Profiting from the Pandemic

Moderating COVID-19 Lockdown Protest, Scam, and Health Disinformation Websites

Yung Au, Philip N. Howard, Project Ainita

SUMMARY

This data memo examines the infrastructural support for controversial COVID-19 websites that (1) protest public health measures such as lockdowns, (2) promote COVID-19 scams, frauds and profiteering, and (3) disseminate disinformation about public health. What hosting, functionality, and networking services do these controversial websites rely upon? We systematically use an open source toolkit to investigate a wide array of third-party and infrastructure services that generate revenue for technology firms from websites with content that are targets of takedowns or other forms of content moderation. First, we find that Google, GoDaddy and Cloudflare are among the single largest firm providing infrastructural support. Second, Google and Facebook are among the single largest firms providing a vast array of third party technology services. Finally, we find that websites utilize behavioral analytics, tracker systems, and cross-platform integration tools that connect them back to large technology firms in multiple ways. We demonstrate how firms up and down the technology stack profits from contentious COVID-19 websites, even after steps such as ad removals or content moderation.

INTRODUCTION

The COVID-19 pandemic is being exacerbated by campaigns against public health measures, such as face masks, social distancing, and lockdowns. There are significant COVID-19 scam websites selling fake cures and preventative measures. Other websites simply keep COVID disinformation in circulation. Major social media platforms often flag such content for moderation or remove it altogether from their platforms. Using a curated list of websites, we examine how these firms continue to enable contentious content through the back-end.

What third-party hosting, functionality, and networking services do these controversial websites rely upon? How are third parties generating revenue by supporting controversial content?

There are a variety of levels to the infrastructure that supports the web and are capable of moderation. For instance, at the first level is the open web which is accessible by anyone. Building on top of this are platforms which are technology-enabled content intermediaries. At the next level, cloud services provide access to resources on demand through remote computing servers, so clients do not need to own such infrastructures themselves. Content delivery networks (CDNs) offer geographically distributed servers to provide rapid delivery of content. Registrars are the accredited providers that handle website name registration. Finally, Internet Service Providers (ISPs) provide access to the network of devices that make up the internet, and all of these levels together make the "technology stack" that is our modern information infrastructure (see Online Supplement).[1]

It is important for Facebook, Instagram, and YouTube to take down problematic content. However, such actions do not always impact the revenue stream that accrues to these firms if they continue to provide infrastructure support. Moderation of the front-end may not have lasting impact unless there are parallel efforts to close off the back-ends that enable such content.

METHODS

We examine the back-end services that controversial websites rely upon. We use a variety of open source tools and shell scripting to run batch analysis. In particular, this memo examines the registrars, hosts, cloud services, CDNs, and the variety of third-party web-based technologies that websites use (see Online Supplement).

Successful websites, especially those integrated with social media or sales platforms, require a certain degree of technical skills and resources to operate. Likewise, networking is not as straightforward as with social media, where there are usually predefined sets of audiences. Steps involved in producing a website include purchasing a website name, registering it and finding a host. Next is creating the website's html code, implementing widgets for interactive elements, implementing analytics, ensuring the website is accessible, registering security certificates, considering search engine optimization and linking the website to the wider internet ecosystem. Webmasters must also maintain the security and service delivery of their websites, for example using CDN services, which requires a certain degree of technical knowledge.

The benefit of analyzing website infrastructure is that many of these processes are openly documented. In contrast, social media platforms restrict information on how they operate and support their users, and only provide data through highly curated APIs.[2]

We examine 120 websites, with 40 in each of the three categories: lockdown protest websites in the US, COVID-19 scam, fraud, and profiteering websites, and COVID-19 disinformation websites. The websites included in these curated samples are not necessarily illegal. Rather they are included because they produce content that has been subject to moderation by the major social media firms. In each section ahead, further detail about selection criteria are documented. Only working websites were included.

(1) Lockdown Protest Websites in the US

Beginning in April 2020, a series of COVID-19 lockdown protests kicked off in the US, in the midst of the global pandemic. Even though the social media following and national news coverage was significant, in-person turnout at protests was small.[3], [4] Facebook, Instagram and Twitter have taken down posts, events and accounts that promote protests that break lockdown rules in the US.[5], [6] Facebook and Discord have also both removed far-right "Boogaloo" networks that were promoting protests against state lockdowns and using this opportunity to recruit new members.[7], [8] However, such moderation may be insufficient, and Bellingcat reports that Facebook and Instagram's policy of banning the use of Boogaloo terms has had a minimal impact on curbing the growth of the movement on its platforms.[9]

A sample of websites was used from Krebs Security's list of lockdown websites, and additional websites acquired from snowballing this initial list. [10] Websites within this sample were used as forums, for selling merchandise, announcing events, and fundraising. Most of the websites first appeared in April and May 2020, at the height of these protests. A few were repurposed from existing websites, including several that promoted second amendment rights. A few have since expanded to new themes, such as conspiracy theories about voter fraud in the US election.

