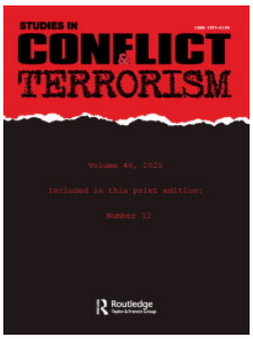

Studies in Conflict & Terrorism

ISSN: 1057-610X (Print) 1521-0731 (Online) Journal homepage: www.tandfonline.com/journals/uter20

The Unintended Consequences of the Removal of Terrorist Content and the Case of Bitchute

Joe Whittaker & Anne Craanen

To cite this article: Joe Whittaker & Anne Craanen (09 Dec 2025): The Unintended Consequences of the Removal of Terrorist Content and the Case of Bitchute, Studies in Conflict & Terrorism, DOI: 10.1080/1057610X.2025.2595843

To link to this article: https://doi.org/10.1080/1057610X.2025.2595843

Published online: 09 Dec 2025.

STUDIES IN CONFLICT & TERRORISM
https://doi.org/10.1080/1057610X.2025.2595843

Routledge
Taylor & Francis Group

The Unintended Consequences of the Removal of Terrorist Content and the Case of Bitchute

Joe Whittaker[a] and Anne Craanen[b]

[a]Department of Criminology, Sociology, and Social Policy, Swansea University and the VOX-Pol Institute; [b]Doctoral Candidate, Swansea University, UK

ABSTRACT

Content removal has become the primary method of countering terrorism online. This can be effective but also entails significant costs. We outline two interrelated ways in which removal leads to negative consequences: creating ideologically homogenous clusters – i.e. "echo chambers" – and forcing malign actors to innovate, potentially increasing the risk of radicalization. We argue that removal must be part of the response, but in some situations, other options may be preferable. We offer a case study of BitChute to demonstrate that if a platform is willing to work against terrorists, it may be better to avoid content removal.

Introduction

In 2014, Benson published a paper in *Security Studies* titled "Why the Internet is not increasing terrorism." In it, he poured cold water on widespread concerns of online radicalization by arguing that, in their pursuit of terrorists, security services gained as much, if not more, from the Internet than the terrorists themselves.[1] He was not the only person at the time to make this assertion. In this journal in 2013, Neumann argued that the tactical intelligence and evidence that could be gained from the Internet was the most effective way of dealing with online radicalization.[2] However, given the movements in both the evolution of terrorism on the Internet and the breakneck pace of technological change over the past decade, these arguments do not seem to have permeated into policy decisions. Instead, successive pieces of legislation and regulation have sought to remove as much terrorist content – such as propaganda and the social media accounts of those sharing it – from the Internet as possible. At first glance, it is difficult to argue with this. After all, we do not want terrorists to be able to communicate, propagandize, and potentially radicalize in any context, including online.

This article seeks to challenge the idea that the current paradigm is the most appropriate way to respond to terrorist exploitation of online platforms. Terrorist content *should* be taken down and removal is a useful weapon in the moderation arsenal, but it also comes with significant unintended consequences which have now

CONTACT Joe Whittaker j.j.whittaker@swansea.ac.uk Department of Criminology, Sociology, and Social Policy, Swansea University and the VOX-Pol Institute.

become apparent. In a sense, we see it as the spiritual successor to the arguments offered by Benson and Neumann above, updated to include the ecosystem a decade on.

What follows below consists of three sections: The first offers a brief introduction to how we got here; the journey to the current policy norm of as much content removal as possible, with a particular focus on the recent pieces of legislation in the European Union, which are likely to set a global precedent for dealing with content online. The second section outlines two interrelated unintended consequences of deplatforming: the forced ideological clustering of supporters to an environment in which terrorist groups have much greater control of their message and creating the incentive to innovate, which has led to much greater resilience against takedowns and to greater operational security for terrorist plots. Taken together, these two consequences may exacerbate radicalization and hamper law enforcement efforts. While research demonstrates that content removal can reduce the reach of terrorist sympathizers online, meaning that fewer people are subjected to recruitment efforts, it is possible that those who do make it find themselves in a considerably more extreme and operationally secure environment.

The third section opens the debate on a more measured and nuanced response to the proliferation of terrorist content online. To do this, we offer the example of BitChute, the video streaming platform to show that in circumstances in which the platform is happy to be a willing participant in the fight against extremism, an array of other options exist, such as helping law enforcement investigations, the algorithmic downranking of problematic content and the amplification of counter narratives. To be clear, we do not advocate for a return to the "wild west" of the early days of the Internet in which little-to-no terrorist content was removed. Clearly, much of it should be. Instead, we argue that there are situations in which relationships with platforms that may play a key role within extremist ecosystems could call for a degree of nuance.

Our article provides several contributions to the existing academic literature. To begin, we provide a small but important contribution to the wider debate of Internet regulation and governance; the majority of the present policy discussion and upcoming legislation is focused on the removal of potentially harmful content from the Internet, but as this article shows, this comes with significant unintended consequences. Moreover, our work adds to the dearth of research on BitChute as a platform, which occupies a central position within extremist ecosystems. Finally, we offer the beginnings of a debate into future solutions in thinking about how social media platforms that are willing to work in the fight against terrorism can leverage their technology in the most useful ways possible.

1. Policy Direction of Travel

In earlier years in the Internet era, there was little motivation from tech companies and nation states to remove content from the Internet. Emboldened by Section 230 of the United States' Communications Decency Act 1996, platforms tended to take the view that they were not liable for content that was posted on their sites.[3] Platforms often believed that because their servers were located in the United States, they were entitled to the strong speech protections offered by the First Amendment, although this was frequently put to the test in instances such as the Yahoo/LICRA case, in

which French courts decided that Yahoo's auction site must geo-block illegal Nazi memorabilia to users located in France.[4] The founders of these tech companies often held philosophical views that were aligned with the First Amendment and were therefore not keen to police what they deemed as political speech on their platform, leading to Twitter's (now X) unofficial motto of the platform being "the free speech wing of the free speech party"[5] or Meta's founder Mark Zuckerberg repeatedly stating that he did not wish to be the arbiter of truth on his platforms.[6]

This approach to content moderation (or lack thereof) was put to the test in the 2010s and the growth of the so-called Islamic State (IS). The group – in addition to its proto-state territorial gains across Syria, Iraq, and beyond – was able to disseminate its sophisticated propaganda far and wide on some of the largest social media platforms on the Internet.[7] In response to widespread condemnation from Western governments, platforms began to take a considerably more proactive approach to jihadist terrorist content toward the end of 2015, banning accounts much more rigorously and utilizing artificial intelligence and hash-sharing technology to degrade such groups' capability to disseminate their materials.[8] Although jihadist groups were the first to be disrupted, similar approaches were eventually applied to many far-right groups, particularly those that have been designated as terrorist organizations, such as National Action or Atomwaffen Division,[9] although multiple problems remain which hamper the ability to disrupt the far-right online.[10] The research from this period often suggests that such degradation was a success; the reach of these groups was demonstrably diminished,[11] causing them to migrate to platforms that either relied on end-to-end encryption[12] – making content more difficult to detect and remove – or platforms that had little or no policy on content removal.[13]

Despite this more proactive approach by some tech companies, legislation that focused specifically on terrorist and extremist content online followed toward the end of the 2010s and into the 2020s. One of the first countries to adopt such legislation was Germany with their Network Enforcement Act (NetzDG) in 2017.[14] Since then, other countries such as Australia (2022)[15] and the United Kingdom (2023)[16] have followed suit, with Canada currently drafting legislation.[17] Despite these pieces of legislation at the national level beginning to appear, the most wide-ranging regulation are the two pieces that were passed by the European Union: the Terrorist Content Online (TCO) regulation and the Digital Services Act (DSA).

