2023-12

# Content moderation through removal of service: Content delivery networks and extremist websites

Looney, S



10.1002/poi3.370
Policy & Internet
Wiley

Received: 7 June 2023 | Accepted: 26 August 2023

DOI: 10.1002/poi3.370

RESEARCH ARTICLE

P&I Policy & Internet PSO WILEY

# Content moderation through removal of service: Content delivery networks and extremist websites

**Seán Looney**

School of Society and Culture (Faculty of Arts, Humanities and Business), University of Plymouth, Plymouth, England

**Correspondence**

Seán Looney, School of Society and Culture (Faculty of Arts, Humanities and Business), University of Plymouth, Plymouth, England.
Email: sean.looney@plymouth.ac.uk

## Abstract

Considerable attention has been paid by researchers to social media platforms, especially the 'big companies', and increasingly also messaging applications, and how effectively they moderate extremist and terrorist content on their services. Much less attention has yet been paid to if and how infrastructure and service providers, further down 'the tech stack', deal with extremism and terrorism. Content Delivery Networks (CDN) such as Cloudflare play an underestimated role in moderating the presence of extremist and terrorist content online as it is impossible for these websites to operate without DDoS protection. This is evidenced by the takedown of a wide range websites such as The Daily Stormer, 8chan, a variety of Taliban websites and more recently the organised harassment site Kiwifarms following refusal of service by Cloudflare. However, it is unclear whether there is any formal process of content review conducted by the company when it decides to refuse services. This article aims to first provide an analysis of what extremist and terrorist websites make use of Cloudflare's services as well as other CDNs, and how many of them have been subject to takedown following refusal of service. Following this the article analyses CDNs' terms of service and how current and upcoming internet regulation applies to these CDNs.

**KEYWORDS**

Content Delivery Networks, content moderation, extremism, regulation, websites

## INTRODUCTION

Content Delivery Networks (CDN) are a necessity in the modern internet ecosystem for websites to operate. Without them, websites are liable to be either too slow to function or overloaded with user requests, legitimate or otherwise. It does not appear that there is any consistency to CDNs approach to violent extremist and terrorist content being temporarily hosted on their servers and whose services allow them to operate. The lack of a clear standardised process of content moderation may lead to the current situation where CDNs largely ignore or remain ignorant to this prohibited use of their services until public pressure and negative press becomes too difficult to resist.

The main victim of this process thus far has been Cloudflare. The most recent example of this was the Kiwifarms incident. Kiwifarms was an internet forum known for its active targeting and harassment of trans people, leading to it being blamed for the suicides of some of their targets. In August of 2022 the forum set their sights on Canadian Twitch Streamer and Trans Activist Clara Sorrenti, also known as Keffals. The forum members called in a fake bomb threat to her home, caused the police to turn up to her home and subsequently tracked her around the world once she fled Canada. If this had occurred on one of the big social media platforms such as Facebook, Twitter and YouTube, Sorrenti may have had some recourse to a form of content moderation. However, as Kiwifarms is a stand alone website she had no such recourse. Instead she utilised her online following, starting a 'Drop Kiwi Farms' movement to get the site kicked off the internet by targeting the companies that allow them to operate, the primary target of this campaign was Cloudflare.

While Cloudflare initially tried to deflect the responsibility for keeping Kiwifarms operational, in September it ultimately backed down and stopped offering services to the site. The CEO of Cloudflare made clear that they did so reluctantly: 'You don't want some random guy who lives in the United States picking what is and is not online … I have no political legitimacy, right? At all'. (Taylor, 2022). This echoes the statements made by Cloudflare's CEO during the Charlottesville incident (Prince, 2017). Kiwifarms then found another CDN in the form of Diamwall whose CEO, Hugo Carvalho, made a blog post defending their initial decision to onboard Kiwifarms, that the 'owner of Kiwi Farms came in need of DDoS protection and because their website was offline due to DDoS, we didn't really know about their website's content. They had a PROBLEM and we had the SOLUTION'. (Carvalho, 2022). Carvalho's blog sets out the perspectives of the CDN companies to this problem. First, he is at pains to explain what a CDN does and doesn't do. To him CDNs are only a proxy that filters website traffic and blocks malicious requests, therefore they do not host any website, are not responsible for any websites content and cannot control every service's content. The company does not and cannot analyse every single website that uses their services. Thus, the Diamwall CEO is distancing his company from the need for content moderation in a technical and logistical sense, as opposed to the Cloudflare CEO's normative sense.

Despite this Carvalho immediately explains that Diamwall will also be suspending Kiwi Farms service with them. While Diamwall does not think it's fair to terminate any service because of public pressure, in the case of Kiwi Farms they 'think there is some foundation behind all those requests and we really do not want to have anything to do with it'. The blog post ends by warning the reader that this will not fix the issue, only delay it. Kiwi Farms will find another provider that can protect them and will be online once again.[1] This episode highlights the issues at play in this article. There are many websites such as Kiwifarms which should not be accessible on the internet, however without clear rules and obligations this scenario will simply repeat.

This is an exploratory article which seeks to elucidate the issues surrounding CDNs, their importance in the internet ecosystem and their role in allowing terrorist, extremist and conspiracist propaganda to spread online. This article consists of three main parts. First it

examines a series of terrorist, extremist and conspiracy websites to ascertain what CDN is providing services for them. This section utilises Davies et al.'s (2015) extremism and recruitment frameworks to provide a sense of the content found on these sites. Next the article examines the liabilities and obligations of CDNs under the Digital Services Act to provide a clear picture of what is and isn't expected of CDNs operating within the European Market going forward. Finally, this article examines the terms of use of the CDNs found within the first section. Assessing whether there is evidence of self-regulation and content moderation to be found.

