insurance. Their intrusive data-collection policies and the fact that quoted rates remain static regardless of questionnaire input indicate that their priority is to resell the personal data they’ve collected.

5.2 Methods

We established a list of Google searches by analyzing Google Trends data for popular queries similar to “California Health Insurance”. We used these search terms to conduct our own queries, tracking results that did not direct to ACA-approved marketplaces or major insurers. We analyzed these sites in terms of their own copy (including searching to see if the copy was “borrowed” from another site), design, and social media footprint.

Finally, we reached out to these sites of interest directly by phone to get quotes, inquire about their services and learn more about their business models and data-privacy practices.
5.3 At least one current search result implicated in FTC lawsuits

We found that obamacare-plans.com, a third-party lead generator for a firm subject to a 2018 FTC lawsuit, was one of the top Paid Search results as of November 2021. The FTC has a history going back to 2010 of customer awareness and legal actions against “medical discount scams”. In November 2018, the FTC filed a lawsuit against Simple Health LLC. In a press release, the FTC stated that Simple Health LLC would market a plan described as “comprehensive” costing consumers.
near “$500 per month”. The plan itself “was actually a medical discount program” that “effectively left consumers uninsured.”

Figure 19: Left: FTC screenshot of Craigslist ad from Simple Health LLC operators hiring sales agents. Right: Current homepage of Simple Health operated site, now placed in receivership.

The FTC filing indicated that Simple Health and its affiliates operated the following first-party lead generator sites:

- Premiumhealthquotes.com
- Healthinsurance4me.com
- Trumpcarequotes.com
- Usamedsupp.org
- Hbcquotes.direct
- Myobamacareapplication.com
- Usahealthinsure.net
- Americanhealthinsure.com
- Medigapquote.com
- Freedomcarequotes.com
- Supremehealthplans.com
- Americashealthcareadvisors.com
- Healthinsurancedeadline2018.com
The archived pages feature very similar copy writing to each other. These first-party lead generators also tend to use the logos and icons of reputed healthcare providers.

![Figure 20: Trumpcarequotes.com Wayback machine capture, 11/16/2018](image1)

The FTC's latest press release on Simple Health indicates that it has settled with Simple Health's CCO in exchange for her cooperation.

Our research found that at least one third-party (i.e., not operated directly by Simple Health) lead generator connected to Simple Health is still online.

![Figure 21: Supremehealthplans.com wayback machine capture, 8/9/2018](image2)
In November 2021, we ran healthcare related queries such as “California Health Insurance” on Google and found that obamacare-plans.com was still available as a promoted search result via Google Paid Search.

Using CrowdTangle shows that this site has been shared by a few high-profile political and media-affiliated Facebook pages that may not have been aware that the site was not an approved ACA marketplace:
When we called the number listed on obamacare-plans.com on November 11, 2021, we received a quote for a plan offered through a provider named “Altrua,” which the agent claimed was affiliated with Aetna. The rate quoted by the agent on the day of our call was $367 per month. The agent warned it would go up by $100 if we waited to enroll. Using expiring offers to create a sense of urgency has been documented as a common “social engineering” tactic used in scams as well as phishing attacks in the healthcare space.

5.4 Bait-and-switch data grabs

One category of sites acts as a broad filter for collecting and reselling data for marketing purposes. Mymedicare.info, for instance, directs users to either fill out a survey on their site or talk with an employee directly on the phone. Users are asked to give their home address, employment history, health history, income, SSN, and other personally identifiable information. The quote provided is a static page, which does not change with any of the information provided.
Figure 26: A screenshot of Mymedicare.info/complete. The “View My Quote” buttons are linked to the hompages of the listed orgs.