(2) COVID-19 Scam Websites

There has been a spike in Internet scams since the first wave of the pandemic that used COVID-19 as a pretense. Scams have included procurement fraud relating to medical equipment, advance fee fraud, fake charities and COVID-19 themed websites with hidden malware. Fraud Watch International reports over 18 million attempts of phishing and malware attacks using COVID-19 lures in just one week in April 2020.[11] Online scams are often spread through dedicated websites, emails, messaging apps, and social media.

Fraudulent schemes appear to have elicited swift action down the technology stack. At the website level, in March 2020 the US Department of Justice filed its first court action against a website operator for committing fraud, citing an intention to profit from the coronavirus pandemic.[12] At the platform level, Facebook and Amazon have banned ads that, they have stated, exploit coronavirus fears, including price gouging ads.[13], [14] App stores have also cracked down on malicious COVID-19-themed apps.[15]

At the registrar level, the New York Attorney General has sent open letters to six of the largest registrar companies, requesting that they implement measures to crackdown on COVID-19 scam websites.[16] NameCheap has acted by stopping automated registration of coronavirus themed-websites. GoDaddy and Endurance have removed illicit websites through pre-existing detection and reporting mechanisms. ICANN have facilitated a COVID-19 Cyber Threat Coalition in order to better monitor threats during the pandemic.[17] The UK government identified scam websites and requested that ISPs take them down.[18]

Despite action being taken, scam websites still appear to be overwhelming service providers and content moderation measures still appear to be insufficient. For example, a report from the Digital Citizens Alliance documents the complicity of website brokers at the registration stage.[19] They found that they were able to easily purchase websites, and even when explicitly revealing fraudulent intentions. Likewise, others have found that it is easy to create ads to promote fake businesses on Google and Facebook's ad platforms.[20], [21]

A sample of websites was acquired from a list of still-active COVID-19 scam websites curated by Artists Against 419.[22] These websites imitate medical equipment and trading shopfronts, and most were established in 2020, although a number of them appear to be re-purposed websites.

(3) COVID-19 Disinformation Websites

Finally, coronavirus disinformation has consistently been a widespread issue. The intentional and unintentional spread of misleading information is prevalent across social media platforms, chat apps, and websites.

As with the lockdown protests, moderation has often been discussed at the platform and application level. Most large social media platforms have expressed commitments to preventing the spread of COVID-19 disinformation, and have formed a coalition that includes Facebook, Google, LinkedIn, Microsoft, Reddit, Twitter, and YouTube.[23]

Platforms have moved to demonetize, remove, and suspend content premised on COVID-19 disinformation.[24] Google's search engine has elevated authoritative sources for COVID-19 searches.[25] Apple and Google are cracking down on disinformation apps such as Alex Jones' InfoWars app[26]. Likewise, Google Maps have removed fake reviews and misleading information about healthcare locations.[27]

Nevertheless, it has proven extremely different to consistently moderate disinformation. Activists, regulators, and users highlight a variety of faults with the current measures, such as inconsistency with the ways in which content removals are decided, increasing automation, and the lack of transparency and accountability.[24], [28]

A sample of US-based websites was selected from a list of websites that the Computational Propaganda Project has been monitoring for the circulation of false claims about COVID-19 since March 2020 (see previous data memos). This sample includes websites that are circulating misleading information about alternative medicine, anti-vaccination news and pandemic denial content as well as more general websites known to circulate hoaxes. Less than a third of the websites were established in 2020.

FINDINGS

Infrastructure Services

Through WHOIS and IP geolocation lookups, we examined three important attributes of website infrastructure: the company providing registration services, the company providing hosting and CDN services, and the associated IP location.

Figure 1 reveals that lockdown protest websites tended to rely on GoDaddy, Google and Cloudflare as registrars and hosts/CDNs. Meanwhile COVID-19 scam websites have much more variation in services and rely on a host of technology giants but also many lesser known companies. The COVID-19 disinformation websites tended to rely on GoDaddy, Google, Cloudflare, and Amazon Web Services.

Websites across all samples mostly have associated IP addresses located in either the US or Canada when visited from within the US. In particular, the COVID-19 disinformation websites that target the US audience have edge IP addresses based in Canada through the proxy servers of Cloudflare and Fastly.