## HOW DO CDNS WORK?

For clarity it is useful to fully define and explain what a content delivery network is and how it functions. Donovan (2019) places CDNs on level 4 of the 'tech stack'. The tech stack is a way of explaining how the internet functions. It describes a range of levels from the open web down to government and telecom infrastructure. On level 4 of the stack, CDNs purpose is to help match user requests with local servers to reduce network strain and speed up websites. This is important for general use of the internet as without it more popular websites would, with enough users attempting to access them, be slowed to the point of unusability or would be rendered offline due to server overload. A typical CDN will consist of a combination of back-end and front-end servers. The former exist to allow for efficient intra-CDN distribution of content, the latter handle user-server communications (Stocker et al., 2017) Schwemer et al. (2021) divide CDNs into two technical and legal functions dependent on their customer. The first is the provision of traditional caching services to benefit Internet Access Providers (IAP) based on content requests from users. This is contrasted with the provision of CDN services on behalf of the content owner.

By distributing demand to multiple servers the CDN reduces the amount of strain suffered by the websites hosting service. This raises a question however, as it is unclear whether the CDN is effectively hosting this content on these alternative servers. For example, a CDN provider can guarantee the availability of a website, even when the customer's website is temporarily inaccessible. This becomes an issue when it comes to illegal, extremist and terrorist content as the CDN can be said to have beomce a 'surrogate host' for the customer's content (Schwemer et al., 2021).

CDNs are also essential for dealing with more malicious access attempts, specifically denial-of-service attacks (dos) that aim to overwhelm a server. This acts along the same logic as server overload due to popularity. However there are multiple ways to facilitate such an attack. One of which is to trick the server into forming an increasingly long queue of people it is trying to communicate with. A distributed denial-of-service (ddos) attack is this same process but utilising a network of computers. This can either be a peer-to-peer network of users attacking the same target or a bot-not of hacked computers. The advantage of the distributed approach is that while a server could simply block the IP address of a single attacker, it is much more difficult to block a distributed network with multiple redundent IP addresses.

For the purposes of this article these two aspects of CDNs are essential, just as they are essential for the functioning of a modern website. As mentioned above there is a question of whether CDNs legally act as a host for the purposes of liability. If the CDN hosts, albeit temporarily, illegal or extremist content for the purpose of sharing it with users, then this is functionally similar to the act of hosting by the website provider. For the latter, the DDoS protection which is provided by CDNs is a necessity for most websites, but in particular for controversial, illegal and extremist websites. This is due to how they are more likely to be targeted by DDoS attacks either by activists, intelligence agencies or rival groups.

# LITERATURE REVIEW

## Content delivery networks

Research on content delivery networks have largely focused on improving their potential for to meet content demands of the contemporary internet (Chard et al., 2017; Gkatzikis et al., 2017; Salahuddin et al., 2018; Thomdapu et al., 2021; Zolfaghari et al., 2020). Stocker et al. (2017) provide a thorough outline of the differing CDN architectures and their relative strengths and weaknesses. Their typology of CDN architectures highlights how discussing CDNs as one monolithic type of entity, as I tend to here, has a tendency to be reductive. These networks can range from data centre based to highly distributed across a network, or even peer-to-peer. The efficacy of these networks is highly dependent on both the geographic location and virtual location of their servers. Distributing CDN servers over a wider geographic area expands the range of options for serving content from a server that is geographically close the end user, thus reducing delay times. Simultaneously internet routing protocols do not route packets based solely on the geographic distance between the source and destination, rather routing is based on their virtual location as determined by their IP address. Two IP addresses belonging to the same domain may actually be thousands of miles apart, such as the distance between New York and Los Angeles. Conversely two IP addresses may geographically be in the same city but belong two different administrative domains, requiring network paths that require traversing thousands of miles and even national borders. Maillé and Tuffin (2014) provide an analysis of the economics of CDNs and specifically in relation to net neutrality. Pathan and Buyya (2007) provided a taxonomy and survey of CDNs.

## Content moderation and CDNs

There is less of a focus both in the CDN literature and content moderation literature on the acts of content moderation by these infrastructure companies. Ruddock and Sherman call for a widening of the lens on content moderation to aspects such as CDNs. Ruddock and Sherman (2021) attempt to map out the online information system and in doing so divide the differing services and companies into the different ways they allow internet users to access information such as accessing, delivering, hosting and securing, browsing, content-curating, and financially facilitating. CDNs are placed in the delivering category which routes internet traffic from users to sought-after content. It is placed alongside registries, registrars and domain name system operators. The authors point out that CDNs can effectively be a source of control for states. Such as before banning Google, the Chinese government first blocked the Google cache. Similarly in Vietnam state owned telecommunications companies forced Facebook's local Vietnamese servers offline for 7 weeks. During this time the connection was so slow for users in Vietnam that Facebook was effectively unavailable to many users. Similarly, Trivedi (2023) outlines how proposed sets of principles such as the Santa Clara Principles and the Manila Principles on Intermediary Liability may impact not just telcos but app stores and CDNs. Jardine, (2019) work focuses on how content moderation interacts with the Dark Web, highlighting Cloudflare's attempt to minimise Dark Web traffic by placing time consuming CAPTCHAs on all traffic coming from known Tor exit relays and attempting to access websites protected by the company. This article aims to contribute to this literature by emphasising the role these networks play in the maintenance of extremist websites and the corresponding lack of content moderation present.

