SITES: NEW SERIES · VOL 18 NO 1 · 2021

DOI: http://dx.doi.org/10.11157/sites-id496

– ARTICLE –

SALVAGING FLAWED DISCOURSES SURROUNDING NZ'S 'COUNTER-TERRORISM LEGISLATION BILL'

Kevin Veale[1]

ABSTRACT

Public-facing announcements from Labour minister Kris Faafoi and Prime Minister Jacinda Ardern around the 'Counter-Terrorism Legislation Bill' that was introduced to Parliament on the 13th of April 2021 has included a number of flawed discourses that risk making the legislation less effective. The current focus on 'lone actors' speaks to a misunderstanding of online community dynamics within the hate-groups that motivate terror attacks. Additionally, there is little attention either in the foundational document for the 'Christchurch Call to Action Summit' or the discussions surrounding the 'Counter-Terrorism Legislation Bill' of the ways that online economies drive the expansion of extremist groups and raise the odds of terrorist actions. This article will explore the background to these issues, what makes the current discursive framing from the government around the legislation problematic, and what initiatives could be concretely taken to mitigate these issues.

Keywords: Christchurch call, social media, surveillance capitalism, extremism, online communities

INTRODUCTION

The 'Counter-Terrorism Legislation Bill' (Faafoi 2021) was introduced to the Parliament of Aotearoa-New Zealand on the 13th of April 2021, and accompanied by announcements to local news services. The Bill's goal is to enhance Aotearoa-New Zealand's ability to prevent terrorist action through changes such as creating new offences tied to terrorist activity and planning, criminalising wider forms of material support for terrorist activities, and clarifying the definition of a terrorist act. Unfortunately, both the Bill and the public-facing discourse from the Labour government about it demonstrate ignorance over ongoing conversations in media and cultural studies regarding how commu-

nities function in digital spaces. In particular, there is a lack of awareness of how media studies has explored both the ways 'networked publics' shape the communities which form within them (boyd 2011, 39, 55), and how dynamics internal to hate-groups online motivate terrorist actions (Veale 2020a, 59; Dena 2008, 42–43; 2009, 239–58). This article will explore how the Bill has been framed in problematic ways that either conceal or ignore the realities behind how online hate moves into the everyday world.

FRAMING THE BILL

In introducing the Bill, Labour Justice Minister Kris Faafoi made reference to the March 15th 2019 terror attacks on the Christchurch Al-Noor Mosque and Linwood Avenue Islamic Centre, and suggested that the updated law was part of a response designed to make the country safer from this kind of attack:

> 'This is the government's first step to implementing recommendation 18 of the Royal Commission into the Terrorist Attack on Christchurch masjidain on 15 March 2019, which called for a review of all legislation related to New Zealand's counter-terrorism effort to ensure it is fit-for-purpose and enables public sector agencies to operate effectively,' Justice Minister Kris Faafoi said. 'The attack also mirrored how the nature of terrorism has been changing internationally, involving lone actors rather than organised terrorist groups. We need to ensure our laws can respond to that,' he said. (RNZ 2021a, paragraph 6)

Trying to distinguish between 'organised terrorist groups' such as state actors and threats like the terrorist attacker in Christchurch is not unreasonable, but this solution obscures more than it reveals because 'lone actors' (often referred to as 'lone wolves') are not a real problem. Juliette Kayyem, faculty chair of the homeland security program of Harvard University's Kennedy School of Government, argues that 'lone wolves' do not exist, and that focusing on them is a fundamental mistake:

> White-supremacist terrorism has what amounts to dating apps online, putting like-minded individuals together both through mainstream social media platforms and more remote venues, such as 8chan, that exist to foster rage. It is online, much like Islamic terrorism, that white supremacy finds its friends, colleagues who both validate and amplify the rage. When one of them puts the violent rhetoric into action in the real world, the killer is often called a 'lone wolf,' but they are not alone at all. They gain strength and solace from like-minded

> individuals. No one would have said an individual Klansman attending a Klan meeting in the woods was a lone wolf; 8chan and other venues are similar meeting spaces in the digital wild. (Kayyem 2019, paragraph 6)

The language of 'lone actors' and 'lone wolves' does not appear in the proposed legislation itself (Faafoi 2021).[2] However, the discursive framework is worth highlighting because it speaks to assumptions around the nature and context of the kinds of threat embodied by the Christchurch terrorist that this law change seeks to address. Events like the 2019 Christchurch terror attack exist in a context where the individual terrorist is simply the most active and visible tip of a much larger iceberg formed from online extremist communities that inspire them to attack, and then amplify their actions. This amplification is driven by algorithms and infrastructures online tied to the business models and fundamental economics of online spaces.