The TCO, which came into force in June 2021, is focused on hosting service providers (HSPs) removing terrorist content. HSPs fall within the scope of the regulation if they either have a significant number of users in the EU, or target their activities to one or more member states.[18] The definition of "terrorist content" is informed by the EU Combating Terrorism Directive.[19] The enforcement bodies of the TCO are national "Competent Authorities," that are official bodies in the member states, that can send removal orders to tech companies.[20] Importantly, tech companies then have an hour to remove such material, with the first removal order allowing up to 12 h to get the content removed.[21] Beyond removal, the TCO focusses on implementing transparency and accountability, by stipulating that tech companies publish transparency reports and have accessible appeal mechanisms. HSPs that systematically or persistently

fail to remove content within one hour of receipt of a removal order may incur a fine of up to 4% of global turnover.[22]

The DSA came into force for all platforms in February 2024 and in the European Commission's words is designed to "prevent illegal and harmful activities online… [while ensuring] user safety."[23] The DSA goes beyond regulating hosting service providers and includes three types of intermediary services: mere conduit services, caching services, and hosting services.[24] The intermediaries must either be established in the EU, have a significant number of recipients of its services in an EU Member State, or target its activities toward a Member State. Rather than solely focusing on removal, the DSA focusses on the detection, flagging, and proactive content moderation by platforms and takes a risk-based approach. The DSA sets different requirements for so-called Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), which are defined as those that reach more than 10% of the EU's 450 million consumers, including the need to look at risks created, not just by illegal content, but also legal material that may affect fundamental rights, including public security, gender-based violence, public health, and mental and physical wellbeing.[25] If platforms are deemed to be in breach of the DSA, the European Commission may impose a fine of up to 6% of the global turnover of a VLOP or VLOSE.[26]

The existence of legislation which seeks to both compel platforms to remove terrorist content and force them to have adequate systems to deal with content is a positive step – and certainly better than the years of tech self-regulation that preceded it. However, there is a concern that the incentive structure of both pieces of policy will inevitably lead to the over-removal of content. Barata and Calvet-Bademunt argue that the provisions within the DSA are overly broad and therefore raise several concerns with regard to freedom of expression.[27] There are similar concerns with the TCO; Ahmed notes that the combination of broad definitions of terrorism and the one-hour removal deadline raised criticism from many stakeholders, including the EU Agency for Fundamental Rights and the United Nations Special Rapporteur on freedom of expression.[28] Both the TCO and DSA state that they aim to protect free speech, but the reality is that platforms are being compelled to remove content quickly or face expensive fines and there is no counterweighing incentive to avoid the removal of false positives.

The EU may only represent around 450 million people (around 5% of the world's population), but it is one of the most important players when it comes to legislation because of the so-called "Brussels Effect." In short, because the EU makes up one of the largest markets in the world and is frequently a forerunner in regulation, any global company must meet the EU's often stringent regulatory demands, which tends to facilitate broader compliance in other markets.[29] The Internet is a perfect example of this, and it has been demonstrated that the Global Data Protection Regulation (GDPR) increased data protection compliance far outside the European Union.[30] Nunziato argues that the effect of the DSA will be to incentivize platforms to adopt content moderation policies that are in line with EU regulations, rather than those of the US with its stringent protection of speech under the First Amendment.[31] Burchett makes the same argument with the TCO, noting that it will inevitably apply to all service providers globally that wish to do business within the EU, suggesting that the EU has a substantial capacity to regulate global markets.[32] Therefore, although the

recent regulatory movements only legally apply to the EU, it is likely that they will set precedents across the Internet.

It should be noted that this will not necessarily be a clear and linear effect; in January 2025, Meta have announced a sizable rollback in their moderation policy in the name of free speech,[33] with X having adopted this approach after the takeover in 2022.[34] It remains to be seen how these changes will affect their compliance with regulation; the punishments that are given; and whether they change course afterwards. In forthcoming years we can expect to see an ongoing tussle between platforms and nation states (or institutions such as the EU) who wish to regulate them. A recent example of this is the shutdown of X in Brazil after its Supreme Court ordered it to suspend violative accounts, nominate a legal representative in Brazil, and pay a fine. After originally refusing, X eventually relented.[35] While it is possible that platforms may hold firm on their free speech principles, 30 years of Internet history – from Yahoo/LICRA to Brazil's shutdown of X – has typically demonstrated two things: i) Platforms will obey local law if they are sufficiently incentivized and ii) they often follow the path of least resistance by complying with the regulation of the largest markets (i.e. the "Brussels effect").

2. The Effects of Deplatforming and Migration

2.1. Ideological Clustering and Controlled Messages

While there are demonstrable benefits to the removal of terrorist and extremist content, it is prudent to be cognizant of the negative unintended consequences that it may bring. Although the underlying logic of deplatforming is that it reduces opportunities to become radicalized by stemming the flow of radical content to users, it is possible that it solidifies the online radical milieu for those who are already inside it. Discussing the removal of IS accounts from Twitter in 2015, Berger and Morgan note that suspensions reduce the group's propaganda reach, but do not make it impossible to follow the organization.[36] They express concern that, for those who remain, it is a much louder echo chamber: "The increased stridency and monotonic content may discourage some new members of the network from remaining. For others, there is a risk that the more focused and coherent group dynamic could speed and intensify the radicalization process."[37] They argue that this is analogous to old al-Qaeda training camps, in which individuals were subjected to "cult-like techniques" and cut off from the outside world, and the selection of information was carefully managed by the group.

This argument has also been made in the context of deplatforming the far-right. Rauchfleisch and Kaiser conduct an analysis of 20 YouTube channels that were banned and subsequently moved to BitChute.[38] The authors find deplatforming to be a success insofar as it limits the reach of problematic speech such as extremism and misinformation, since YouTube channels are substantially more likely to have more views and interactions than on BitChute. However, their analysis did show that it was possible for channels to grow in their new home, and most worryingly, that "deplatforming effectively opens up a chance for potential further radicalization" by offering them a place to regroup and strengthen their collective identity.[39]

There is good reason to be concerned that syphoning individuals into ideologically controlled echo chambers could be, as Berger and Morgan suggest, more conducive to radicalization.[40] This observation has proved particularly prescient in the case of platforms such as which are not typically moderated externally. Research demonstrates that acting within an ideologically homogeneous community may lead to more negative sentiment amongst posters.[41] Being within these communities "causes reinforcement and fosters confirmation bias, segregation, and polarization. This comes at the expense of the quality of the information and leads to proliferation of biased narratives fomented by unsubstantiated rumors, mistrust, and paranoia."[42] Analyzing far-right conspiracy narratives, Schulze *et al.*, find that between March 2020 and February 2021, Telegram discourse became more radicalized, with violence-supporting posts increasing significantly. [43] They note that deplatforming measures imposed by Telegram are likely to have shifted to become more radical and moved violence-supporting communications to clandestine areas of the Internet. Similarly, Vergani *et al.* also found hate speech to increase on Telegram channels which hosted conspiracy theories.[44] Discussing IS chatrooms on the same platform, Valentini, Lorusso and Stephan note that moderators have high selection control, unlike on mainstream platforms, and use it to form "radical conclaves" of ideologically homogeneous messages. [45]

It is also possible that echo chambers may lead to *less* toxic language. Mekacher, Falkenberg, and Baronchelli found that when they compared Twitter users to those of Gettr, many more users were banned on the former platform for their posting activity.[46] However, users' language was generally more toxic on the mainstream platform (Twitter)[47] than on the fringe alt-tech site that purports to protect free speech (Gettr). They attribute this to the fact that posters were in close contact with their political adversaries in highly charged discussions, particularly in matters of race and gender. By contrast, they find that fringe platforms offer a safe haven in a politically homogeneous environment with like-minded people. However, this environment and the lack of moderation on Gettr played an important part in offline violence; the authors demonstrate a relationship between the platform and the Brasilia insurrection in 2023, showing that users were "mobilized within a short time period [which led] to real world harms."[48]

It is also likely that censoring fringe views may offer a degree of credibility to propagandists amongst those that are already within the echo chamber. Allington warns that deplatforming may have an exacerbatory effect on radicalization, arguing that their removal from mainstream platforms can have an effect in which individuals are given "martyrdom" status by promoting themselves as censored, giving them more credibility and entrenching the belief that the conspiracy is being further marginalized.[49] Similarly, when IS began to face a more hostile environment on Twitter, scholars argued that it created a community – the "Baqiya family" – which provided emotional and social benefits to members. When individuals are suspended, it signals to other members of the community that they are trustworthy and have paid their dues.[50] Deplatforming was also adopted into the group's propaganda discourse, in which suspensions were framed as a specific tool to persecute Muslims.[51] This level of censorship creates a "Streisand effect" in which censored information is perceived as more valuable because of efforts to suppress it. This is taken by users to be a hostile act by the perceived out-group as an attempt to suppress the "truth."[52]