## Terrorist, extremist and conspiracist websites

This article is predominantly examining two areas: terrorist and extremist websites and internet infrastructure. Much like their nonextremist counterparts, Terrorist and extremist websites as a topic enjoyed relative popularity in the 2000s before being supplanted by the study of social media platforms and networks (Caiani & Parenti, 2009; Qin et al., 2007; Yilu Zhou et al., 2005; Alexander, 2011). However, there has been a recent uptick in attention paid to extremist websites. Conway and Looney qualitatively examine the content of an ideological diverse range of extremist and terrorist websites. Bloch and Myer (2018) compared the discourse of 52 US based nativist extremist groups to the debate transcript of Donald Trump during the 2016 presidential campaign. Yasin (2014) documented the use of websites by extremist groups to promote fundraising initiative and the sharing of tradecraft bomb-making materials.

Hanley et al. (2022) examine the relationships between various websites either run or frequented by QAnon conspiracy theorists. Utilising 8kun and Voat as seed websites, the authors curated the largest known corpus of QAnon websites derived from hyperlinks. One of the most useful outputs of this project is the database of 324 QAnon related websites curated by the authors. Dahlke et al. (2022) utilise a mixed-methods approach to ascertain the website consumption of QAnon conspiracy theorists. Specifically, they examined the web-browsing data collected by the survey company YouGov in combination with the database curated by Hanley et al. above. Finding that while relatively few Americans were exposed to QAnon website content, they extrapolate that this 3.7% exposure means that over 9.5 million American adults were exposed to such content during the 2020 US Presidential Election.

Tech Against Terrorism (2022) produced a report into terrorist and violent extremist operated websites, identifying 198 websites that they assessed as being operated by terrorist actors or by violent extremists that pose a credible and urgent threat to society. Seventy-nine of these sites related to violent Sunni Islamist actors, 18 to violent Shia Islamist actors, and 101 liked to the violent far right. The report examined a representive sample of 33 websites finding that 91% displayed audio/visual propaganda, 73% had an archive of historic content and 57% contained a communication feature. The total average monthly visits to these 33 sites was 1.54 million. Likewise, the Institute for Strategic Dialogue have produced reports into terrorist and extremist websites (Guhl et al., 2020; Thomas, 2021). This article aims to contribute to this literature on the renewed importance of extremist websites by widening this discussion to the infrastructure which enables and supports the use of websites by extremist groups.

# METHODOLOGY

This article aims to give an indication of which CDNs are being used by extremist and conspiracist groups to operate their websites and what content is being hosted by these websites. Utilising the categories established by Conway and Looney (2021), this study examined 56 website domains over the period of 01 December 2022–06 January 2023 to ascertain who was responsible for their content delivery network. In this article 'website' refers to a form of standalone, largely noninteractive multimedia site. Online discussion forums, social media platforms and messaging applications are therefore excluded from the scope of this article. The aim of this method was not to provide a representative sample of all extremist websites but rather to give an indication of the importance of CDNs to the continuing functionality of extremist websites. The method utilised to obtain this information

was the inspect function of google chrome. Examining any element under the network tab reveals the server which communicated the html page to the browser (Figure 1).

It isn't sufficient to examine just one element as certain plugins may be provided by another server. One common example is elements provided by google plugins. It is most accurate to examine the element containing the website's address.

Each of the examined websites were then classified according to Davies et al.'s (2015) web extremism and recruitment scales. It should be noted that this coding was conducted solely by this article's author which may limit the reliability of results. The web extremism scale ranges from level 1 where websites are informational only. The information presented by these websites actively avoids the presentation of violence and the use of hate speech. A level 2 website also avoids the presentation of violence but encourages visitors to join the site's cause in some manner. A level 3 website features violent content without explicitly encouraging participation in the website's cause. Finally, a level 4 website actively encourages individuals to support the cause, including violent actions (Davies et al., 2015, p. 116).

Following on from this the recruitment framework orders websites from 0 to 3. A website with a 0 rank contains no recruitment materials at all. A website with a 1 rank points towards to the presence of efforts to pique the curiosity of site users, such as public discussion forums or opportunities to subscribe to newsletters and magazines. A website with a 2 rank refers to the encouragement of 'indirect action', such as donating to the group, cause or the maintaining of the website itself. Finally, a score of 3 indicates active recruitment, including announcements and invitations to events as well as overt calls to 'real world' violent action (Davies et al., 2015, p.117).

In line with Conway and Looney (2021) the examined websites were divided into categories based on the believed operators of the site. The first is Terrorist Operated Websites (TOW) which are sites that are expressly and officially affiliated with a terrorist group or movement. Conversely, the second category proposed by the authors is Fan Sites (FS) which are websites publicly claiming support for—and sometimes affiliation with—a terrorist group, but without being run directly by it. The third category is Ideologically Adjacent or 'fellow traveller' websites (IFT) which are unaffiliated with particular terrorist groups but are ideologically supportive of one or more such groups or movements and thus extremist in their orientation. For the purposes of this article a fourth category has been added; Conspiracy sites. These sites were drawn from Hanley et al.'s (2022) study of Qanon believer's website consumption and accordingly are largely