Prime Minister Jacinda Ardern herself opened the door to examining this dimension of online extremism in her public-facing comments surrounding the bill. However, those comments also featured counter-productive discourses around the subjects of online infrastructure, algorithms and accountability tied to the Christchurch Call to Action Summit (also known as the Christchurch Call) of 2019. The purpose of the Christchurch Call was to begin a global discussion regarding ways to combat the proliferation of violent extremist content online (Ardern 2019), and brought together a coalition of nations[3] and large corporations.[4] The pledge document that signatories nominally agreed to is non-binding, three-pages long, and contains provisions under three broad umbrellas, all of which were published publicly online ('Christchurch Call' 2019). One of the agreed provisions of the Christchurch Call focused on algorithmic dimensions to extremist content, where online service providers signing on to the Call agreed to,

> Review the operation of algorithms and other processes that may drive users towards and/or amplify terrorist and violent extremist content to better understand possible intervention points and to implement changes where this occurs. ('Christchurch Call' 2019, 2)

One of the public-facing comments from Jacinda Ardern about the 'Counter Terrorism Legislation Bill' referred back to this provision, but also minimised the fact that only 10 percent of members of the Christchurch Call considered it an 'important first step' by saying 'I'd probably place a higher priority on it than that' (RNZ 2021b). Ninety percent of the members of the Christchurch

Call not considering a foundational element of the agreement to be a high priority is a problem worth highlighting and working towards changing, rather than simply stating a personal disagreement. Given that the Christchurch Call includes a total of eight technology companies, it is also not clear what '10 percent' means in this context. Effectively, Ardern's framing minimises a central element of an international agreement and downplays its importance, which risks undermining the good it has done to get the topic on the table of an international stage.

Ardern also highlights the importance of research into dynamics that are presented as a new problem that is currently not well understood:

> Also research into this space, understanding what happens when people first access content that we might not consider as harmful but what leads them down into what we would consider these more harmful items online that might trigger violent extremist activity down the track. (RNZ 2021b, paragraph 16)

The patterns by which people are exposed to the radicalising content that Ardern highlights are of vital importance, particularly when combined with an understanding of algorithmic developments. However, the problem with the statement is that it implies the research does not currently exist, when that is not the case. Bodies of work already exist that explore the ways that online communities produce pathways to extremism, and this work often connects to how algorithms and online platforms are used to amplify the process. Presenting the research as 'not yet done' suggests that the government of Aotearoa is unaware of bodies of research relevant to the problems it is seeking to solve with legislation. The alternative is that it is building a public-facing pretence to excuse not acting upon that research, potentially because of the risks to political capital involved in challenging powerful international interests whose business models are inextricably involved in these processes, and who the public largely take for granted.

Next, this article will explore the ways that understanding online extremism and its relationship to terrorist acts is impossible without understanding the relationship between online business models and their impact on community dynamics. It will then suggest a series of interventions that could be concretely taken to mitigate these problems at a national and international level.

THE ALGORITHMIC, ECONOMIC AND COMMUNITY DYNAMICS OF ONLINE EXTREMISM

One of the disquieting dimensions to understanding online hate-groups are the extent to which their community dynamics are very similar to those in other online spaces, but with extremely different community goals.[5] Christy Dena introduced a useful model for understanding these dynamics while writing about Alternate Reality Games (ARGs): she uses the term 'tiers' to describe how ARG communities stratify around different levels of activity and engagement (Dena 2008, 42–43; 2009, 239–58). In broad strokes, the members of the primary tier are the most active members of an ARG, and they bring in new material; the secondary tier fits that material together; and the tertiary tier forms an audience that engages with the output of the other tiers. People move between tiers as their levels/types of engagement fluctuate.

Hate-groups and harassment communities also exhibit these dynamics, except that the context of tiering adapts to a situation where the goal is committing concrete harm to someone's ability to live their life, or a community's ability to exist undisturbed. The challenge of the 'game' comes from overcoming any resistance provided by the people being terrorised as they try to protect themselves and those close to them. The tertiary tier functions almost exactly as it would for a normal ARG, and is made up of people who are following the activities of the hate-group by supporting them without participating themselves. The secondary tier of extremist communities seek opportunities to capitalise upon and promote particular achievements made by those in the primary tier. Those achievements encapsulate a diverse set of activities because of how wildly diverse the activities of the primary tier itself is – something also true of normal ARGs.