Another relevant concern is that ideologically homogeneous groups with little-to-no external content moderation may promote false consensus. Humans are generally poor at estimating public support for their beliefs, typically believing their views are more widely shared than is actually the case. Survey-based research on neo-Nazi forums found that individuals overestimated public support and this effect increases as more time is spent engaging on the forum.[53] Experimental research has also demonstrated that individuals are likely to infer public support for their own attitudes from the content that they encounter[54] and that greater use of the Internet makes this effect more likely.[55]

It should be noted that, despite substantial research into the effects of echo chambers online, their role in facilitating political violence is still underdeveloped. This is to say, research shows that they form in online spaces; that terrorists can control their message; and that language tends to become more extreme. However, finding a causal link to participating in political violence is a challenge. There are several reasons for this: Firstly, echo chambers are largely under-theorized and subject to "concept-stretching," secondly, data which successfully bridges the online domain (echo chambers) and offline behavior (violence) is difficult to ascertain and is noisy, and thirdly, establishing causation in any kind of political violence remains elusive.[56]

2.2. Spurring Innovation

The second concern with content removal as a strategy is that it inadvertently creates an extremist ecosystem which is more sophisticated and operationally secure. As discussed above, deplatforming has had demonstrable benefits in disrupting the reach of groups like IS from platforms such as Twitter, Facebook, and YouTube. However, terrorists have learned to adapt to the hostile ecosystem that they face. Fisher, Prucha and Winterbotham outline three categories of platform which are used to maintain a presence online: "Beacons," (e.g. Twitter and Telegram), which direct users to "content stores," (e.g. archive.org and YouTube), which work in tandem with "aggregators" to store and link to content on Facebook pages or websites.[57] These categories of platforms have different uses based on the affordances that they provide and the level of content moderation that they face. The beacons can draw the largest number of users and act as a base of operations. The content stores face the lowest level of moderation (particularly if the meta data do not give away that it is terrorist content) and the aggregators act as places where several links can be spammed without the platforms knowing the nature of the content.

Surveying the jihadist ecosystem in 2022, Fisher and Prucha note that despite the disruption in the mid-2010s, jihadists continue to maintain a persistent presence online, particularly amongst their Arabic-speaking audience. In fact, they argue that the current jihadist ecosystem, of which the pillars are platforms such as Telegram, RocketChat, and Matrix, is "much more dynamic, secure, encrypted, decentralized, and resilient than the [ecosystem] which emerged by 2014."[58] The features of these platforms, they argue, renders many of the current content removal tactics obsolete. Conway, Watkin, and Looney, also observe that despite substantial content removal efforts on many social media platforms, jihadist groups maintain a persistent presence on platforms such as Telegram and RocketChat,[59] while Europol points to the exploitation of

decentralized platforms Ignite and DTube.[60] In their study of jihadist propaganda dissemination strategies, Macdonald and McCafferty analyze 12 channels across four platforms, finding that over half of the 4,164 posts outlinked to other platforms.[61]

Data from Tech Against Terrorism also demonstrate a wide and often sophisticated extremist ecosystem. The Terrorist Content Analytics Platform (TCAP) identifies 13 categories of platforms which are exploited.[62] While it includes many of the platforms discussed above, such as file sharing, social media, and messaging services, it also contains audio sharing, link-shortening, and photo-sharing platforms. Terrorist-operated websites (TOWs) have also become essential to the ecosystem. Conway and Looney identify five different terrorist groups are exploiting TOWs: IS; the Taliban, Hamas, Nordic Resistance, and the PKK.[63] Similarly, Tech Against Terrorism identifies 189 websites used by the far-right, Sunni extremists, and Shia extremists,[64] while Europol highlights that TOWs are a central part of terrorist propaganda strategies.[65] The increased use of cloud-hosted websites creates further challenges since they are used for internal communication as well as for storing of large archives of terrorist content, which is assessed to be due to content removal elsewhere.[66]

The key concern is that it is at best difficult, and at worst, impossible to apply content removal techniques to several platforms in the contemporary ecosystem. Decentralized platforms such as RocketChat, Matrix, Ignite, and DTube, are not controlled by a single entity, but by its individual users operating independently.[67] TOWs are also run independently and as such, the threshold for removal by infrastructure providers is often higher than other tech companies such as social media platforms[68] which in turn gives them greater control over their message.[69] There is some level of moderation on platforms like Telegram, including Europol's "Referral Action Days" in 2018 and 2019 in which they specifically targeted jihadists on the platform. These efforts led to disruptive effects, but they prompted individuals to experiment on new platforms, such as Twitter, Rocket.Chat, TamTam, and nandbox.[70] Even when platforms are successfully taken down, there is an abundance of available options within the terrorist ecosystem and new channels can be set up with considerably more ease than it takes for stakeholders to remove them.[71]

This movement toward creative innovation is familiar to scholars of terrorism and of online conduct more broadly. In their analysis of Telegram, Amarasingam, Maher and Winter draw on the concept of "malevolent creativity."[72] Supporters were driven to migrate due to the hostile ecosystem and their choices of platform were based on three factors: security, sustainability, and utility. In particular, IS' social media strategy of "centralized decentralization" was particularly suited to such creation given that flexible organic structures are more conducive to innovation.[73] Kfir also examines the concept of innovation, finding that IS' forced migration from social media to gaming (and gaming-adjacent) platforms did not stop the group from producing and disseminating their content, but does yield unintended consequences, such as the emergence of uncensored violence and the increased difficulty of content removal.[74] The problem of removing deviant content leading to innovation is not limited to terrorism: Horton-Eddison and Cristofaro demonstrate that the FBI's seizure of the original Silk Road drug market spurred technological innovation toward a more decentralized payment system, arguing that it may have been counter-productive in the long run.[75] Similarly, Reid and Fox highlight how human traffickers and child sexual abusers

adapted to a hostile environment by using the Dark Web and cryptocurrency technologies, which makes law enforcement investigations considerably more difficult.[76]

2.3. How These Consequences Affect Terrorists' Plots

Taken together, these two unintended consequences can work together to create an environment that is more conducive to political violence. The current state of technological innovation has led us to a point in which terrorist groups and their sympathizers have greater control over their messaging because they are not subject to content removal and do not have to sanitize their language to evade platform rules (as they did on platforms such as Facebook or YouTube). This is concerning, given it is the premise of the warning given by Berger and Morgan; groups are able to craft messages with care and be selective about what information enters the group.[77] Similarly, this control is likely to increase the level of false consensus of members within the group.

It is also possible that the forced creativity and innovation has made plots more likely to be successful than before. Empirical research into the online behaviors of terrorists by both Jensen *et al.*[78] and Whittaker[79] demonstrates that terrorists that use social media are less likely to be successful in their plots than those who do not. Both propose that the reason for this could be that radicalizing individuals may be using open social media platforms recklessly and therefore leaving themselves vulnerable to identification by law enforcement. This finding is mirrored by Hamid and Ariza who find that individuals that they classify as "radicalized offline" were three times more likely to be successful in their planned attacks than those who are "radicalized online."[80] To this point, Benson argues that the Internet *does not* increase the risk of terrorism because it is of equal or greater value to law enforcement than it is to terrorists.[81] An illustrative example of this is Lloyd Gunton, who – in advance of his planned attack – asked his Instagram followers "Cardiff, are you ready for our terror?" which led to his apprehension by law enforcement.[82] However, these scales may have now tipped in the opposite direction: content removal may have displaced a lot of low-hanging fruit from platforms such as Facebook or Twitter (who generally comply with court orders to share user data with law enforcement) to platforms that are either unwilling or unable comply. To put it simply, would-be terrorists are often reckless, and the removal of their accounts or content may be forcing them to think more about their operational security.[83]

3. Breaking the Impasse

Rather than blanket banning content and creating pariah platforms, it may be prudent to consider options that keep problematic content within arm's reach (for platforms that want it) and work proactively together. This will create options that are not available when content is removed and extremists migrate to security-focused platforms, such as sharing relevant information with law enforcement and prosecutors; down-ranking borderline content; and algorithmically amplifying strategic communications. To demonstrate this point, we offer a hypothetical case study of how a platform – Bitchute – could be utilized to achieve this.