This practice is made clear by the terms of service including a non-exhaustive list of hundreds of companies mymedicare.info provides user information to.
Mymedicare.info is part of a network of sites run by Excel Impact LLC. Through Google Tag Manager Id searching on Passive Total RiskIQ, the sites listed on the Excel Impact website, and the Better Business Bureau page for Excel impact, we assembled the following list of sites controlled by Excel Impact:

- AA Media Inc.
- AARP
- Absolute Health Agents
- AccuQuote
- Acquisition Technologies, LLC
- Admaric Insurance Agency, Inc.
- AdNet, Inc.
- Adrea Rubin Marketing, Inc.
- Advocate Health LLC
- Ad Practitioners LLC
- Aetna
- Affluent Ads, LLC
- Affordable Health Group Inc.
- AGENCY INCLINE, LLC
- Agentra Healthcare
- Agile Health Insurance
- AIG
- Akify, Inc.
- Allera Healthcare
- All Web Leads
- Alliance321, LLC
- Allied Insurance Partners
- Allied Insurance
- Allstate
- All in Marketing Inc.
- Alpine Digital Group, Inc.
- Amac
- America’s Health Center, Inc.
- American Classified Services
- American Continental
- American Health & Life Associates LLC
- American Income Life Insurance Company Family
- American Insurance Agencies Direct, LLC
- American Insurance Organization
- American Republic
- Americo Life, Inc.
- AmeriLife
- Amigos BPO LLC
- Angelic Marketing Group
- Anthem
- AP of South Florida, LLC
- Apollo Interactive, Inc.
- Applied General Agency, Inc.
- ARROYO MEDIA
- Assurance IQ, Inc
- Assuran
- Assured Life
- Astoria Company
- Atlantic Blue Media
- Atlantic Health Advisors LLC
- Atlantis Health Group LLC
- AutoSmart Insurance Agency
- Avenda Management, Inc.
- Avenge Digital, LLC
- AXIOM EQUITY, LLC
- Bankers Hill Insurance
- Bankers Life & Casualty
- Bankrate
- Bantam Connect
- Benefit Advisors
- Benefits Network, Inc.
- Benefath, Inc.
- Best Obamacare
- BETTER HEALTH CHOICE, LLC
- BIG Insurance
- Bilp Marketing
- Blueberry Insurance Agency, LLC
- Blue Summit Insurance Solutions
- Blue Wing Ads, LLC
- BOOMSOURCING LLC
- BOOST HEALTH INSURANCE AGENCY, INC
- Call Trader LLC
- Bridgenet Insurance Agency LLC
- Bright Health Solutions
- C3 Data, LLC
- Call Trader LLC
- Caremore

Figure 27: A portion of the listed companies that Excel Impact says they may sell users data to. Source
5.5 Challenges and conclusions

A lack of transparency about prior search results and Paid Search data presents challenges to open source investigative researchers. Without first-party archiving of search results, we resorted to the Internet Archive to find prior results for common search terms. Relying on someone in the right place having archived search results for a particular term is not an efficient or comprehensive approach. Finding a way to track top search results for a given set of terms over some period of time would prove useful to future investigations and research.

Though we tried to systematically select a set of terms and a set of resulting sites, we believe that further research can refine our approach. We look forward to seeing more research in this space.

Leo Glikbarg (lglik@stanford.edu, @LeoGlikbarg) is a computer science and international relations student at Stanford with a strong belief in the power of technology to improve the world. He builds rockets, robots, radios, and other things that start with ‘r’ for fun. Eli MacKinnon (elimac@stanford.edu) is a second-year master’s student at Stanford studying cybersecurity and cyber policy, with a focus on digital privacy. Eli Wald (MS, 2023) is currently studying computer science with a specialization in computer and network security living in San Francisco. His interests include safety in systems engineering, open-source investigation, and speculative fiction. You can follow his work at https://blog.diffy.info and @DifficultHell. Songchen Yao, Stanford Class of 2023, is a Chinese expat loving economics.
6 QAnon on Tumblr

Mishaela Robison

6.1 Key Findings

• Unlike other social media sites, Tumblr appears to have made no effort to address or curtail QAnon content on their platform.