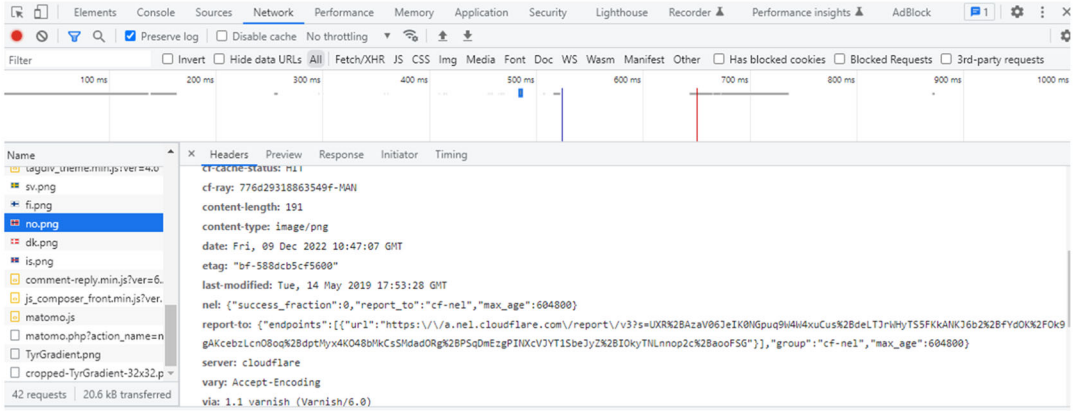


**FIGURE 1** The inspect function of Google Chrome on a webpage.

focused on Qanon however other conspiracy theories such as concerning the COVID-19 pandemic and vaccinations were also found on these websites. Likewise, the other three categories the websites were compiled via literature review primarily as well as the author's prior work. Where the literature did not provide an exact URL to follow, the websites were found through a mixture of trial and error, search engines and the sharing of information with colleagues. This is another limitation of this study, a future study could utilise a more thorough method such as web scraping to build a more representative sample such as in the work of Mei and Frank (2015). However, this is not necessary for the limited scope of this article (Tables 1–5).

**TABLE 1** Websites per CDN provider.

| | Cloudflare | Nginx | Apache | Litespeed | Squarespace |
|---|---|---|---|---|---|
| Terrorist operated website | 2 | 3 | 2 | 1 | 0 |
| Ideological fellow traveller | 13 | 5 | 2 | 0 | 0 |
| Fan sites | 0 | 0 | 0 | 0 | 0 |
| Conspiracy sites | 8 | 15 | 4 | 0 | 1 |
| Total | 23 | 23 | 8 | 1 | 1 |

Abbreviation: CDN, Content Delivery Networks.

**TABLE 2** Extremism scale per CDN provider.

| | 1 (fact based) | 2 (join-the-cause) | 3 (displays of violence) | 4 (call-to-violence) |
|---|---|---|---|---|
| Cloudflare | 10 | 6 | 7 | 0 |
| Nginx | 10 | 8 | 5 | 0 |
| Apache | 6 | 0 | 2 | 0 |
| Litespeed | 0 | 1 | 0 | 0 |
| Squarespace | 0 | 1 | 0 | 0 |
| Total | 26 | 16 | 14 | 0 |

Abbreviation: CDN, Content Delivery Networks.

**TABLE 3** Recruitment scale per CDN provider.

| | 0 (none) | 1 (passive) | 2 (indirect action) | 3 (active) |
|---|---|---|---|---|
| Cloudflare | 5 | 2 | 9 | 6 |
| Nginx | 4 | 7 | 12 | 1 |
| Apache | 3 | 0 | 5 | 0 |
| Litespeed | 0 | 0 | 1 | 0 |
| Squarespace | 0 | 1 | 0 | 0 |
| Total | 12 | 10 | 27 | 7 |

Abbreviation: CDN, Content Delivery Networks.

**TABLE 4** Extremism scale per website type.

| | 1 (fact based) | 2 (join-the-cause) | 3 (displays of violence) | 4 (calls-to-violence) |
|---|---|---|---|---|
| TOW | 4 | 2 | 1 | 0 |
| IFT | 3 | 7 | 10 | 0 |
| CS | 19 | 6 | 3 | 0 |
| Total | 26 | 15 | 14 | 0 |

Abbreviation: TOW, Terrorist Operated Websites.

**TABLE 5** Recruitment scale per website type.

| | 0 (none) | 1 (passive) | 2 (indirect action) | 3 (active) |
|---|---|---|---|---|
| TOW | 5 | 0 | 1 | 2 |
| IFT | 5 | 4 | 5 | 5 |
| CS | 2 | 6 | 20 | 0 |
| Total | 12 | 10 | 26 | 7 |

Abbreviation: TOW, Terrorist Operated Websites.

## RESULTS

The results are as follows:

It is clear that Cloudflare and Nginx are the main provider of CDNs for the websites present in the sample with 46 of the 56 websites being provided services by them. However, there are a number of other providers present websites examined, namely apache, litespeed, and squarespace which will be examined in further detail below. The eight TOWs present in the sample are more or less evenly split between Cloudflare, Nginx, Apache and Litespeed, with only Squarespace lacking a TOW. It is important to note that the TOWs present here are ideologically diverse including websites affiliated with Hamas, PKK, Al Qaeda, PFLP, Earth First!, Blood and Honour and Hizbullah. In terms of IFTs Cloudflare supports the most with 13 compared to Nginx's 5 and Apache's 2. Ideologically these IFTs are split between violent jihadist and extreme far right with websites representing groups and movements such as the Nordic Resistance Movement, Patriot Front, the American Nazi Party, Identity Evropa, Blood and Soil and the Daily Stormer. The violent jihadist IFTs were supportive but not expressly affiliated with groups such as the Muslim Brotherhood, Hizb ut-Tahrir and Jaish ul-Adl. Unfortunately, due to their relative lack of stability and availability Fan sites were not found within the sample however this may be a result of its small sample size and the relative difficulty of finding these supporter sites who cycle through stable addresses rapidly. The omission of Fan Sites is a major limitation of this article, and a future study of the use of CDNs by extremist websites should aim to build a wider, more representative sample of websites. Finally, the largest category of sites in this data set were the Conspiracy Sites, with the majority being provided a CDN by Nginx (15/28) and Cloudflare (8/28).