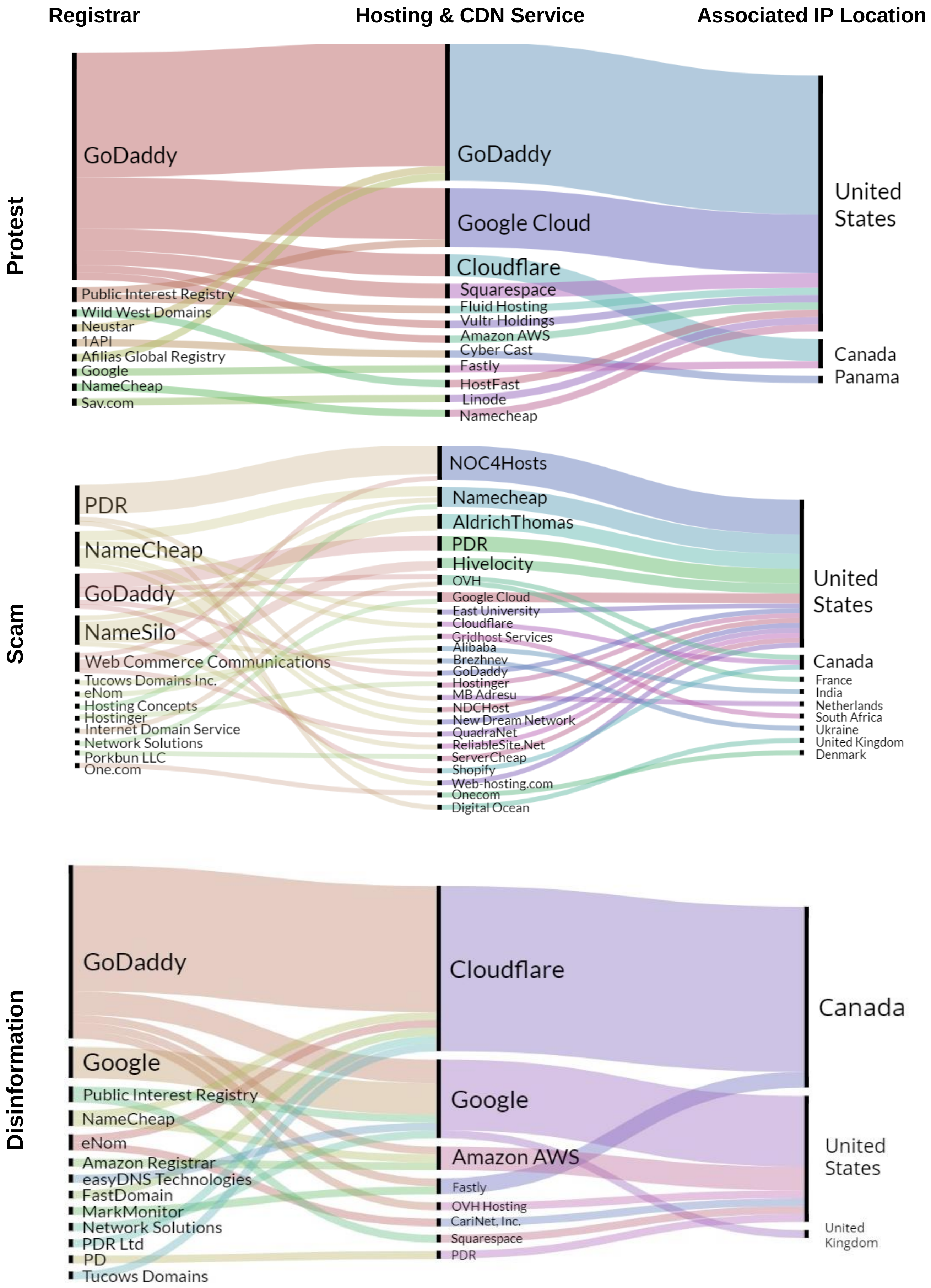
This gives an indication of how controversial websites use a large pool of services and the geographical spread of providers. In such a saturated market, when webmasters are faced with pro-active moderation, they are able to transfer to other service providers, without considerable repercussions. Furthermore, according to many terms of service agreements, clients are given time to find another service provider when they are found to be in breach of a service provider's terms of services. Transferal to alternative service providers can be undertaken smoothly and swiftly. Webmasters can also opt to switch to a provider in another legal jurisdiction without too much effort. This implies that a more concerted effort across companies and jurisdictions may be needed for effective moderation.

Networking and Data Mining Services

Websites also rely upon a variety of web-based third-party technologies for various functionalities. Third-party services have attracted controversy, particularly since Cambridge Analytica misused Facebook users' data through their role as a third-party firm.[29] Nevertheless, the third-party marketplace has continued to grow and includes a host of services, such as plugins that help website functionality, e-commerce tools, and interactive elements. All of these networking and data mining services are vital to the success of lockdown protest, scam and disinformation websites.

We found 321 separate components belonging to third-party businesses in the lockdown protest websites. 355 components were found in the scam websites. 858 components were found in the disinformation websites. Figure 2 identifies the top five companies providing

Figure 1: Key Infrastructure Services for COVID-19 Lockdown Protest, Scam, and Health Disinformation Websites



Source: Visualization based on data collected 1/7/2020 – 20/8/2020.
Note: The associate IP address is not the origin IP address (see Online Supplement). IP geolocation also only provides a partial view of website infrastructures, especially as CDNs help to conceal a web server's origin identity through processes such as reverse proxy services. Edge IP addresses are often the only visibly IP address as CDN server networks are usually not public.

networking and data mining services, for each of the three types of lockdown protest, scam and disinformation websites we catalogued.