3.1. Bitchute

BitChute is a video-sharing platform hosted in the United Kingdom. The platform, which uses WebTorrent, was set up in 2017 by Ray Vahey, who, when asked about why he created the platform, said "the idea comes from seeing the increased levels of censorship by the large social media platforms in the last couple of years. Bannings, demonetization, and tweaking algorithms to send certain content into obscurity and, wanting to do something about it."[84] The platform quickly became known as the alternative to YouTube and is in a way, itself, a product of deplatforming.[85] BitChute is hosted on Epik, a domain name registrar which is known to host far-right extremist websites.[86]

Given the platform's intention to host content that was being removed by bigger social media platforms, BitChute quickly became a safe haven for far-right extremists. This led BitChute to be banned from both Paypal and Stripe in 2019.[87] The extent of the problem was brought to light in 2020, when three research and policy institutes – Hope Not Hate,[88] the Anti-Defamation League,[89] and the Community Security Trust[90] – each wrote reports on the state of BitChute and the alarming volume of extremist and terrorist content found on the platform. The reports also highlight the prevalence of far-right content, antisemitic material, anti-LGBTQIA+ hate speech, misogynistic material, disinformation, and conspiracy theories on the platform. More recently, Trujillo *et al.* conducted an empirical assessment of the platform, finding there to be more hate speech than on the alt-tech platform Gab, but less than 4Chan.[91]

The Hope Not Hate report by Davis found that there was official content produced by several designated terrorist organizations including Atomwaffen Division[92] and National Action[93] on BitChute, in addition to official content produced by IS.[94] In addition, crisis material was also detected, predominantly the livestream and manifesto created by the Christchurch attack perpetrator who killed 51 people on March 15, 2019. The manifesto and the livestream are classified as illegal by the New Zealand Classification Office.[95]

More recently, there has been a substantial policy shift in the removal of officially designated terrorist content. Examining the platform in 2022, the UK's communications watchdog and regulator of the Online Safety Act, Ofcom, and Tech Against Terrorism have both elaborated on their positive engagement with BitChute over the previous two years.[96] Since Tech Against Terrorism started working with BitChute in 2020, the platform has removed all terrorist content reported by Tech Against Terrorism (including crisis material in case of the Christchurch attack and Buffalo shooting). The platform has also added violent extremist groups to its banned organizations list, incorporated a user-reporting feature, and produced several transparency reports to date.[97] The first transparency report published by BitChute mentions that between 2017 and 2021 the company grew from 2 part-time founders to 12 employees. This increased their content moderation capacity and shows an increased commitment to responding to terrorist content on the platform.[98] Since then, Bitchute has published another transparency report for 2023.

Ofcom notes that while it still considers BitChute to be an attractive option for hosting harmful content, due to the nature of the platform, it has nonetheless been able to engage constructively with the company following the introduction of the

interim regime that regulates video-sharing platforms.[99] In response to the attack in Buffalo,[100] "BitChute has consistently removed content violating its terms and conditions when third party organisations have reported it to them, including footage of the Buffalo attack."[101] Regarding material which is illegal under specific statutes, BitChute also has a portal to report content that is illegal under the German Network Enforcement Act (NetzDG).

If BitChute were to use content removal as its primary method of countering extremism, it could lead to moving some individuals directly toward extremist recruiters. Parler, an alt-tech social media platform, was forcibly shut down after being implicated in the attack on the Capitol on January 6, 2021. After the shutdown, there was a mass migration to Telegram in the course of which Trump supporters joined more extreme far-right channels where violent extremists were actively trying to recruit them.[102] If BitChute were to be completely shut down or implement a substantially more restrictive content removal policy, this may create a further migration to terrorist and violent extremist spaces on Telegram or decentralized platforms. As discussed above, recruiters have substantially more control within such spaces, and they may prey on individuals who have identifiable risk factors, such as a belief in conspiracy theories,[103] which are prevalent on BitChute, to which a grievance narrative can be added under controlled supervision.

3.2. How Can Bitchute Respond to Violent Extremism?

As discussed above, one risk of deplatforming violent extremists and terrorists is that they are likely to migrate to platforms or parts of the online terrorist ecosystem that are increasingly hard to moderate, because there is no infrastructure and no desire to do so, such as decentralized or end-to-end encrypted platforms, fringe platforms, or terrorist operated websites. On these sites, it is very hard for material to be removed or for communications to be monitored, which, as we argued in the first section, may create an unintended consequence whereby law enforcement miss low-hanging fruit because users migrate to platforms in which detection is more difficult.

However, BitChute's commitment to protect potentially problematic speech means that most of the content is unlikely to be removed unless it is officially designated or deemed to be illegal. This means that users may be more likely to leave the low-hanging fruit for law enforcement. Of course, leaving such content online comes with a substantial tradeoff; even if the content is not classified as terrorist, it does not mean that it is not harmful. Rather, even if it does not explicitly call for violence, borderline content could function as "mood music" in the radicalization process.[104] However, as demonstrated above, the idea of stopping all interested individuals from finding such content is not feasible, but restricting the reach of such content may be. Allowing some platforms to host this type of "mood music," while also removing explicitly terrorist content, may be the most pragmatic compromise. Finally, given that this type of content dominates the platform, the political environment is highly homogenous. This may limit the toxicity that would be experienced by users with other political viewpoints, as demonstrated by Mekacher, Falkenberg, and Baronchelli in their analysis of users espousing more toxicity on Twitter than on Gettr, given Gettr's homogenous environment.[105]

Another important point to note is that the platform architecture of BitChute is open; they allow users to view material without creating an account and as such, users have little control over who views their content. This openness makes it unlikely that many extremists and terrorists will use BitChute for operational purposes, including for secure internal communications, attack planning, recruitment, or fundraising, when the likelihood that their communications will go undetected and undisrupted is low. However, given that many terrorists *do* recklessly telegraph their intentions on public platforms,[106] it means that the platform is well-suited for law enforcement to detect individuals that are doing so.

As well as detecting and foiling violent attacks, working with open platforms that are willing to cooperate with law enforcement also provides a means of successfully prosecuting individuals. Benson argues that companies based in the West, such as the Silicon Valley tech giants, are liable to be receptive to subpoenas and to surrender their data.[107] On the other hand, platforms with distributed data structures, such as Telegram, do not respond to subpoenas or data requests because their architecture does not support it.[108] An example is the case of Nicholas Rovinski, who was convicted as part of a small cell of individuals that plotted to kill Pamela Gellar. Rovinski left a long trail of information on several social media platforms including YouTube, Twitter, and Google+, and a court-ordered warrant allowed them to trace back his communications with coconspirator David Wright on Facebook.[109] It is not clear that this case could be so easily built in today's ecosystem.

In short, extremists will continue to exploit online platforms, many of which will be unwilling to work with law enforcement agencies, regulators, and third parties. As such, having a platform in the ecosystem such as BitChute that is somewhat cooperative with law enforcement and court orders may end up being a net benefit, even if it comes at the cost of objectionable material remaining on the platform.

3.3. Other Moderation Options

BitChute utilizes content removal to moderate online terrorist - and to some extent - extremist content. Furthermore, the open nature of the platform minimizes the risk of terrorists using BitChute for operational and recruitment purposes. Where the platform would be used for operational purposes, it is likely that law enforcement would be able to monitor such behavior and work with BitChute given the platform's previous history of cooperation with regulators and third-party organizations.

However, the reliance on content removal and neglecting other strategies does not optimally reduce the threat of violent extremism. It risks BitChute causing unintended consequences by relying on content removal, such as users moving to more secure and unmoderated platforms. Below, we suggest alternative measures BitChute, and similar platforms, could take to challenge terrorists and extremists to an even greater extent, ensuring that the platform features are utilized optimally, whilst accepting that a certain level of hate speech is likely to stay on the platform.