The individuals within the primary tier do incredible amounts of labour to forward the cause of the hate-group, regardless of what form that labour happens to take, and they are most likely to be the people who can be personally identified for their contributions: part of the motivation for the labour is to achieve social capital (or infamy) within the extremist community (Veale 2013; Butt and Apperley 2016). As a result, people in harassment communities are effectively competing with each other for who can do the most harm and get the most respect from their fellow extremists – a dynamic which Kathy Sierra (2014) says fuels the worst kinds of escalation. Joel Finkelstein, director of the Network Contagion Research Institute, has identified the same competitive dynamics within hate-groups as Sierra:

> 'They begin to train one another as to how to become more expertly anti-social. Now you have a race to the bottom. Who can say the edgiest, craziest Thing?' he said. 'Now, someone goes out and actually commits something. That then causes the entire community to rally, to celebrate. They can't stop thinking about these horrible things to do. Eventually, that feeds an impulse to actually do the thing.' (Myrow 2019, paragraph 12)

The people who produced and sold videogames glorifying the terrorist attacks in Christchurch (which were then banned as objectionable material by the NZ Office of Film & Literature Classification) would qualify working within the primary tier (O'Connor 2019; Tait 2019). The people popularising and distributing it would be in the secondary tier, and the people playing it are in the tertiary tier – and potentially recruitable into the more active tiers.

Within the primary tier of hate-groups are a subset of individuals willing to both threaten credible physical violence and then to carry it out (Robertson 2014; Sarkeesian 2014). A chilling example of this dynamic is Elliot Rodger, who murdered six people in 2014 after posting a sexist 'incel' manifesto online on 4chan. Rodger has been praised as a 'saint' by some online extremist communities – with further killers directly claiming him as inspiration for their attacks on women (BBC 2018a; 2018b; Cecco 2020; Hern 2018). Incels have since been categorised as a terrorist group by the Canadian government and Royal Canadian Mounted Police (Bell 2020). Kiwi Farms is a community that has driven more than one person to suicide (Fogel 2018; 'lightninggrrl' 2016; Pless 2016). Both 8chan and Kiwi Farms have been linked to multiple mass killings that were celebrated in their communities (Hankes 2018; Neiwert 2015). Additionally, Kiwi Farms hosted videos recorded from the livestream of the Christchurch terrorist attacks, and directly defied attempts to get them removed (NZ Herald 2019; Newshub 2019; Macklin 2019).

It is in this light that we have to understand the Christchurch attacker referring to the livestream of his massacre as an 'effort post' on 8Chan – in contrast to a low effort 'shitpost' (Hoverd, Salter, and Veale 2020 2020b, 4, 10; Macklin 2019; Rowe 2019). His livestream was an exemplar first-tier attempt to court the social capital and approval of existing white supremacist hate-groups online. As such, it is a claim to infamy that most within the extremist community can only aspire to – although the monstrous fact is that many were inspired to achieve similar atrocities for themselves:

> The attacker from Poway wrote 'he showed me it could be done'[6]

> and the Bærum attacker glorified {*name removed*} for the propaganda of the deed by posting 'it's my time, I was elected by Saint {*name removed*}.'[7] Users of the extreme right 8chan board had also devoted considerable energy to spread the Christchurch manifesto in order to encourage more shootings. […] Real life action is further motivated through the gamification of acts. The online community counts scores and compares those of different attacks. 'Scores' refers to the number of individuals killed. The Poway shooter was ridiculed after his attack for the little score he achieved.[8] This international competition is likely to motivate individuals to make their attacks deadlier and deadlier. (Wegener 2020, paragraph 5)

To this list, we can also add an attempted terror attack seeking to mimic the Christchurch atrocity by attacking mosques in Singapore (Andelaine 2021). Additionally, it is worth highlighting that the use of 'Saint' to refer to the Christchurch terrorist is evidence of overlap between the extremist communities who celebrate the 'incel' mass-murder committed by Elliot Rodger and white-supremacist hate-groups, an overlap we can also see in the distribution of the terrorist's livestream on Kiwi Farms.