• While the most popular Tumblr content tagged as #QAnon largely contains content opposed to the group, popular posts using more “specific” QAnon tags, such as #wwg1wga, chiefly feature support for, and narratives common among, QAnon.

• Both pro-QAnon and anti-QAnon content typically do not originate on Tumblr, instead the content is crossposted or screenshotted from other social media platforms.

• While QAnon content on Tumblr directs users to other sites, QAnon communities on other sites do not direct users to Tumblr.

• Accounts posting QAnon content vary widely: while some uniformly share far-right themes, others intersperse QAnon content with explicit imagery or feature far-left content.

6.2 Introduction

By most metrics, Tumblr is a dying social media platform. After a 2018 ban on pornography, explicit images, and “female-presenting nipples,” the site’s already-dwindling userbase decreased significantly. Shifts in the company’s ownership and the overall social media landscape have often left the site as an afterthought in investigative circles.

Nevertheless, Tumblr deserves analysis. The site continues to maintain an active userbase, particularly surrounding fandoms, popular culture, and activism. In recent years, these numbers have seen a resurgence thanks to younger users: 61% of new accounts and 48% of active users belong to Gen Z. It also provides a unique case study for the spread of QAnon content; while hashtags such as “QAnon” and “wwg1wga” are flagged on other social media platforms, my research finds that QAnon activity continues uninhibited on Tumblr while encouraging QAnon content on other platforms. I also found a substantial amount of anti-QAnon content among the QAnon tag.
6.3 #QAnon vs #wwg1wga

In a qualitative analysis of the 50 most popular posts tagged with #QAnon (as identified by Tumblr’s “most popular” feature,) 47 were anti-QAnon and 0 were pro-QAnon, while 3 were unrelated. Anti-QAnon content made fun of or directly opposed QAnon adherents, often taking the form of screenshots from other platforms.

Content tagged with more “specific” QAnon-related hashtags (eg. #wwg1wga, #16+1) however, tells a different story. The 50 most popular #wwg1wga posts largely supported QAnon (34), though some contained anti-QAnon messages (10) or unrelated content (6.) Still, the most popular content tagged #QAnon receives more average engagement than the most popular content using more specific hashtags such as #wwg1wga. Tumblr does not publicly list the blogs that an account follows so it is not possible to determine the interconnectedness of QAnon blogs, but the most popular blogs did have overlapping “big fans” who would interact with their content frequently.
6.4 Crossposting

Regardless of sentiment, only a minority of QAnon content originated on Tumblr. Most of these posts take the form of images and videos, often linking either directly (posting a link to another site, most commonly Rumble, TikTok, or Instagram) or indirectly (a meme with clear watermarks) to other platforms.

Some of these watermarks point to social media pages connected to state-affiliated media, such as this post which contains the handle of “Soapbox Stand,” a channel affiliated with the Russian government which appears to be targeting young Americans. (While the account which shared this meme, Spainonymous, is not openly affiliated with RT or Soapbox and does not post their direct content frequently, it has indirectly shared RT content, as described below.)

Some popular text-based posts, while less common than images, contain copypasta circling around the Internet.

or Instagram) or indirectly (a meme with clear watermarks) to other platforms.
Figure 32: A Tumblr textpost tagged #QAnon opposing mask mandates and COVID-19 lockdowns, posted on August 11, 2020. Versions of the same post were also shared on Twitter nine days prior, with an article from a month earlier referring to the copypasta on Facebook.

Figure 33
6.5 Connection to QAnon communities on other platforms

Some accounts, such as the active Tumblr jayandamy, post direct links to their Telegram channel. When I sent the account a direct message, it responded with the link to their Telegram channel and did not respond further, despite being active on Tumblr since then.

Other accounts post hyperlinks to videos on other social media sites (ex. Bitchute, Rumble, and TikTok) without alleging personal connection to the content that they link. When I direct messaged Tumblr user “slickrickmaga555,” the account referred me to a Rumble channel.