We found an extensive array of third-party services. At the same time, a handful of big technology companies offer the most services. From largest to smallest presence amongst the samples, these are: Google, Facebook, Cloudflare, Apple, and Amazon. Other companies include Shopify, a service that helps websites set up an online shop. Shopify has previously been criticized for benefitting from sales of merchandise from Breitbart.[30]

Google and Facebook are particularly pervasive. Google's services include reCAPTCHA, Google Pay, Google Reseller, Google Remarketing, Google Interactive Media Ads, Google Apps for Business, Google Translate Widget, Google Cloud, and a wide variety of trackers. Services that link back to Facebook services in some way includes Facebook Like Box, Facebook CDN, Facebook Comments, Facebook Custom Audience, Facebook Embedded Video, Facebook Pixel, Click to Chat for WhatsApp, WhatsApp Me, Instagram Feed and a variety of widgets.

These third-party web technologies connect controversial websites back to Google and Facebook in various ways. For example, Google Ads Remarketing and Facebook Pixel allows websites to target ads to people who have visited their website. A user who visits a disinformation website may be retargeted when they are browsing YouTube or Instagram at a later time for instance.

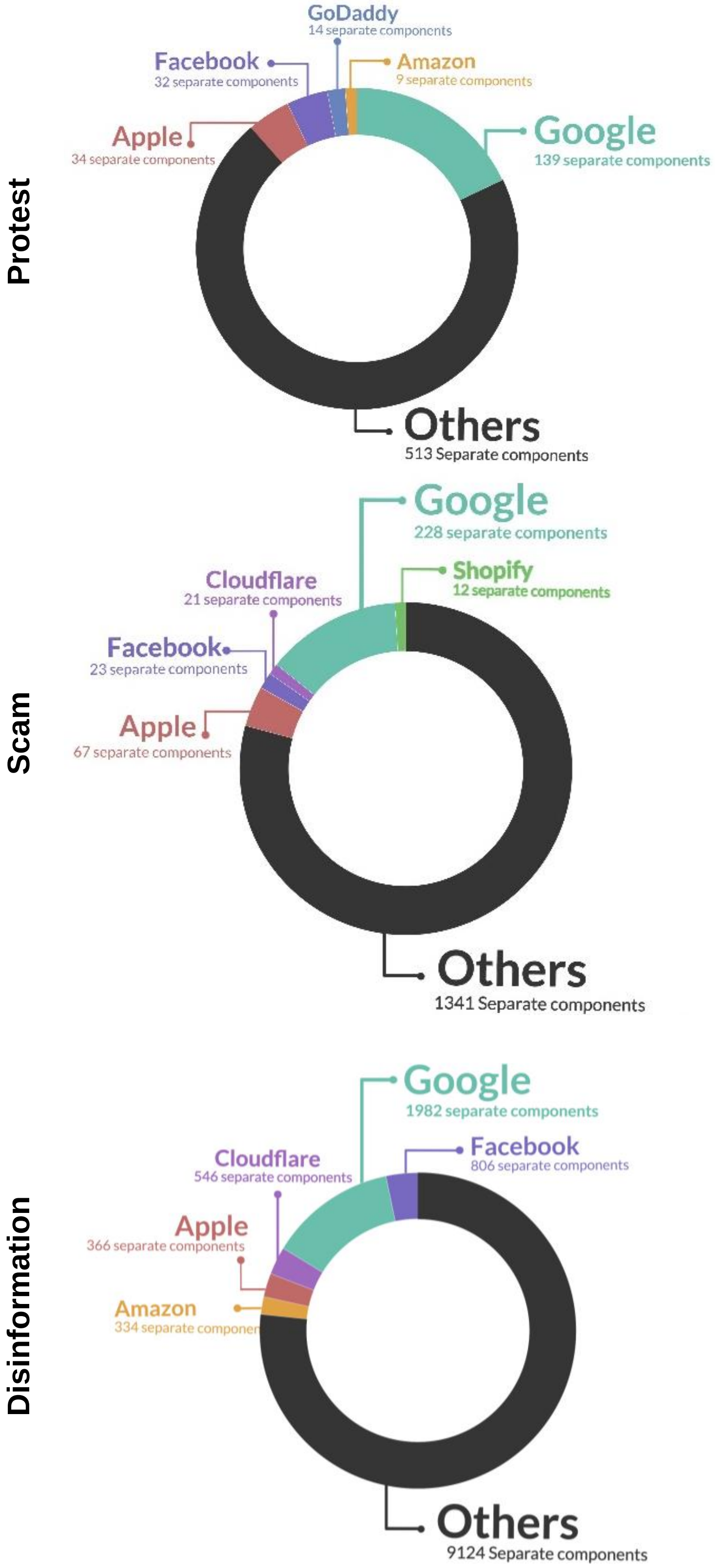
An economies of scale logic is important to third-party services where different data flows can improve such services. The range in types of data that can be collected is large. For example, Google's reCAPTCHA crowdsources streams of data to help label characters that are not accurately recognized through automated optical character recognition (OCR). However, the data collected through Google analytics are more related to building a profile of users to predict behavior. These various streams contribute to an accumulation of data which offers a particular advantage in analytics, advertising, and targeting in the technology space.