As a result of these dynamics, we can say that the Christchurch terrorist's attempt to win social capital within broader extremist communities was – unfortunately – wildly successful. Extremist groups have continued circulating the video as an active recruitment exercise, and used it for fundraising. Methods for corresponding with the terrorist within the justice system of Aotearoa were shared online, leading to enough mail that he was then banned from using the service (Bateman 2019). There are fan-sites dedicated to him, and he has likely been informed of them through the correspondence that arrived before the ban. And hate-groups have ensured that the footage of the livestream continue to circulate in ways designed to terrorise Muslim communities online (Ali 2021).

What is missing from many discussions surrounding how and why these kinds of attacks are so successful for extremist communities are the ways that online infrastructures and economies directly contribute to their success, and sometimes actually profit from it. James Bridle has highlighted how YouTube's algorithms drive the creation and recommendation of disturbing content in pursuit of profit (Bridle 2017; 2018; Hern 2017). Rebecca Lewis has illustrated a network of neo-Nazis, white supremacists, anti-feminists and other extremist groups online using YouTube as a platform for their content (D'Anastasio 2018; Lewis 2018, 36–42).

YouTube's algorithms mean members of the audience that enter the network from any direction will be introduced to more and more extreme content through the recommendation engine. As a result, YouTube's algorithms both provides a means of interconnection between those creating content in the network, and encourages the creation of more extreme content because it will be rewarded both financially and with more views (Veale 2020a, 90).

Zeynep Tufekci highlights that YouTube encourages and rewards the production and distribution of radicalising extremist material, and that YouTube's recommendation algorithms ensure audiences encounter more extreme content over time to keep them engaged so that the platform can profit from their engagement (Tufekci 2018).

Facebook's algorithms follow the same dynamics in ways that were known to its internal leadership for years, while executives scuttled attempts to fix the problem and kept the information from the public: this includes the fact that 64 percent of the people joining white supremacist extremist groups did so because Facebook's own recommendation algorithms sent them there (Horwitz and Seetharaman 2020). Platforms have even gone so far as to change their own rules in order to continue supporting profitable extremist content (Thompson 2019, 84). Critics have argued that one of the reasons toxic content is permitted on social media platforms is because the people posting it and engaging with it are 'the really valuable ones' to the site's bottom line (Schipp Page, paragraph 25).

Alongside cases where social media platforms are actively implicated in driving the creation of extremist content, we can explore cases where they refuse to use available tools to tackle problems on their networks. These include examples such as:

> Twitter refusing to apply tools it has used to remove GIFs, images and footage of the Olympic Games after copyright claims to the task of preventing harassment via spamming targets with images of the Holocaust or GIFs designed to cause seizures in anyone with epilepsy. A report from the UK government highlighted that Google has very similar issues with YouTube (Eichenwald 2016; Home Affairs Committee 2017, 10, 21; Silverman 2016; Warzel 2016b)

The rules and guidelines by which Twitter operates, and even the terms and services, are also frequently not applied, even in clear-cut cases (Sarkeesian 2015; West 2014; Warzel 2016a).

Twitter is legally required to block neo-Nazi accounts within France and Germany and created a tool to do so in 2012, but refuses to apply the same tool to its networked public globally (Feiner 2019; Lomas 2017; Martin 2017). We are left to speculate as to why a tool that would be easier in some ways to apply globally has instead been applied to the lowest number of countries required by law (Veale 2020a, 116–17).

Twitter refuses to apply online tools used successfully to remove content from Da'esh supporters across its network to white supremacist extremism since that would also filter Republicans in the United States (Cox and Koebler 2019).

In 2020, a Twitter account resharing content from Donald Trump with no alterations was suspended after operating for 68 hours on the grounds it was 'glorifying violence', while Trump's account itself was defended as 'public interest' (Yeo 2020).

The ways that social media platforms amplify extremist material produced by hate-groups are designed to show it to more people, and expand those extremist communities, in order to profit from them. The same capitalist motivation extends to platforms neglecting to apply available tools to mitigate problems on their networks: they are rewarded financially for not making the effort.

Because of the tiering effects associated with online communities, including hate-groups, the broader the base of the community and the more people recruited into it, the larger the pool of extremists who might decide or be persuaded to climb into the more active tiers. In effect, the larger the extremist community, the greater the odds that individuals within that community will choose to take murderous terrorist action against vulnerable, marginalised communities. The surveillance capitalism business models of social media platforms directly drive that process, effectively making money from dynamics that produce terrorists.