Despite referrals to other sites, none of the top Tumblr posts for #QAnon, #wwg1wga, #save the children, or #16+1 promote other Tumblrs. An analysis of notable QAnon Telegram channels also found no links to Tumblr accounts, suggesting a unidirectional flow away from Tumblr.

6.6 Trends among QAnon Tumblrs

6.6.1 Right-wing Q: Slickrickmaga555

Tumblr identifies Slickrickmaga555 as the “top blog” using #wwg1wga. The account’s posts are pro-QAnon, right-leaning, anti-vaccine, pro-Trump, and anti-Democrat. Despite posting content since 2017, Slickrickmaga555’s 10 most-interacted posts were all posted between July and November 2021. The second and third most popular of these posts did not include tags, meaning they spread only through the reach of the account’s followers. The account appears to occasionally use some form of automation to post in rapid succession.

Slickrickmaga555 occasionally posts pictures of an Instagram account stick- rick555maga. The Instagram account posts almost exactly the same content as the Tumblr account, sometimes at the exact same time. In one post, the account appeared to risk suspension for violating Community Guidelines.
Figure 34: The slickrick555maga Instagram account. The name “Trick Jones” may refer to an offline identity or be a red herring (potentially an R&B artist with the same name).

Figure 35: Image posted at the same time (8:36 pm PST on Sunday, December 5, 2021) on both Slickrickmaga555 Tumblr and Slickrick555maga Instagram.
6.6.2 Q + erotica: n-e-w–y-0-r-k

N-e-w–y-0-r-k is another account that uses #wwg1wga and #16+1. As with Slickrickmaga555, n-e-w–y-0-r-k's popularity increased recently, skyrocketing between 2019 and 2021.

N-e-w–y-0-r-k mostly contains two types of content: QAnon/right-leaning political posts, and erotic photos of young women. These posts are blended in a bizarre cacophony: misinformation about vaccines followed by a sexually explicit gif and then a gif of a puppy.

N-e-w–y-0-r-k is by no means the only account to mix misinformation with erotica. Other accounts, such as viperdew similarly swap between such posts. Viperdew's account, which was taken down between the writing and publication of this article, contained slews of content reblogged from slickrickmaga555 interwoven with reblogged sexually explicit content (despite Tumblr's ban on such content,) as evidenced by the screenshot to the right.
6.7 Liberal QAnon in Spanish: Spainonymous

“Spainonymous” posts mostly in Spanish, often accompanied by an English translation. When translated to English, the account’s bio reads “Antifa. Lower class white European. Valencia Country,” indicating that the blog is run in Spain.

The account posts left-leaning content, supporting anti-fascist movements and the LGBT community. Spainonymous tags several types of content as #QAnon: pro-Antifa, anti-Biden, anti-police and anti-capitalist rhetoric, to name a few. Few of these posts directly relate to QAnon. Although claiming to live in Europe, Spainonymous posts almost exclusively about the United States, often critical of the government and police.

On occasion, Spainonymous posts content from the Russian state-controlled news organization RT, such as posting screenshots from Spanish-language RT articles while cropping the RT logo or a video of an attack with the RT watermark.

![Figure 37: A post from Spainonymous showing an article without any identifying features, next to the same article from the actualidad.rt.com website](image)

- Figure 37: A post from Spainonymous showing an article without any identifying features, next to the same article from the actualidad.rt.com website
Mishaela Robison (mishaela@stanford.edu, @michaelarobison) is a senior at Stanford studying the psychology behind the spread of misinformation on social media.
The Stanford Internet Observatory is a cross-disciplinary program of research, teaching and policy engagement for the study of abuse in current information technologies, with a focus on social media. The Stanford Internet Observatory was founded in 2019 to research the misuse of the internet to cause harm, formulate technical and policy responses, and teach the next generation how to avoid the mistakes of the past.