Trackers

This final analysis focuses more specifically upon the subsection of third-party add-ons called trackers. Trackers are pieces of software that are meant to collect information about users and user activities. Tracking commonly occurs through browser cookies, browser fingerprinting and IP tracking.

Trackers have become an important element of websites. They establish new relationships between websites beyond the hyperlink by embedding

Figure 2: Top Five Companies Providing Networking and Social Media Services for COVID-19 Lockdown Protest, Scam, and Health Disinformation Websites



Source: Visualization based on data collected 1/7/2020 – 20/8/2020.
Note: The Other category for lockdown protest websites contained over 200 firms, such as Adobe, Cloudflare, Microsoft, PayPal, NameCheap, Wix, Twitter, Reddit, Pinterest, and Yahoo. The Other category for scam websites contained over 200 firms, such as Adobe, NameCheap, Flickr, PayPal, Pinterest, and Wix. The Other category for disinformation websites contained over 600 firms, including Adobe, Flickr, Microsoft, LinkedIn, Reddit, Twitter, Uber, Wix, and Wordpress.

trackers that are often linked to data mining services.[31]

Using the Digital Method's Initiative's TrackerTracker tool and Gephi, we visualize the tracker ecology of our sample.[32] The tool utilizes Ghostery's browser extension to compare web tracking networks across websites.[33] We categorize four different trackers in a slightly adapted version of TrackerTracker's default categories:

- **Advertising**: Advertising services such as data collection, behavioral analysis and re-targeting
- **Analytics**: Data analytics, website usage, and performance trackers
- **Essential**: trackers critical to a website's functionality such as tag managers and privacy notices
- **Widgets**: Embedded on multiple websites, carrying information across websites (often back to social media platforms)

On average, websites protesting public health precautions and websites profiteering from the crisis have roughly the same proportions of trackers. About a third of their trackers are for advertising, a third are for analytics, and a third are a mixture of essential trackers and widgets. In contrast, almost two thirds of the trackers on COVID-19 disinformation websites are advertising trackers, revealing how much they depend on advertising as a revenue source.

Google and Facebook have a particularly ubiquitous presence across all four tracker categories and in all website samples. The visualization in Figure 3 show the network of trackers from each sample. All three visualizations show that Google dominates in advertising (Google DoubleClick, Floodlight and related trackers), analytics (Google Analytics) and essential trackers (Google Tag Manager). Facebook dominates in widgets (Facebook Connect, Facebook Social Graph, Facebook Social Plugins) but also ad trackers (Facebook Custom Audience). Trackers from smaller companies tend to only offer services in one of the categories. In particular, the tracker ecologies of the disinformation websites appear to be especially dense with many tracker modules.

As mentioned, Google and Facebook have removed ads that are seen to be exploiting the pandemic. However, it is not entirely clear to what extent ads have been removed and from which platforms. For instance, if an ad is removed from YouTube or Instagram, it is unclear whether they are also removed from Google's and Facebook's more general advertising and analytic ecosystems.

The tracker economy has become a large part of the data mining industry, where dominance here elevates the data accumulation of certain companies. Research has demonstrated that trackers exacerbate the accumulation of data by certain companies by facilitating an unequal flow of data.[31] For example, Facebook carefully regulates outside access to its data but has created many wide funnels for drawing in external data, metadata, and content from the open web. This includes widgets like the Facebook Like button which can track user's habits, even if users do not explicitly interact with them.