While distinguishing terrorists, such as the Christchurch attacker, from more structured and organised terror groups is important, it is vital that the distinction does not misunderstand the problem. We are not dealing with isolated, atomised individuals who are stumbling onto *The Anarchist's Cookbook* online, and yet that appears to be what Prime Minister Jacinda Ardern implied in one of her public-facing comments about the 'Counter-Terrorism Legislation Bill' under development:

> Jacinda Ardern told *Morning Report* it's unrealistic to expect the

> internet to be free from all content that is of concern.
>
> 'The idea that the vast space that is the internet, that we would be able to rid ourselves completely of some of the content that would be of grave concern to us, I don't think we've set ourselves necessarily that unrealistic goal at that stage,' Ardern said. (RNZ 2021b, paragraph 5)

It is neither necessary nor possible to remove all concerning extremist content from the internet, but that is not what is being suggested. There is currently an extremely well-funded international network profiting from ensuring that extremist content gets into the hands of anyone who *might* be interested in it, just in case they can be persuaded to keep engaging with it. As a result, there is a connection between the business activities of global internet platforms and terrorist violence. This is a dimension of the problem that needs to be factored into responses at a governmental level.

Far from atomised individuals encountering extremist content or *The Anarchist's Cookbook*, there is a multi-billion dollar infrastructure designed to connect those people together into existing or new hate-groups, and reward them for making and distributing hateful content, alongside attempted and successful terrorist attacks. This is not a hypothetical problem: as Jeff Horwitz and Deepa Seetharaman (2020) have highlighted from leaks internal to Facebook, more than 65 percent of the people in active white-supremacist groups on Facebook are there because Facebook's own algorithms suggested them.

Fortunately, we are not powerless in the face of this infrastructure, and there are steps that individual countries and the international community can take – once the problem is understood and acknowledged at high levels.

INTERVENTIONS

There are two primary areas in need of intervention: firstly, that the infrastructure of major social media companies drives extremism in pursuit of profit, and secondly, the community dynamics of extremist groups that make terrorist actions more likely as a result.[9] Legislation is not going to be an appropriate tool to address all of the elements making up these problems, so there is work that can be done in a number of areas. It is quite possible that potential solutions prompted by flaws within public-facing discourse will not usefully map onto conversations happening within high-level government agencies: they may not be novel, or have already been considered and discounted. Alternatively, the problem may be one of funding, resourcing

and/or staffing rather than of comprehension. Hopefully, these contributions are useful for the ongoing conversations unfolding as we collectively try to improve the troubling status quo.

Online Economies Driving Extremism

The most substantial intervention possible in this area lies in the space of regulation, including the possibility of considering banning some platforms outright. The Security Intelligence Services (NZSIS) and other branches of Aotearoa's government will undoubtedly have had many wide-ranging, well-resourced conversations about the value of participating in the international Five Eyes surveillance agreement, and whether the benefits outweigh the costs involved (NZSIS n.d.). Platforms like Facebook have such a high level of penetration into society and communities across the country that they represent at least as much agency as individual states might represent within our surveillance spaces. The question that needs to be asked at high levels is whether the costs of allowing specific social media platforms to function within Aotearoa's jurisdiction outweighs the costs. Applying a similar level of high-level scrutiny and cost/benefit analysis as has been applied to the Five Eyes network would help answer that question. There would likely be a *substantial* social and technical cost involved in banning them from operating within Aotearoa's territory, leaving aside the costs in political capital, but it is an area worth exploring to, at the very least, find the lines in the sand that we would find intolerable for a social media platform to cross. It is not currently illegal, globally or locally, for social media companies and online spaces to profit from the harm caused by extremist communities online, while amplifying the possibility of future attacks. Is that something we accept? If this is not a line in the sand, what would be?