3.3.1. Downranking

A strategy that is often employed by the larger and more mainstream social media platforms is reducing the prevalence of problematic content. As Whittaker discusses

in his literature review of extremist content and recommendation systems, many platforms – including Facebook, YouTube, Twitter/X, and Reddit – have taken to downranking what they call "borderline content," which is content that is not clearly terrorist, violent, or illegal, but which platforms nonetheless do not want their algorithms to promote.[110] This is generally presented as a compromise between user safety and free speech.

BitChute employs a recommendation algorithm which they call "People Power," which ranks specific types of content to the top of the home screen, as determined by the number of subscribers, views, and likes (in a manner that is similar to many other platforms, although –from what detail is given – is more simplistic than sites such as Twitter, YouTube, or Facebook). Although we argue above that the amount of terrorist material on BitChute is low, at the time of writing, and as reports and articles have shown, content on the platform mostly centers around disinformation and often racist, misogynistic, and antisemitic material. Therefore, the amount of hate speech and disinformation on BitChute is extremely high and through its People Power feature, problematic material is lifted to the top of BitChute's feed. In addition, personal feeds are tailored to a person's individual preferences which again risks frontloading material that is borderline or worse in nature.[111]

There is potential for BitChute to use its recommendation system to drown out extremist rhetoric by downranking it. As Gillespie notes, this has become a popular form of content moderation for the largest mainstream social media platforms.[112] Moreover, it can be a flexible strategy depending on the users and content in question. He highlights three ways in which content can be made less visible:

1. Do not recommend *at all* - the content or creator is completely removed from recommendations;
2. Do not recommend *as much* - problematic content can be included, but is ranked lower the non-problematic content;
3. Do not recommend *to some* - either of 1) or 2) could be applied specifically to users based on a range of factors including age, time of day, geo-location, or watching history.

Content flagged as "Not Safe for Life" [NSFL] and/or "Not Safe for Work" [NSFW] could be omitted or downranked from the Power People, meaning that users would have to specifically search for it.

It is important that downranking is not confused with the colloquial Internet concept of "shadow banning" – when a user or their content is muted (or their content is made harder to find) without their knowledge.[113] The key differentiation here is transparency – platforms should make it clear that downranking is part of their moderation toolkit and users should be made aware when their content is downranked. An example of this in action is on Twitter/X, where a downranked post can carry the text "Visibility Limited: this post may violate X's rules on hateful conduct."[114]

To be clear, we argue that illegal material should be subject to content removal. However, we also acknowledge that there will always be a substantial grey area in which content is not clearly illegal. Moreover, the premise of our argument is that problematic content *will* appear online, and it may be better for cooperative platforms

to bias algorithmic preferences actively, rather than sending extremists in a single stroke to the darkest corners of the Internet, where they have complete control of their message. However, even if content is downranked, as opposed to removed, there are still clearly important free speech implications that should be carefully considered. Macdonald and Vaughan highlight three ways in which downranking can be improved to be in line with human rights norms: greater definitional clarity of what constitutes "borderline content;" the necessity and proportionality of downranking; and transparency.[115]

3.3.2. Uplifting Strategic Communications

The downranking of content may be unpalatable for BitChute, particularly given the founder has complained about YouTube "tweaking algorithms to send certain content into obscurity."[116] However, the same technology can be used to create debate and provide additional voices. Vahey has articulated that one of his aims with BitChute is to call out extremist narratives and let them be debated.[117] However, given that monotonic content dominates, there is presently little scope for drowning out extremist or borderline content with strategic communications.

Therefore, strategies to counter extremism ought to go further than merely removing or downranking content because it "creates an information vacuum, and vacuums will always be filled. Whilst disruption is one side of the coin, the other necessary side is an effective communication strategy to control what fills the vacuum."[118] Many social media platforms are already doing this. Facebook (even after its change in moderation policy) *Removes* violative content, *Reduces* misleading content, and *Informs* users with additional context where necessary.[119] Similarly, as well as *Removing* violative content and *Reducing* (i.e. downranking) borderline content, YouTube is also *Raising* authoritative speakers and *Rewarding* trusted voices,[120] although the mechanisms of how these voices are raised are not clear.

This strategy could be deployed by means of a partnership between BitChute and third-party message designers to introduce fact-checking. This would confer legitimacy and credibility on the platform and would warn users that what they are seeing is deemed inaccurate by experts. While this may not convince users who strongly oppose the presence of such information given their existing beliefs, it will create room for more debate on the platform, which could potentially be viewed by third-party bystanders. It also raises the possibility of counter-narratives, which are often maligned for lacking evidence of efficacy.[121] However, recent empirical research suggests that well-crafted messages may show more promise. Braddock demonstrates that "inoculation" messages in advance of an extremist narrative can promote resistance to persuasion,[122] while Carthy and Sarma found that offering individuals a tailored counter-narrative, which invited individuals to write down counterarguments to violence, made them less likely to be supportive of extremist propaganda.[123]

The tactics of downranking potentially problematic content and the raising of trusted or counter-narrative sources have the ability to break the existing ideological clustering that appears on BitChute.[124] In essence, such tactics give less power to extremist content creators and present opposing views to their potential audiences. While there are free speech issues engaged by downranking (although clearly fewer than removing it entirely), the idea of allowing for a wider range of voices to be heard in any given

debate is congruent with the founder's commitment to debate and free speech. Given BitChute's willingness to moderate and work with the regulator and third-party organizations, they may be more open to this approach, and a unique opportunity may have arisen for counter narratives to be delivered where terrorists sympathizers are currently congregating.

While we believe that this approach can help to effectively counter terrorism online, it is not without limitations. To begin, it clearly requires online platforms to play ball and buy in to the concept of countering terrorism, and apply moderation techniques to borderline content, which is highly politicized. Many platforms have positioned themselves as an alternative to the mainstream and as such being seen to cooperate with governments' counter-terrorism policies may be unpalatable. However, we believe that there are enough platforms – like BitChute – who can straddle the divide between "alternative" and advocating for free speech, while also accepting terrorism as a problem to be challenged. Secondly, both downranking and counter-narratives may be unpopular with the users on these platforms. People do not like to feel like they are being manipulated which can cause interventions to backfire – this is sometimes called "psychological reactance."[125] Put simply, if users feel like they are trying to have their minds changed, they may dig their heels in and believe *more deeply* in their original idea. This is why the types of counter-narrative that are presently showing the most promise – inoculation – attempt to use psychological reactance to their advantage by creating messages to show that extremists are trying to manipulate them.[126]

There are also other approaches that we have not covered here that could be used in conjunction with those that we have suggested. One is what could be called "mowing the grass" – platforms operating a permissive everyday environment then intermittently purging content.[127] The idea is that this is done infrequently enough as to not foster innovation, but frequently enough to damage terrorists' reach and networks. There is little-to-no academic literature on this tactic, although Telegram's occasional collaboration with Europol in their "Referral Action Days" would be an example. Given the dearth of literature, we believe it is a good candidate for future empirical research.[128]

Finally, the case study of BitChute and our potential recommendations only speak to how one individual platform may benefit from not removing some types of content. As we discussed in part 2, terrorists now operate in a wide and complex ecosystem, meaning that they could use a platform such as BitChute for hosting "borderline" ideological material while hosting other content, such as operational planning or fundraising on more secure platforms. This is an inevitable aspect of the contemporary Internet, and it is why we argue that regulation which mandates content removal is still a vital tool for disrupting. However, our argument is that we should work within the confines and realities of the ecosystem that exists; if there is a possibility to work with some platforms that host problematic content and provide either law enforcement or counter-extremism interventions, this may be preferable to indiscriminately enforcing widespread removal of content.

Conclusion

While it is a laudable goal to attempt to remove all problematic content from the Internet, the contemporary web does not allow us to do this, nor does it save us from

the negative unintended consequences entailed by attempting to do so. In this article, we have argued that platforms need not face a binary choice between "remove as much as possible" or "remove nothing," but that a realistic view can be taken which accepts our limitations and attempts to mitigate them. The current focus on content removal has allowed a sophisticated terrorist ecosystem to evolve which has become, and will continue to become, harder to penetrate. While the large-scale removal of terrorists and extremists from many mainstream platforms has successfully reduced their reach to new recruits, this has come at the expense of increasing their operational security and resilience to content takedown.