CONCLUSIONS

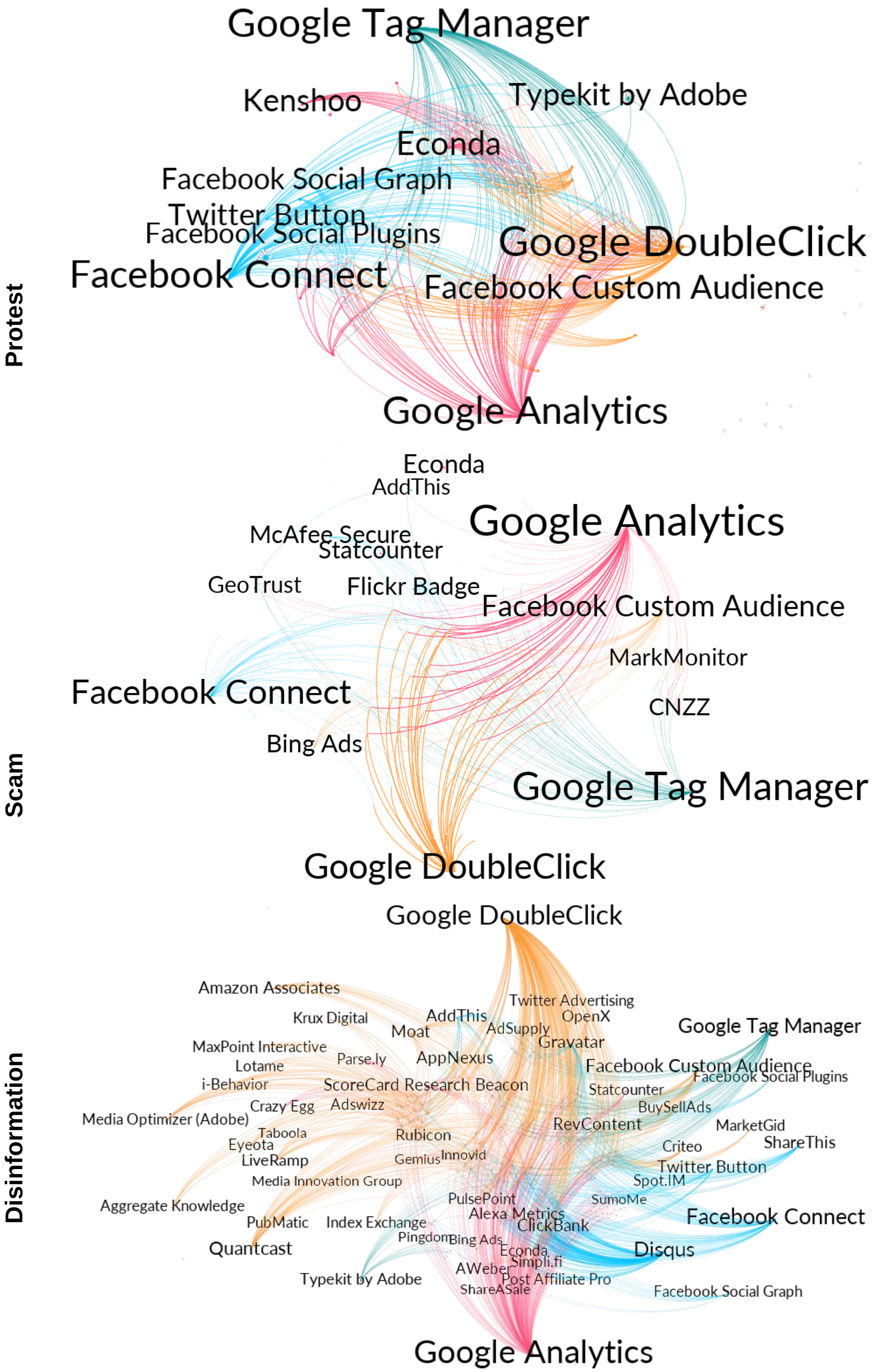
With the three samples of controversial websites this memo finds that while there is a wide variety of third-party services, a handful of technology giants dominate the third-party landscape. In relation to the variety of third-party services, we might ask whether isolated action by individual companies are sufficient. In relation to the prevalence of large technology companies, we might ask whether isolated action by these technology giants on their individual subsidiaries are sufficient.

Google and Facebook may flag content for being problematic on their social media networks but are still providing fundamental infrastructure for that content and supporting the revenue streams that make the purveyors of such content financially viable. The methods we have used here do not allow us to know how much revenue is generated for the major technology firms, or how much profit is made by the webmasters, scam artists, and junk news purveyors—only the firms themselves could provide that information.

This means that while social media platforms may remove harmful content on their most visible interfaces, they can still benefit and enable that content through other services they offer down the stack. For example, while Google can remove harmful content from YouTube, it can still continue to benefit from less prominent, back-end services such as advertising trackers, payment services and cloud services in terms of financial and data flows. Likewise, while Facebook can remove harmful content from its main social media website, it can still benefit and enable controversial content through its various widgets, advertising and analytic trackers.

The findings in this memo support the argument that platforms such as Google and Facebook have grown to be infrastructure-like.[34] Large technology companies that offer multiple levels of services can moderate controversial content on the front-end while still benefitting from the back-end of these same activities. This is noteworthy as both Google and Facebook are companies that derives most of their profit from advertising and data analytics. In 2018, ad revenue drove 85% of Alphabet's (Google's parent company) profit and 99% of Facebook's profits.[35] Both companies have grown beyond their original, single platform services and have become increasingly pervasive and essential in today's digital landscape. The stretch of services, add-ons, and embedded pieces of software that they offer cut across many infrastructural activities, which places them in unique positions in relation to the data and financial flows that

Figure 3: Tracker Services for COVID-19 Lockdown Protest, Scam, and Health Disinformation Websites



Source: Visualization based on data collected 1/7/2020 – 20/8/2020.
Note: Larger text size denotes more usage from the websites in this sample. Colors denote category of tracker: 🟧 = Advertising, 🟥 = Analytics, 🟩 = Essential, 🟦 = Widgets.

support COVID-19 websites organizing resistance to public health measures, promoting health scams, and circulating health misinformation.