None of the examined sites meet the requirements for rank 4 on the extremism scale as none actively incite users to take violent action for the cause. The largest category (26/56) of websites scored a 1 but this is largely due to the presence of the conspiracy sites which, for the most part, avoid calls to violence, action or hate speech. Rather they are focused on

spreading misinformation in accordance with their chosen conspiracy, predominantly Qanon. The IFT sites skewed more toward 3, as they feature violent imagery, content and hate speech but stop short of direct calls to violent action. Finally, the TOW sites were mostly focused on providing information to the user. In terms of recruitment the websites were mostly focused on soliciting funding for the maintaining of the group or the website (26/56), rather than actively encouraging participation in group activities (7/56).

## EXISTING LEGISLATIVE PRESSURE ON CDNS

It's clear that CDNs are essential for the above websites to operate, however its not clear what legislative pressure there is on these companies to moderate the websites to whom they provide services. CDNs, in particular Cloudflare, have already come to the attention of the EU Commission in the area of counterfeiting and online piracy. For the previously explained action of providing anonymity to the operators of websites conducting illegal activity, in this instance piracy. Here the Commission drew a distinction between hosting providers and CDNs, explaining that while some hosting providers have policies against copyright infringement and regularly take action against such users, others do not. These other hosting providers utilise CDNs to provide anonymity to the operators of the pirate sites. Cloudflare was highlighted as being used by approximately 40% of the pirate websites in the world. Of the top 500 infringing domains, based on global Alexa rankings, 62% are using Cloudflare as a CDN provider. Respondents to the Commission's public consultation, which included Member States, recommended that Cloudflare's cooperation with rightsholders should be improved and for the company to follow due diligence when opening accounts for websites to prevent illegal sites from using its services (European Commission, 2018, p. 21).

### The Digital Services Act (DSA)

Article 3(g) of the DSA (2022) clarifies issues surrounding CDNs by defining intermediary services as three separate categories: 'mere conduit' services, 'caching' services and 'hosting' services. Each are subject to different liabilities and obligations, the latter two will be discussed here as they are most pertinent to CDNs.

Article 5 of the DSA defines 'caching' service as where the service provided consists of the transmission in a communication network of information provided by a recipient of the service. The provider of such a service shall not be liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making the transmission of information more efficient or secure. This is subject to several conditions. The provider cannot modify the information, must comply with conditions on access to the information and comply with industry rules regarding the updating of the information. They must also not interfere with the lawful use of technology to obtain data on the use of the information. Finally, they must act expeditiously to remove or disable access to stored information upon receiving actual knowledge that the information has been removed by the source, such as the website operator, or if a judicial or administrative authority has ordered such removal or disablement.

On the other hand Article 6 defines 'hosting' service consists of where the service provider stores information provided by a recipient of the service. Here, the service provider shall not be liable for information stored subject to two conditions. The first is that the host does not have actual knowledge of illegal activity or illegal content, and the second is that upon obtaining such knowledge or awareness the host acts expeditiously to remove or to disable access to the illegal content.

As per Articles 11–15 DSA, in terms of obligations 'caching' and 'hosting' services share several obligations such as tranparency reporting where the all providers must make publicly available, machine-readable and easily accessible reports on any content moderation that they engaged in during the relevant period. They must both provide due account of fundamental rights in their terms of service. They must both cooperate with national authorities if ordered to do so and must maintain points of contact and, where necessary, legal representatives.

There are two additional obligations for hosting services which 'caching' services are exempt from. The first are notice and action mechanisms which allow any individual or entity to notify them of the presence on their service of what the individual or entity considers to be illegal content. These mechanisms are required to be easy to access and user friendly and shall allow for the submission of notices exclusively by electronic means. These notices shall be considered to give rise to actual knowledge of the specific item reported, thus the service provider is required to address the content mentioned by the notice expeditiously. Importantly Article 16 and 17 provide an expectation of due process for both the reporter and those whose use may be effected by the noitce. For the reporter the hosting provider shall inform them that the report has been received, notify them of the decision and provide information on the possibility of redress in respect of that decision. For those whose content or use of services may be impeded by the report the 'hosting' provider shall provide a clear and specific statement of reasons to any affected recipients of the services. This applies for both the grounds that the report concerns illegal content or that it is incompatibile with their terms and conditions. This applies to all forms of restrictions including reduced visibility, demoting content, removal of content, suspension or termination of monetary payments, service in whole or in part or accounts.

The level of information required in this process is high and includes clearly stating the reasons for the restriction as well as the facts and circumstances that led to this decision, whether the report was voluntary and, where strictly necessary, the identity of the notifier. It also includes whether the decision to impose restrictions was in any way automated. Where the decision concerns allegedly illegal content the legal ground relied on must be referenced and the reasoning behind why the content is considered to be illegal. Similarly, where the decision is instead in conflict with the service's terms and conditions the contractual ground must be referenced and the conflict justified. Finally there must be clear and user-friendly information on the possibilities for redress such as internal complaint handling mechanims, out-of-court dispute settlement and judicial redress.

The second key difference in obligations concerns the notification of suspicions of criminal offences. In particular, where the hosting provider becomes aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place, or is likely to take place, it must promptly inform the relevant law enforcement or judicial authorities. If they cannot reasonably identify the relevant member state to notify they must inform the member state where they are established or Europol, or both. Both articles state that these liability exemptions do not affect the possibility for a judicial or administrative authority, in accordance with a Member State's legal sytem, to require the service provider to terminate an infringement.

There is clearly a much higher level of obligation for hosting services as opposed to caching services. This is important in this context as it isn't clear whether a CDN such as Cloudflare or Nginx should be considered a 'caching' service or a 'hosting' service. Drawing back to Schwemer et al. above, CDNs are left in an awkward position where their different functions may or may not leave them liable to different liabilities and in particular obligations. Considering that the function that concerns terrorist and extremist content is the surrogate hosting function, it remains to be clarified whether CDNs can rely on being treated simply as caching services rather than hosting services.