Given that we do not live in a perfect world, it may be better to attempt to leverage those platforms uniquely placed to help to counter extremism. To further explain this point, we have drawn on the case study of BitChute; a platform which has shown willingness to remove *terrorist* content, but still maintains a firm stance against most other types of content removal. Therefore, if terrorists and extremists still wish to access this platform, they must do so on an "open" platform which cooperates with court orders, where they will not find designated terrorist content, and in which borderline content may be subjected to downranking and supplementary narratives which attempt to seize control of the information environment. This is a somewhat hypothetical case study; we do not speak for BitChute, and it is entirely possible that they will not wish to cooperate as we have suggested. Instead, this article offers a prospectus of the ways in which other tactics can be deployed to mitigate some of the unintended consequences of the current content moderation paradigm.

We also recognize that this discussion cannot exist independently of a broader ethical debate about the harms of allowing, removing, and downranking content. We chose the language of this article carefully; within the field of applied ethics there is a long history of debates on "unintended consequences" – dating back to Thomas Aquinas – which evaluate the permissibility of actions that are intended to achieve a good outcome but in doing so may cause harm. The removal or otherwise of terrorist and extremist content involves ethical debates such as free speech (concerning both those who abuse its freedoms and those who are denied them), the rule of law, as well as business ethics and corporate social responsibility. It is also worth noting that for some, the good outcome may simply be the removal of problematic content, rather than the long-term effect of a reduction in violent extremism. Other parts of this article can also not be discussed without recognition of wider debates; it would be simplistic to claim that "helping law enforcement" is to be an undeniable good given the range of ways in which these powers have been abused and often target already vulnerable populations.[129] In this sense, we offer a small, but we hope important, contribution to this wider debate.

Notes

1. David C. Benson, "Why the Internet is Not Increasing Terrorism," *Security Studies* 23, no. 2 (2014): 293–328, doi: 10.1080/09636412.2014.905353.
2. Peter Neumann, "Options and Strategies for Countering Online Radicalization in the United States" *Studies in Conflict & Terrorism* 36, no. 4 (2013): 431–459.

3. Maura Conway, "Routing the Extreme Right: Challenges for Social Media Platforms," *RUSI Journal* 165, no. 1 (2020): 108–113, doi: 10.1080/03071847.2020.1727157.
4. Marc Greenberg, "A Return to Lilliput: The LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market" *Berkeley Technology Law Journal* 18, no. 4 (2003): 1191–1258.
5. Josh Halliday, "Twitter's Tony Wang: 'We are the Free Speech Wing of the Free Speech Party'." *The Guardian*, March 22, 2012, https://www.theguardian.com/media/2012/mar/22/twitter-tony-wang-free-speech.
6. Tom McCarthy, "Zuckerberg Says Facebook Won't be 'Arbiters of Truth' After Trump Threat." *The Guardian*, May 28, 2020, https://www.theguardian.com/technology/2020/may/28/zuckerberg-facebook-police-online-speech-trump.
7. J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," *The Brookings Project on U.S. Relations with the Islamic World*: Analysis Paper, March 2015; Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq" *Studies in Conflict & Terrorism* 38, no. 1: 1–22.
8. J. M. Berger and H. Perez, "The Islamic State's Diminishing Returns on Twitter: How Suspensions are Limiting the Social Networks of English-Speaking ISIS Supporters," *George Washington University: Program on Extremism*, February 2016, 1–20, https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional%20Paper.pdf; Maura Conway, "Violent Extremism and Terrorism Online in 2016: The Year in Review," *Vox Po*l, December 2016.
9. Tech Against Terrorism, "Terrorist Content Analytics Platform: Transparency Report," 2021.
10. Maura Conway, 'Routing the Extreme Right."
11. Maura Conway, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson, and David Weir, "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts," *Studies in Conflict and Terrorism* 42, no. 1–2 (2018): 141–160, doi: 10.1080/1057610X.2018.1513984; Daniel Grinnell, Stuart Macdonald, David Mair, and Nuria Lorenzo-Dus, "Who Disseminates Rumiyah? Examining the Relative Influence of Sympathiser and Non-sympathiser Twitter Users," April 2018.
12. Chamin Herath and Sneha Dawda, "Balancing End-to-End Encryption and Public Safety," *RUSI Occasional Paper*, 2022.
13. Lella Nouri, Nuria Lorenzo-Dus, and Amy-Louise Watkin, "Impacts of Radical Right Groups' Movements across Social Media Platforms – A Case Study of Changes to Britain First's Visual Strategy in Its Removal from Facebook to Gab," *Studies in Conflict & Terrorism* (2021), doi: 10.1080/1057610X.2020.1866737.
14. "Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech," Global Legal Monitor, July 6, 2021, https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/#:~:text=In%202017%2C%20Germany%20passed%20the,noncompliance%20with%20existing%20legal%20obligations (accessed October 2023).
15. Government of Australia, "Learn about the Online Safety Act" *eSafety Commissioner* (n.d.), https://www.esafety.gov.au/newsroom/whats-on/online-safety-act.
16. HM Government, "Online Safety Act: Explainer," (n.d.), https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer.
17. Government of Canada, "Proposed Bill to Address Online Harms" (n.d.), https://www.canada.ca/en/canadian-heritage/services/online-harms.html.
18. Thomas Wahl, "Rules on Removing Terrorist Content Online Now Applicable, EUCrim, June 7, 2022, https://eucrim.eu/news/rules-on-removing-terrorist-content-online-now-applicable/.
19. European Union Agency for Fundamental Rights, "Directive (EU) 2017/541 on Combating Terrorism — Impact on Fundamental Rights and Freedoms – Summary," September 28, 2022, https://fra.europa.eu/en/publication/2022/directive-eu-2017541-combating-terrorism-impact-fundamental-rights-and-freedoms.
20. European Commission, "List of National Competent Authority (Authorities) and Contact Points" *Migration and Home Affairs*, July 25, 2024, https://home-affairs.ec.europa.eu/policies/

internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en.
21. Tech Against Terrorism Europe, "European Regulation on Terrorist Content Online (TCO)" (n.d.), https://www.techagainstterrorism.org/hubfs/TCO-Guide.pdf.
22. Ibid.
23. European Commission, "The Digital Services Act" (n.d.), https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.
24. Ibid.
25. European Commission, "DSA: Very Large Online Platforms and Search Engines" (n.d.), https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops.
26. European Commission, "The Enforcement Framework Under the Digital Services Act" (n.d.), https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement.
27. John Barata and Jordi Calvet-Bademunt, "The European Commission's Approach to DSA Systemic Risk is Concerning for Freedom of Expression" *Tech Policy Press* (2023). https://www.techpolicy.press/the-european-commissions-approach-to-dsa-systemic-risk-is-concerning-for-freedom-of-expression/.
28. Reem Ahmed, "Negotiating Fundamental Rights: Civil Society and the EU Regulation on Addressing the Dissemination of Terrorist Content Online" *Studies in Conflict & Terrorism* (2023).
29. Anu Bradford, *The Brussells Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020).
30. René Mahieu, Hadi Asghari, Christopher Parsons, Joris van Hoboken, Masashi Crete-Nishihata, Andrew Hilts, Siena Anstis, "Measuring the Brussels Effect through Access Requests: Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens?" *Journal of Information Policy* 11 (2021): 301–349.
31. Dawn Carla Nunziato, "The Digital Services Act and the Brussels Effect on Platform Content Moderation" *Chiago Journal of International Law* 115 (2023): 115–128.
32. Julia Burchett, "Countering Extremist Ideologies: What are the Synergies Between the EU's Internal and External Action?" *New Journal of European Criminal Law* 14, no. 2 (2023): 138–156.
33. Hannah Murphy and Daneil Thomas, "Meta's 'Free Speech' Overhaul Sparks Advertisers' Concern." *Financial Times*, January 12, 2025, https://www.ft.com/content/9b33c935-1da6-4c81-ab0b-cba8c781c702
34. Mathieu Pollet, "Elon Musk's X Tells the EU: We're a Safe Space for Free Speech," *Politico*, November 28, 2024, https://www.politico.eu/article/elon-musks-x-eu-safe-space-free-speech-digital-services-act/#:~:text=and%20hate%20speech.-,X%20said%20it%20had%20moved%20from%20a%20%22binary%2C%20absolutist%20take,accounts%20than%20ban%20them%20altogether.
35. Corynne McSherry, "The X Corp. Shutdown in Brazil: What We Can Learn," *Electronic Frontier Foundation*, October 8, 2024, https://www.eff.org/deeplinks/2024/10/x-corp-shutdown-brazil-what-we-can-learn.
36. J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," *The Brookings Project on U.S. Relations with the Islamic World*: Analysis Paper, March 2015.
37. Berger and Morgan, "Twitter," 58.
38. Adrien Rauchfleisch and Jonas Kaiser, "Deplatforming the Far-Right: An Analysis of YouTube and BitChute" (2021), Available at SSRN: https://ssrn.com/abstract=3867818 or http://dx.doi.org/10.2139/ssrn.3867818.
39. Rauchfleisch and Kaiser, "Deplatforming," 23.
40. Berger and Morgan, "Twitter."
41. Michela Del Vicario, Gianna Vivaldo, Alessandro Bessi, Fabiana Zollo, Antonio Scala, Guido Caldarelli, and Walter Quattrociocchi, "Echo Chambers: Emotional Contagion and Group Polarization on Facebook," *Nature Publishing Group* (2016): 1–14, doi: 10.1038/srep37825.
42. Michela Del Vicario, Alessandro Bessi, Fabiana Zollo, Fabio Petroni, Antonio Scala, Guido Caldarelli, H. Eugene Stanley, and Walter Quattrociocchi, "The Spreading of Misinformation