Google and Facebook have evolved into entities that are simultaneously platforms and infrastructures by virtue of being ubiquitous and essential. Growing beyond their initial social media offerings, these companies have become thoroughly embedded in the digital landscape through the myriad of services that they provide. While major technology firms may have instigated content moderation on the front-end of their social media services, they still generate revenue from a wide range of back end services.

Regulations that curb potentially harmful online content cannot begin or end with the most visible aspects of the internet. Instead, there is a need to pay attention to the more hidden ways that companies benefit from financial and data flows emerging from controversial content.

REFERENCES

[1] J. Donovan, 'Navigating the Tech Stack: When, Where and How Should We Moderate Content?', *Centre for International Governance Innovation*, 2019. https://www.cigionline.org/articles/navigating-tech-stack-when-where-and-how-should-we-moderate-content.

[2] J. Gray, L. Bounegru, and T. Venturini, '"Fake news" as infrastructural uncanny:', *New Media Soc.*, Jan. 2020, doi: 10.1177/1461444819856912.

[3] E. Chenoweth, 'Media coverage has blown anti-lockdown protests out of proportion', *Vox*, May 10, 2020. https://www.vox.com/2020/5/10/21252583/coronavirus-lockdown-protests-media-trump.

[4] IREHR, 'New Far-Right Groups on Facebook Protesting Stay-at-Home Directives', 2020. https://www.irehr.org/covid19updates/dashboard-new-far-right-groups-on-facebook-protesting-stay-at-home-directives/.

[5] Culliford, 'Facebook removes anti-quarantine protest events in some U.S. states', 2020. https://www.reuters.com/article/us-health-coronavirus-usa-facebook/facebook-removes-anti-quarantine-protest-events-in-some-us-states-idUSKBN2222QK.

[6] R. Lerman and E. Dwoskin, 'Twitter crackdown on conspiracy theories could set agenda for other social media', *Washington Post*.

[7] Tech Transparency Project, 'Extremists Are Using Facebook to Organize for Civil War Amid Coronavirus', *Tech Transparency Project*, Apr. 22, 2020. https://www.techtransparencyproject.org/articles/extremists-are-using-facebook-to-organize-for-civil-war-amid-coronavirus.

[8] Owen, 'Discord Just Shut Down the Biggest "Boogaloo" Server for Inciting Violence', 2020. https://www.vice.com/en/article/akzkep/discord-just-shut-down-the-biggest-boogaloo-server-for-inciting-violence.

[9] 'The Boogaloo Movement Is Not What You Think', *bellingcat*, May 27, 2020. https://www.bellingcat.com/news/2020/05/27/the-boogaloo-movement-is-not-what-you-think/.

[10] Krebs on Security, 'Who's Behind the "Reopen" Domain Surge?' https://krebsonsecurity.com/2020/04/whos-behind-the-reopen-domain-surge/.

[11] FraudWatch International, 'Increasing Scams Amid the COVID-19 Pandemic', *FraudWatch International*, Apr. 24, 2020. https://fraudwatchinternational.com/brand-abuse/increasing-scams-amid-the-covid-19-pandemic/.

[12] The United States Department of Justice, 'Justice Department Acts To Shut Down Fraudulent Websites Exploiting The Covid-19 Pandemic', Aug. 12, 2020. https://www.justice.gov/opa/pr/justice-department-acts-shut-down-fraudulent-websites-exploiting-covid-19-pandemic.

[13] Associated Press, 'Facebook will ban certain ads to prevent efforts to exploit coronavirus fears', *the Guardian*, Mar. 07, 2020. http://www.theguardian.com/world/2020/mar/07/facebook-mask-ad-ban-coronavirus.

[14] Matsakis, 'As Covid-19 Spreads, Amazon Tries to Curb Mask Price Gouging', 2020. https://www.wired.com/story/covid-19-amazon-curb-face-mask-price-gouging/.

[15] UMB, '3 Ways Cybercriminals Are Exploiting the COVID-19 Crisis', 2020. https://www.umb.edu/news/detail/3_ways_cybercriminals_are_exploiting_the_covid_19_crisis.

[16] C. Cimpanu, 'New York asks domain registrars to crack down on sites used for coronavirus scams', *ZDNet*. https://www.zdnet.com/article/new-york-asks-domain-registrars-to-crack-down-on-sites-used-for-coronavirus-scams/.

[17] ICANN, 'Keeping the DNS Secure During the Coronavirus Pandemic', 2020. https://www.icann.org/news/blog/keeping-the-dns-secure-during-the-coronavirus-pandemic.

[18] Finextra Research, 'HMRC takes down nearly 300 Covid-19 phishing scam sites since March', *Finextra Research*, May 06, 2020. https://www.finextra.com/newsarticle/35771/hmrc-takes-down-nearly-300-covid-19-phishing-scam-sites-since-march.

[19] Digital Citizens Alliance, 'Domains of Danger: How Website Speculators and Registrars Trade Internet Safety for Profit'. Digital Citizens Alliance, 2020.