## EXAMINING CDN TERMS OF USE

Thus far this article has shown how there are a number of extremist, terrorist and conspiracy sites utilising CDN services, in particular the services of Cloudflare, Nginx and Apache. It has also explored the upcoming legislative requirements which will be placed on CDNs as per the Digital Services Act. With both of these in mind the final part of this article examines a number of CDNs' acceptable use policies or terms of service. This is done in pursuit of two objectives, the first is to see whether the CDNs explicitly prohibit the use of their services for illegal or extremist purposes. The second is to examine whether there is any information available to the user as to the process behind termination of services or any other form of restrictions, and whether they have any form of redress.

### Cloudflare TOS

Cloudflare makes clear that with respect to the services they provide, Cloudflare 'operates pass-through network services used to improve network performance, not hosting provider services'. As such they claim they have no way of removing improper or infringing material from their users' websites, third party sites or their hosting services.

Cloudflare lists a variety of prohibited uses of their services. These include the utilisation of their services in most forms of computer misuse or cybercrime such as the transmitting of viruses, worms, defects and trojan houses, attempting to bypass the limits of Cloudflare services, or using Cloudflare services to gain access to another computer or system via hacking or password mining. There is no explicit mention of extremist content or the use of Cloudflare's services by terrorist or proscribed groups however this is essentially covered by the prohibition on using Cloudflare's services in ways that violate US or international laws and regulations (Conway & Looney, 2021).

Cloudflare recently launched its foray into Web3 with its Distribute Web Gateway. Web3 generally refers to the use of a decentralised online ecosystem based on blockchain, so this would not apply to the websites examined here. For this Cloudflare retains the right, but importantly not the obligation, to block content from its distributed web gateway that Cloudflare determines to be illegal, harmful or in violation of these terms. Cloudflare goes on to define such harmful or illegal material as including but not limited to: (a) content containing, promoting or facilitating child sexual abuse or human trafficking; (b) copyright or intellectual property violating material, (c) content that discloses sensitive personal information, incites or exploits violence, or is intended to defraud the public and (d) content that seeks to distribute malware, facilitate phishing or otherwise constitutes technical abuse.

Cloudflare provides multiple avenues via which users can report abuse of Cloudflare services. In addition to an automated form located on the Cloudflare website, concerned individuals can mail their complaint the Cloudflare legal department. For frequent reporters Cloudflare offers an automated process via granting access to an abuse API token. Nonetheless they are at pains to assure the readers that termination of use is at Cloudflare's sole discretion, with or without notice for any reason or no reason at all (Cloudflare, 2022).

### Nginx and Apache TOS

Nginx and Apache are open-source software, while there is a paid option for both, they are predominantly open source. The Apache license agreement was written in 2004, and is predominantly focused on helping the Apache software community develop software in a collaborative fashion (Apache, 2022) There is no mention of misuse of the product or

termination of the license agreement. Nginx on the other hand is a mix of open source and paid service. Nonetheless the Nginx End User Licence Agreement has no explicit reference to prohibited use of their software apart from a series of restrictions on selling the software yourself, reverse engineering or copying the software. Like Cloudflare, Nginx states that the license shall be governed by and construed in accordance with a specific governing law. However, Nginx provide three different possible governing laws based on the specific Nginx entity the user does business with. For users operating in Asia the laws of Singapore apply, for those in Europe the laws of England and Wales apply and for those in the USA the laws of the State of Washington apply (Nginx, 2022).

This presents an issue due to how so many of the websites examined here utilise either Apache or Nginx as a CDN or cached web server. This may point to a similar development as was seen with extremist users of social media platforms. For example the effective disruption of ISIS accounts on Twitter severely hampered their ability to spread propaganda online (Conway et al., 2019), and caused them to migrate to the encrypted messaging application Telegram (Prucha, 2016). When these websites are reported to Cloudflare or Litespeed they may choose to invest in setting up their own CDN utilising partially open source products such as Nginx and Apache.

## Litespeed TOS

Like Nginx and Apache, Litespeed provides both an open source and paid CDN option for users. It is difficult to tell using the methods employed here whether the individuals running these websites are using the paid or open source versions. The End-User License Agreement for LiteSpeed Software sets out the terms of use. The licence to use points out that users may not use the software product for any illegal activity, which like the Cloudflare terms of use would essentially cover a prohibition on the use of their services by proscribed groups and the presence of extremist material. The specific governing law cited by the EULA is the laws of the state of New Jersey and controlling US federal law, although the EULA also sets out its compliance with GDPR. Litespeed adds that it is not liable for the content of any websites powers with their software. If the end user fails to comply with any provision of this EULA, the EULA will terminate immediately without notice from Litespeed. Upon termination the user must destroy all copies of the Litespeed software product, additionally the user can terminate the EULA at any time by destroying all copies of the software product (Litespeed, 2022).

## Squarespace TOS

The web design and hosting service Squarespace also provides its users with a CDN as part of its service. Squarespace sets out its expectations for its users in its terms of service and acceptable use policy. Primarily Section 3.2 of its terms of services states that users must 'Follow the Law', in that the users must represent and warrant that their use of Squarespace services is in compliance with applicable laws. The Acceptable Use Policy goes into more detail, although there is no explicit mention of terrorist or violent extremist content.

The acceptable use policy focuses on a range of inappropriate uses including abusing and disrupting the services such as testing the vulnerability of any system or network, breaching security or authentication or removing any copyright or other proprietary notice from the Squarespace services. The second major category of unacceptable use concerns Fraud and other forms of financial or property crime, such as phishing, deceiving and impersonating others, stealing, and infringing, misappropriating and violating copyright.