Online," *Proceedings of the National Academy of Sciences* 113, no. 3 (2016): 554–559, doi: 10.1073/pnas.1517441113.
43. It should be noted that posts rejecting violence also increased over this time. Heidi Schulze, Julian Hohner, and Diana Rieger, "Far-right Conspiracy Groups on Fringe Platforms: A Longitudinal Analysis of Radicalization Dynamics on Telegram," *Convergence: The International Journal of Research into New Media Technologies* (2022), doi: 10.1177/13548565221104977.
44. Matteo Vergani, Alfonso Martinez Arranz, Ryan Scrivens, and Liliana Orellana, "Hate Speech in a Telegram Conspiracy Channel During the First Year of the COVID-19 Pandemic," *Social Media and Society* 8, no. 4 (2022), doi: 10.1177/20563051221138758.
45. Daniele Valentini, Anna Maria Lorusso, and Achim Stephan, "Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization," *Frontiers in Psychology* 11 (2020), doi: 10.3389/fpsyg.2020.00524.
46. Amin Mekacher, Max Falkenberg, and Andrea Baronchelli, "The Systemic Impact of Deplatforming on Social Media," *Cornell University*, March 2023, https://doi.org/10.48550/arXiv.2303.11147.
47. This research was published prior to Musk's rebranding of Twitter to X with subsequent changes to content moderation on the platform.
48. Mekacher, Falkenberg, Baronchelli, "systemic impact," 7.
49. Daniel Allington, "Conspiracy Theories, Radicalisation and Digital Media," *Global Network on Extremism & Technology*, 2021.
50. Amarnath Amarasingam, "What Twitter Really Means For Islamic State Supporters," *War on the Rocks,* 2015, https://warontherocks.com/2015/12/what-twitter-really-means-for-islamic-state-supporters/.
51. Elizabeth Pearson, "Online as the New Frontline: Affect, Gender, and ISIS-Take-Down on Social Media," *Studies in Conflict and Terrorism* (2017), doi: 10.1080/1057610X.2017.1352280.
52. Miron Lakomy, "Why Do Online Countering Violent Extremism Strategies Not Work? The Case of Digital Jihad," *Terrorism and Political Violence* (2022), https://doi.org/10.1080/09546553.2022.2038575.
53. Magdalena Wojcieszak, "False Consensus Goes Online Impact of Ideologically Homogeneous Groups on False Consensus," *Public Opinion Quarterly* 72, no. 4 (2008): 781–791, doi: 10.1093/poq/nfn056.
54. Róbert Lusz and Susanne Mayr, "False Consensus in the Echo Chamber: Exposure to Favorably Biased Social Media News Feeds Leads to Increased Perception of Public Support for Own Opinions," *Cyberpsychology* 15, no. 1 (2021): 1, doi: 10.5817/CP2021-1-3.
55. Christopher J. Bunker and Matthew E. W. Varnum, "How Strong Is the Association Between Social Media Use and False Consensus?" *Computers in Human Behavior* 125 (2021): 106947, doi: 10.1016/j.chb.2021.106947.
56. Joe Whittaker "Online Echo Chambers and Violent Extremism," in *The Digital Age, Cyber Space, and Social Media: The Challenges of Security & Radicalization*, ed. Syed Munir Khasru & Riasat Noor (Dhaka: Institute for Policy, Advocacy and Governance, 2020), 129–150.
57. Ali Fisher, Nico Prucha, and Emily Winterbotham, "Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability," *Global Research Network on Terrorism and Technology*, no. 6 (2019).
58. Fisher and Prucha, "Mapping," 4.
59. Maura Conway, Aloyse Laetitia Watkin, and Sean Looney, "Violent Extremism and Terrorism Online in 2021: The Year in Review," *Radicalisation Awareness Network* (2022), http://www.voxpol.eu/download/vox-pol_publication/Year-In-Review-WEB.pdf.
60. Europol, "Terrorism Situation and Trend Report: 2022" (2022).
61. Stuart Macdonald and Sean McCafferty, "Online Jihadist Propaganda Disseminations Strategies," Vox Pol, 2024.
62. Tech Against Terrorism, "Terrorist Content Analytics Platform: Transparency Report," 2021.

63. Maura Conway and Sean Looney, "Back to the Future? Twenty First Century Extremist and Terrorist Websites," *Radicalisation Awareness Network* (2022).
64. Tech Against Terrorism, "The Threat of Terrorist and Violent Extremist-Operated Websites," January 2022, https://www.techagainstterrorism.org/2022/01/28/report-the-threat-of-terrorist-and-violent-extremist-operated-websites/.
65. Europol, "Trends."
66. Tech Against Terrorism, "Trends in Terrorist and Violent Extremist Use of the Internet | Q1–Q2 2021," (July 2021), pp. 1–6.
67. Conway, Watkin, and Looney, "Violent Extremism."
68. Tech Against Terrorism, "Websites."
69. Conway and Looney, "Future."
70. Amarnath Amarasingam, Shiraz Maher, and Charlie Winter, "How Telegram Disruption Impacts Jihadist Platform Migration," *CREST* (2021).
71. Lakomy, "Digital jihad."
72. Amarasingham, Maher, and Winter, "Telegram."
73. Paul Gill, John Horgan, Samuel T. Hunter, Lily D. Cushenbery, "Malevolent Creativity in Terrorist Organizations," *Journal of Creative Behavior* 47, no. 2 (2013): 125–151, doi: 10.1002/jocb.28.
74. Isaac Kfir, "Innovating to Survive: A Look at How Extremists Adapt to Counterterrorism," *Studies in Conflict & Terrorism* (2021), doi: 10.1080/1057610X.2021.1926069.
75. Martin Horton-Eddison and Matteo Di Cristofaro, "Hard Interventions and Innovation in Crypto-Drug Markets: The Escrow Example," *Global Drug Policy Observatory*, Policy Brief (2017).
76. Joan Reid and Bryanna Fox, "Human Trafficking and the Darknet: Technology, Innovation, and Evolving Criminal Justice Strategies," *Advanced Sciences and Technologies for Security Applications* (June 2020): 77–96, doi: 10.1007/978-3-030-41287-6_5.
77. Berger and Morgan, "Twitter."
78. Michael Jensen, Patrick James, Gary LaFree, Aaron Safer-Lichtenstein, and Elizabeth Yates, "The Use of Social Media by United States Extremists," *National Consortium for the Study of Terrorism and Responses to Terrorism* (2018).
79. Joe Whittaker, "The Online Behaviors of Islamic State Terrorists in the United States," *Criminology and Public Policy* 20 (2021): 177–203, doi: 10.1111/1745-9133.12537.
80. Nafees Hamid and Cristina Ariza, "Offline Versus Online Radicalisation: Which is the Bigger Threat?" *Global Network on Extremism & Technology* (2022).
81. Benson, "Why the Internet is Not Increasing Terrorism."
82. Lizzie Dearden, *The Plotters: The UK Terrorists Who Failed* (London: Hurst, 2023).
83. Whittaker, "Online Behaviours."
84. Andy Maxwell, "BitChute is a BitTorrent-Powered YouTube Alternative," *Torrent Freak*, January 29, 2017, https://torrentfreak.com/bitchute-is-a-bittorrent-powered-youtube-alternative-170129/.
85. Community Security Trust, Hate Fuel: The Hidden Online World Fuelling Far Right Terror (2020).
86. Anti-Defamation League, "The Infrastructure of Hate: Epik Hosts Extremist Groups," February 22, 2021, https://www.adl.org/resources/blog/infrastructure-hate-epik-hosts-extremist-groups.
87. Andrew Blake, "BitChute, YouTube Alternative, Cries Foul Over Apparent Punt from PayPal," *Associated Press*, March 7, 2019, https://apnews.com/article/8b442b41f94b39668369d6271719a6e5.
88. Gregory Davis, "BitChute Platforming Hate and Terror in the UK," *Hope Not Hate* (2020).
89. Anti-Defamation League, "BitChute: Hotbed of Hate," 31 August, 2020, https://www.adl.org/resources/blog/bitchute-hotbed-hate.
90. Community Security Trust, *Hate Fuel: The Hidden Online World Fuelling Far Right Terror* (2020).
91. Trujillo, M. *et al.* (2020) "What is Bitchute? Characterizing the 'free speech' Alternative to YouTube," *Proceedings of the 31st ACM Conference on Hypertext and Social Media, HT 2020*, pp. 139–140. doi: 10.1145/3372923.3404833.