[20] Consumer Reports, 'Facebook Approved Ads w/ Coronavirus Misinformation', 2020. https://www.consumerreports.org/social-media/facebook-approved-ads-with-coronavirus-misinformation/.

[21] Laughlin, 'Fake ads; real problems: how easy is it to post scam adverts on Facebook and Google?', *Which? News*, Jul. 05, 2020. https://www.which.co.uk/news/2020/07/fake-ads-real-problems-how-easy-is-it-to-post-scam-adverts-on-google-and-facebook/.

[22] AA419, 'Artists Against 419'. http://wiki.aa419.org/index.php/Main_Page.

[23] N. Statt, 'Major tech platforms say they're "jointly combating fraud and misinformation" about COVID-19', *The Verge*, Mar. 16, 2020. https://www.theverge.com/2020/3/16/21182726/coronavirus-covid-19-facebook-google-twitter-youtube-joint-effort-misinformation-fraud.

[24] E. Simpson and A. Conner, 'Fighting Coronavirus Misinformation and Disinformation', *Center for American Progress*, 2020. https://www.americanprogress.org/issues/technology-policy/reports/2020/08/18/488714/fighting-coronavirus-misinformation-disinformation/.

[25] Bergen and De Vynck, 'Google Scrubs Coronavirus Misinformation on Search, YouTube', *Bloomberg.com*, Mar. 10, 2020.

[26] N. Statt, 'Apple and Google are cracking down on coronavirus apps to combat misinformation', *The Verge*, Mar. 05, 2020. https://www.theverge.com/2020/3/5/21167102/apple-google-coronavirus-iphone-apps-android-misinformation-reject-ban.

[27] Google, 'COVID-19: How we're continuing to help', *Google*, Mar. 15, 2020. https://blog.google/inside-google/company-announcements/covid-19-how-were-continuing-to-help/.

[28] R. Griffin and E. douek, 'How can social media platforms better prevent fake news? 3 questions to evelyn douek', 2020. https://webserver07.reims.sciences-po.fr/public/chaire-numerique/en/2020/07/09/social-media-platform-prevent-fake-news-evelyn-douek/.

[29] R. Brandom, 'Will third-party plugins survive the tech backlash?', *The Verge*, Jul. 06, 2018. https://www.theverge.com/2018/7/6/17538400/gmail-plugin-privacy-app-developers-google-facebook.

[30] J. Pearson, 'People Are Calling For a Shopify Boycott Because It Hosts Breitbart's Store', 2017. https://www.vice.com/en/article/ezmyq4/people-are-calling-for-a-shopify-boycott-because-it-hosts-breitbarts-store.

[31] C. Gerlitz and A. Helmond, 'The like economy: Social buttons and the data-intensive web', *New Media Soc.*, vol. 15, no. 8, pp. 1348–1365, Dec. 2013, doi: 10.1177/1461444812472322.

[32] 'TrackerTracker Tool', *Digital Methods Initiative*. https://wiki.digitalmethods.net/Dmi/ToolTrackerTracker.

[33] A. Helmond, 'Historical website ecology: Analyzing past states of the web using archived source code', in *Web*, 2017, vol. 25, pp. 139–155.

[34] J.-C. Plantin, C. Lagoze, P. N. Edwards, and C. Sandvig, 'Infrastructure studies meet platform studies in the age of Google and Facebook', *New Media Soc.*, vol. 20, no. 1, pp. 293–310, Jan. 2018, doi: 10.1177/1461444816661553.

[35] J. Desjardins, 'How the Tech Giants Make Their Billions', *Visual Capitalist*, Mar. 29, 2019. https://www.visualcapitalist.com/how-tech-giants-make-billions/.

ACKNOWLEGMENTS

We are very grateful for this collaboration with Project Ainita. The authors gratefully acknowledge the support of the European Research Council for the project 'Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe', Proposal 648311, 2015–2020, Philip N. Howard, Principal Investigator. Project activities were approved by the University of Oxford's Research Ethics Committee, CUREC OII C1A 15-044. We are also grateful to the Adessium, Luminate, and Ford Foundations for supporting this work. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the University of Oxford or our funders. We are grateful to Cindy Ma, Claire Robertson, Hammer, John Francis, Lisa-Maria Neudert, Mona Elswah and Nahema Marchal for their contributions to this memo.

ABOUT THE PROJECT

The Computational Propaganda Project (COMPROP), which is based at the Oxford Internet Institute, University of Oxford, involves an interdisciplinary team of social and information scientists researching how political actors manipulate public opinion over social networks. This work includes analyzing how the interaction of algorithms, automation, politics, and social media amplifies or represses political content, disinformation, hate speech, and junk news. Data memos integrate important trends identified during analyses of current events with basic data visualizations, and although they reflect methodological experience and considered analysis, they have not been peer reviewed. Working papers present deeper analysis and extended arguments that have been collegially reviewed and engage with public issues. COMPROP's articles, book chapters, and books are significant manuscripts that have been through peer review and formally published.