Finally, Section 6 of the policy sets out other improper or illegal conduct such as threatening, harassing or abusing individuals, inciting violence, the publication of sexually explicit or obscene material, and condoning or promoting self harm. The policy specifically highlights condoning or promoting violence against any person or group based on race, ethnicity, nationality, religion, gender, gender identity, sexual preference or disability. The prohibition on breaking laws using Squarespace services is repeated (Squarespace, 2022).

In terms of process the Acceptable Use Policy emphasises the discretion of Squarespace in deciding both whether the user's website has misused the services and whether to take action against it. While the company states that 'we try to ensure fair outcomes', they reserve the right to remove content and websites without refund, liability or notice, at any time for any reason (except where prohibited by applicable law). The policy provides an e-mail address where users can report violations of these guidelines directly to Squarespace. Squarespace reserves the right to enforce, or not enforce, the Acceptable Use Policy in their sole discretion and may change this policy from time to time.

## Comparing terms of service

Barring Apache, each of the CDNs described here prohibit the use of their services for illegal means, which would include terrorist websites. Only Squarespace, which provides CDN services for just one of the websites examined here, gives a clear description of what is considered prohibited content or use of their services. Cloudflare only provides such a description for their Web3 product. The remainder rely on referencing the governing law of the jurisdiction their company or organisation is located in. Both Cloudflare and Squarespace provide an e-mail address that concerned parties can use to report the misuse of their products. Notably, none of the terms of service or use make reference to fundamental rights which would apply whether the CDN is considered a caching service or a hosting service. In terms of the hosting service obligation to provide a statement of reasons, possibility of redress or justification for the restriction, none of the terms of use provide any information.

# CONCLUSION

This article has attempted to provide a clearer picture of the issues surrounding CDNs and extremist and terrorist websites. As was demonstrated in the first main section, there are a number of extremist, terrorist and conspiracy websites which cannot operate without employing these CDNs. Cloudflare and Nginx are by far the most popular of those which are examined here. These websites have a wide range in terms of extremism and use of recruitment. Without legal certainty, the moderation and removal of these websites will likely occur in a haphazard way once their respective CDN has received enough negative press attention and complains. As emphasised by Sherman and Ruddock there is a need to widen the lens on content moderation beyond social media networks toward the key internet infrastructure which allows for extremist content to proliferate online. This article as attempted to do so and highlights the need for further study on the technical, legal and practical realities of content moderation on CDNs.

In terms of policy implications; the recently enacted Digital Services Act provides a series of liability exemptions and obligations which differ depending on whether an intermediary service is considered to be a 'hosting' service or a 'caching' service. The issue remains that depending on what function it is fulfilling and who its customer is, a CDN can be considered both a 'hosting' and 'caching' service which provides some confusion as to the level of obligations they must fulfil. This may prove an issue as the terms of service of the CDNs

examined here show that they do not meet the 'hosting' requirements of notice and action mechanisms. Clarifying that a CDN acts as a surrogate host in regard to the content it shares for its customers would allow for legal certainty and for CDN companies to provide due process and possibilities for redress. While this would place additional regulatory burden on these companies the current situation of CDNs playing an integral role in content moderation of websites without any regulatory certainty is unsustainable. At the same time there is a danger that these groups will simply move from more mainstream options such as Cloudflare toward open-source options such as Nginx or Apache, effectively negating the benefits of increased regulation. Future research on this topic will focus on exploring the attributes which make CDNs more or less attractive to extremists and conspiracists and mapping out the challenges of implementing and executing existing legislation on CDNs.

## ORCID

*Seán Looney* http://orcid.org/0009-0007-3114-0806

## ENDNOTE

[1] https://blog.diamwall.com/post/service-continuation-of-kiwi-farms

## REFERENCES

Alexander, D. C. (2011). Student projects involving the analysis of web sites of extremist and extremist-affiliated groups in the United States. *Journal of Applied Security Research*, *6*(2), 184–195. https://doi.org/10.1080/19361610.2011.552004

Apache. (2022). *Apache license, version 2.0*. https://www.apache.org/licenses/LICENSE-2.0

Bloch, K. R., & Myer, Q. W. O. (2018). The normalization of nativism. *Race, Gender & Class*, *25*(3/4), 179–194.

Caiani, M., & Parenti, L. (2009). The dark side of the web: Italian right-wing extremist groups and the Internet. *South European Society and Politics*, *14*(3), 273–294.

Carvalho, H. (2022). *Service continuation of kiwi farms*. https://blog.diamwall.com/post/service-continuation-of-kiwi-farms

Chard, K., Caton, S., Kugler, K., Rana, O., & Katz, D. S. (2017). A social content delivery network for e-science. *Concurrency and Computation: Practice and Experience*, *29*(4), e3854. https://doi.org/10.1002/cpe.3854

Cloudflare. (2022). *Cloudflare website and online services terms of use*. https://www.cloudflare.com/website-terms/

Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A., & Weir, D. (2019). Disrupting daesh: Measuring takedown of online terrorist material and its impacts. *Studies in Conflict & Terrorism*, *42*(1–2), 141–160.

Conway, M., & Looney, S. (2021). *Back to the future? Twenty first century extremist and terrorist websites*.

Dahlke, R., Moore, R. C., Forberg, P., & Hancock, J. (2022). *A mixed methods analysis of Americans' QAnon website consumption*. https://doi.org/10.31219/osf.io/u6vgz

Davies, G., Bouchard, M., Wu, E., Joffres, K., & Frank, R. (2015). 'Terrorist Organizations' use of the internet for recruitment. In M. Bouchard (Ed.), *Social network, terrorism and counter-terrorism: radical and connected*. Routledge.