A more moderate approach would favour regulation, and there are a number of different actions that could be taken, depending on decisions made at this level. Peter Thompson (2019, 92) argues persuasively in 'Beware of geeks bearing gifts: Assessing the regulatory response to the Christchurch Call,' that global companies are extremely wary of being required to respond to different regulatory frameworks in different countries because of the costs to them involved.[10] Regulation along these lines would not innately pour water on the economies that drive extremist groups, but it would lay the groundwork for developing a stronger bargaining position against the global social media giants. Actively advocating for national level regulations encourages social media companies and online spaces to cooperate more broadly: the main mechanism available to companies seeking to avoid such a problem is more enthusiastic involvement with international agreements such as the Christchurch Call in an attempt to

seem to be taking responsibility. Other more targeted shifts in legislation could also have concrete effects. For example, legislation requiring Twitter to add Aotearoa to the same list as France and Germany that blocks white-supremacist accounts and content (Veale 2020a, 116–17; Feiner 2019; Lomas 2017; Martin 2017) would be one efficient step for that platform.

Another possible area of regulation that companies would want to avoid is taxation. Pragmatically, it is difficult to imagine having the political will to regulate such major companies without the political will to tax them, and, so far, the governments of Aotearoa have been reluctant to make many waves in this area. However, it is something beginning to unfold in various countries. Britain and France have levied taxes on the domestic turnover of global platforms, an action which seeks to 'reclaim online commercial turnover as domestic economic activity' (Thompson 2019, 86–87), and the G20 group have recently announced plans to establish global tax rules on major multinationals (RNZ 2021c).[11] Currently, giants such as Facebook and Google pay functionally zero tax in Aotearoa despite both profiting from our citizens in ways that raise the possibility of local terrorism. Applying taxes and/or levies would help correct what are fundamentally extractive business models that treat the activity of a given nation's citizens as valuable, but return none of that value to their nation's economy. In addition, it represents exactly the kind of piecemeal regulatory response that major technology companies and social media platforms would prefer to avoid through engaging in more unified responses like the Christchurch Call, at the same time as being valuable to the individual countries setting the levy.

Thompson's work provides a roadmap for wider regulatory responses than taxation that different territories can follow as well. These include responding to the concentration of content-discovery and e-commerce by '[r]edesignating digital intermediaries as public utilities with civic obligations beyond private shareholders,' and independent regulator access to algorithms (Thompson 2019, 97–98). Effectively, this is an area where the citizens of the world have been presented as powerless for decades, and instead have some options for local political activism. It is possible to build a sufficient diversity of sticks to wield against big players in social media and technology that the carrot of greater simplicity in cooperating with multilateral regulation becomes more attractive as a result.

However, in order for these approaches to work, those multilateral agreements between corporations and nations must be taken seriously. For example, the Christchurch Call presents a very useful initial foundation for such discussions

(Hoverd, Salter, and Veale 2020; Thompson 2019, 90; Veale 2020a, 149–50), but it is in danger of falling victim to the defensive politics of positivity. Current discussions of the Call suggest that 90 percent of the groups involved with the Call can back away from taking the algorithmic dimensions of extremism seriously when that is a core provision of the agreement without substantial challenge (RNZ 2021b). Perhaps this move is being challenged at high levels behind the scenes, and the public-facing discourse on the subject is a diplomatic framework. The problem is that we do not know. The core issue is that such moves *need* to be challenged at high-levels, including through continued engagement with the Christchurch Call and strategic regulation, as has been discussed, rather than minimised and presented as not being a problem. The alternative risks turning the Christchurch Call and agreements like it into a clean bandage of apparent progress wrapped around the untreated, gangrenous wound of the status quo.

The goal of regulation in this space is to work against the online business models and algorithmic infrastructures that encourage and amplify extremism. Even taking all of these steps would not solve the problem of extremism, but anything that limits the growth of hate-groups will be a net, concrete good. The fewer people who make it into such groups, the fewer who may be motivated to take terrorist action.

Community Dynamics of Extremist Groups

It is vitally important that state security apparatus and the wider machinery of government become aware of the online community dynamics of hate-groups, and particularly the spaces they occupy and move through online. That includes acknowledgement of the fact that lone-wolves do not exist, and the patterns of behaviour within extremist groups that encourage people to compete to become a worse monster. It would also be useful to begin developing a legislative framework to account for what happens in both online-harassment and hate-groups, where each individual person in the community contributes a seemingly small amount, but where each snowflake adds up to an avalanche. Traditionally, this is an area in which each person is often considered to be negligibly responsible for the outcome produced by the work of the community (Citron 2014, 24), but the fact the people involved are aware of the possible consequences of group action and participate anyway seems relevant in the modern context. If – as in the example of Kiwi Farms – a community's central organising purpose is to drive people to suicide, then at what point is it worth considering their actions pre-meditated assistance with homicide or manslaughter? If it was proven that the Christchurch terrorist attack could