92. Proscribed as a terrorist organisation in the UK and Canada.
93. Proscribed as a terrorist organisation in the UK.
94. Gregory Davis, "BitChute Platforming Hate and Terror in the UK."
95. Tech Against Terrorism, "Inclusion Policy," https://terrorismanalytics.org/policies/inclusion-policy.
96. Tech Against Terrorism, "Announcing Tech Against Terrorism's Newest Member," 2022, https://www.techagainstterrorism.org/2022/10/06/announcing-tech-against-terrorisms-newest-member-2/; Ofcom, Ofcom's First Year of Video-Sharing Platform Regulation: What We Found, October 20, 2022.
97. Ofcom, "First year," 77.
98. BitChute, Transparency Report June 2022. June 2022, p. 2, https://static.helpjuice.com/helpjuice_production/uploads/upload/image/6342/direct/1654094104600-BitChute%20-%20Transparency%20Report%20-%20June%202022%20v2.pdf.
99. Ofcom, "First year."
100. On 14 May, 2022, a perpetrator attacked a supermarket targeting a black populating, killing ten and injuring 3. Prior to the attack he released a manifesto and he also released a livestream that was cut prematurely by the platform on which it was livestreamed, Twitch.
101. Ofcom, "First year," p. 77.
102. Tech Against Terrorism, "Tech Against Terrorism: Recent Work and Areas of Research," (2021).
103. Bettina Rottweiler and Paul Gill, "Conspiracy Beliefs and Violent Extremist Intentions: The Contingent Effects of Self-efficacy, Self-control and Law-related Morality," *Terrorism and Political Violence* (2020), doi: 10.1080/09546553.2020.1803288.
104. Scott Shane, "The Enduring Influence of Anwar al-Awlaki in the Age of the Islamic State," *CTC Sentinel* 9, no. 7 (2016): 15–20; T. K. Samuel, "At the Crossroads: Rethinking the Role of Education in Preventing and Countering Violent Extremism," in *Handbook of Terrorism Prevention and Preparedness*, ed. A. P. Schmid (The Hague: International Centre for Counter-Terrorism, 2020), 174–213, doi: 10.19156/2020.6.017; Scott Macdonald et al., "The European Far-right Online: An Exploratory Twitter Outlink Analysis of German & French Far-Right Ecosystems," *Resolve Network* (May 2022).
105. Mekacher, Falkenberg, and Baronchelli, "Systemic impact."
106. Jensen et al, "Social media"; Whittaker, "Behaviours."
107. Benson, "Internet."
108. Clifford and Powell, "Encrypted."
109. USA v. Nicholas Rovinski, Government's Sentencing Memorandum, Case 1:15-cr-10153-WGY, United States District Court for the District of Massachusetts, 2017.
110. Joe Whittaker, "Recommendation Algorithms and Extremist Content: A Review of Empirical Evidence," *Global Internet Forum to Counter-Terrorism* (2022), doi: 10.5210/fm.v25i3.10419.
111. BitChute, "Transparency Report."
112. Tarleton Gillespie, "Do Not Recommend? Reduction as a Form of Content Moderation," *Social Media and Society* (2022), doi: 10.1177/20563051221117552.
113. Kelley Cotter, "Playing the Visibility Game: How Digital Influencers and Algorithms Negotiate Influence on Instagram" *New Media & Society* 21, no. 4 (2018): 895–913.
114. X, Hateful Conduct, April 2023, https://help.x.com/en/rules-and-policies/hateful-conduct-policy.
115. Stuart Macdonald and Katy Vaugan, Moderating Borderline Content while Respecting Fundamental Values, *Policy & Internet* (2024).
116. Maxwell, "BitChute."
117. Davis, "Platforming Hate."
118. Alistair Reed, Haroro Ingram, and Joe Whittaker, "Countering Terrorist Narratives," *European Parliament* (2017), p. 30.
119. Tessa Lyons, "The Three-Part Recipe for Cleaning up Your News Feed," *Meta* (2018), https://about.fb.com/news/2018/05/inside-feed-reduce-remove-inform/.
120. YouTube. "The Four Rs of Responsibility, Part 1: Removing harmful content" YouTube Blog, 2019, https://blog.youtube/inside-youtube/the-four-rs-of-responsibility-remove/.

121. Anne-Sofie Hemmingsen and Karin I. Castro, "The Trouble With Counter-Narratives," *Danish Institute for International Studies* (2017); Sarah L. Carthy, Colm B. Doody, Katie Cox, Denis O'Hora, and Kiran M. Sarma, "Counter-narratives for the prevention of violent radicalization: A systematic review of targeted interventions," *Campbell Systematic Reviews* 16, no. 3 (2020), doi: 10.1002/cl2.1106; Michael Jones, "Through the Looking Glass: Assessing the Evidence Base for P/CVE Communications," *RUSI Occasional Paper* (July 2020), doi: 10.1093/jiplp/jpu004.
122. Kurt Braddock, "Vaccinating Against Hate: Using Attitudinal Inoculation to Confer Resistance to Persuasion by Extremist Propaganda," *Terrorism and Political Violence* 34, no. 2 (2022): 240–262, doi: 10.1080/09546553.2019.1693370.
123. Sarah L. Carthy and Kiran M. Sarma, "Countering Terrorist Narratives: Assessing the Efficacy and Mechanisms of Change in Counter-narrative Strategies," *Terrorism and Political Violence*, doi: 10.1080/09546553.2021.1962308.
124. N. F. Johnson, R. Leahy, N. Johnson Restrepo, N. Velasquez, M. Zheng, P. Manrique, P. Devkota, & S. Wuchty, "Hidden resilience and adaptive dynamics of the global online hate ecology," *Nature* 573 (2019): 261–265.
125. Jocelyn Bélanger et al. Do Counter-Narratives Reduce Support for ISIS? Yes, but Not for Their Target Audience, *Frontiers in Psychology* 11, 2020.
126. Braddock.
127. We are grateful to one of our anonymous reviewers for introducing us to this concept.
128. Europol, Europol and Telegram take on terrorist propaganda online, 2019, https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online#:~:text=On%2021%2D22%20November%202019,dissemination%20of%20online%20terrorist%20content.
129. Human Rights Watch, Illusion of Justice: Human Rights Abuses in US Terrorism Prosecutions (2014).

Disclosure Statement

No potential conflict of interest was reported by the author(s).

ORCID

Joe Whittaker http://orcid.org/0000-0001-7342-6369