DIgital Services Act. (2022). *Regulation (EU) 2022/2065 of the European parliament and of the council of 19 october 2022 on a single market for digital services and amending directive 2000/31/EC (Digital Services Act)*.

Donovan, J. (2019). *Navigating the tech stack: When, where and how should we moderate content?* CIGI Online. https://www.cigionline.org/articles/navigating-tech-stack-when-where-and-how-should-we-moderate-content/

European Commission. (2018). Conterfeit and piracy watchlist.

Gkatzikis, L., Sourlas, V., Fischione, C., & Koutsopoulos, I. (2017). Low complexity content replication through clustering in content-delivery networks. *Computer Networks*, *121*, 137–151.

Guhl, J., Ebner, J., & Rau, J. (2020). *The online ecosystem of the German Far-Right*. Institute for Strategic Dialogue. https://www.isdglobal.org/isdpublications/the-online-ecosystem-of-the-german-far-right/

Hanley, H. W., Kumar, D., & Durumenic, Z. (2022). *No calm in the storm: investigating QAnon website relationships*. Proceedings of the International AAAI Conference on Web and Social Media.

Jardine, E. (2019). Online content moderation and the Dark Web: Policy responses to radicalizing hate speech and malicious content on the Darknet. *First Monday*, *24*(12). https://doi.org/10.5210/fm.v24i12.10266

Litespeed. (2022). *End user license agreement for litespeed software*. https://www.litespeedtech.com/docs/webserver/license-enterprise

Maillé, P., & Tuffin, B. (2014). *How do content delivery networks affect the economy of the internet and the network neutrality debate?* 10th International Conference on Economics of Grids, Clouds, Systems, and Services (GECON'2014), Cardiff, United Kingdom.

Mei, J., & Frank, R. (2015). *Sentiment crawling: Extremist content collection through a sentiment analysis guided web-crawler*. 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM).

Nginx. (2022). *Master subscription and services agreement*. https://www.nginx.com/legal/master-subscription-services-agreement/

Pathan, A. M. K., & Buyya, R. (2007). *A taxonomy and survey of content delivery networks*.

Prince, M. (2017). *Why we terminated daily stormer*. https://blog.cloudflare.com/why-we-terminated-daily-stormer/

Prucha, N. (2016). Is and the jihadist information highway–projecting influence and religious identity via telegram. *Perspectives on Terrorism*, *10*(6), 48–58.

Qin, J., Zhou, Y., Reid, E., Lai, G., & Chen, H. (2007). Analyzing terror campaigns on the internet: Technical sophistication, content richness, and web interactivity. *International Journal of Human-Computer Studies*, *65*(1), 71–84.

Ruddock, J., & Sherman, J. (2021). Widening the lens on content moderation. *Joint PIJIP/TLS Research Paper Series*, *69*. https://digitalcommons.wcl.american.edu/research/69

Salahuddin, M. A., Sahoo, J., Glitho, R., Elbiaze, H., & Ajib, W. (2017). A survey on content placement algorithms for cloud-based content delivery networks. *IEEE Access*, *6*, 91–114.

Schwemer, S. F., Mahler, T., & Styri, H. (2021). Liability exemptions of non-hosting intermediaries: Sideshow in the Digital Services Act? *Oslo Law Review*, *8*(1), 4–29.

Squarespace. (2022). *Acceptable use policy*. https://www.squarespace.com/acceptable-use-policy/

Squarespace. (2022). *Terms of Service*. https://www.squarespace.com/terms-of-service

Stocker, V., Smaragdakis, G., Lehr, W., & Bauer, S. (2017). The growing complexity of content delivery networks: Challenges and implications for the internet ecosystem. *Telecommunications policy*, *41*, 1003–1016.

Taylor, J. (2022). *'It's not that hard': Does kicking kiwi farms off the internet prove tech firms can act against hate speech?* The Guardian. https://www.theguardian.com/technology/2022/sep/20/its-not-that-hard-does-kicking-kiwi-farms-off-the-internet-prove-tech-firms-can-act-against-hate-speech

Tech Against Terrorism. (2022). *The threat of terrorist and violent extremist operated websites*.

Thomas, E. (2021). *Open source, self defence: Tackling the challenge of extremist websites and open source tech*. Institute for Strategic Dialogue. https://www.isdglobal.org/wp-content/uploads/2021/08/Open-Source-Self-Defence_v2.pdf

Thomdapu, S. T., Katiyar, P., & Rajawat, K. (2021). Dynamic cache management in content delivery networks. *Computer Networks*, *187*, 107822.

Trivedi, P. M. (2023). Content governance in the shadows: How telcos & other internet infrastructure companies "moderate" Online Content. *Joint PIJIP/TLS Research Paper Series*, *90*.

Yasin, N. A. M. (2014). Understanding the contents in Bahasa Indonesia extremist websites. *Counter Terrorist Trends and Analyses*, *6*(3), 18–24.

Yilu Zhou, Z., Reid, E., Jialun Qin, Q., Hsinchun Chen, C., & Guanpi Lai, L. (2005). US domestic extremist groups on the web: Link and content analysis. *IEEE Intelligent Systems*, *20*(5), 44–51.

Zolfaghari, B., Srivastava, G., Roy, S., Nemati, H. R., Afghah, F., Koshiba, T., Razi, A., Bibak, K., Mitra, P., & Rai, B. K. (2020). Content delivery networks: State of the art, trends, and future roadmap. *ACM Computing Surveys*, *53*(2), 1–34.

**How to cite this article:** Looney, S. (2023). Content moderation through removal of service: Content delivery networks and extremist websites. *Policy & Internet*, 1–15. https://doi.org/10.1002/poi3.370