not have been achieved without the material support, resources, advice and encouragement of a specific individual, there are legal frameworks for handling this. However, what if the same thing was true of the support provided by ten people, or twenty, or fifty, or one hundred? In all cases, the attack could not have proceeded without the contributions of the community, making the community complicit in the attack. The 'Counter-Terrorism Legislation Bill' offers opportunities to respond to this dimension of the problem, since it is already expanding and clarifying offences related to supplying 'material support' to a planned terrorist action (Faafoi 2021, 11). However, it is worth developing specific lines in the legislation around how to respond when a community meets the threshold for having committed an offence under the Bill, while individuals in that community would not individually qualify.

Surveillance of online spaces is also an important step, although one that sounds limited through a lack of appropriate funding and attention. Documents released by the NZSIS after Official Information Act requests indicate that counter-terrorism units began looking at right-wing forums at least as of May 2018 (Pennington 2021a), which is both a useful step and very late in the picture given the number of mass-shootings pre-announced in online spaces like 4chan, 8chan and others. Sites like Kiwi Farms and 8chan, while it was in operation, (and its replacements) exist to break the law. Something like 4chan manages to be problematic on a number of levels while hosting some legal content and communities alongside criminal ones. In comparison, Kiwi Farms and 8chan's replacements have no such defence: Kiwi Farms is a community dedicated to harassment – ideally murderous harassment – of people from vulnerable communities, such as transgender people and those the site believes to have mental illnesses. Kiwi Farms ran a counter of the number of people it had driven to suicide for a time to celebrate their victories. Different online hate-groups target different vulnerable communities, such as Muslims, people with disabilities, anyone non-white, and women online: Alice Marwick's (2021, 6) work highlights substantial intersectional dimensions to the people likely to be targeted by hate online. The formation of 8chan was prompted by child pornography being ejected from 4chan, and was further bolstered when 4chan ejected the Gamergate harassment community. These are spaces within the normal internet that are worth surveilling, alongside others within the dark web, and the activities of their denizens would give clues as to where they may be moving to or drifting between, all without necessarily identifying specific people *in* those communities until later in formal processes.

The work of Jasbir Puar raises a number of important issues in this area, particularly around the logics of pre-emptive surveillance and the impact that

surveillance has in shaping peoples' actions in the future. Puar highlights that pre-emptive surveillance 'seeks to control now, in order to avoid having to repress later' (Kovacs 2017; Puar and West 2014, paragraph 4). It is a process that does not just focus on what people are doing now, but on what they may do in the future, and provides incentives and disincentives for behaviour as a result. Puar and Kovacs highlight that it is a strongly gendered process with significant implications for one's identity, rights and privacy. However, the kinds of surveillance that would be most useful for dealing with online environments like Kiwi Farms and 8Chan's many imitators are less discriminatory than most forms of state surveillance: it is pre-emptive surveillance that focuses its attention on spaces rather than on individuals or groups. This dynamic is still something that must be handled with care, but, in comparison to other examples, the context of these sites reduces the possibility of ancillary harm: no one is actively involved in the Kiwi Farms community because of harmless fun, or would suffer harm if they felt forced to disengage from it. Surveilling these spaces seems similar to surveilling a KKK lodge: the demographics involved are a community collectively enacting hate. These environments also feature layers of anonymity that insulate the people involved from being easily or accidentally identified, and typically flout any approaches from law enforcement due to existing as criminal spaces.

Additionally, the fact is that, currently, members of marginalised and vulnerable communities are already doing ongoing, sustained surveillance of online spaces that they believe may threaten them and their community. Their surveillance puts them at risk from the extremist groups they are surveilling, and the process has a substantial personal cost through exposing them to deeply traumatic material. If the most vulnerable among us are capable of doing this – and consider doing so vital to their safety, even at significant mental and emotional cost – then the state can as well. Additionally, community-level surveillance of dangerous spaces is an area where Puar's concerns about pre-emptive surveillance and the construction of key identities is absolutely important to consider. Any surveillance of these spaces would need to be aware that there will be communities of 'lurkers' staying abreast of possible threats and potentially archiving material for the defence of themselves and their communities.[12]

White supremacist terrorists have been identified in Aotearoa by volunteer watch-dog groups and members of the public sooner than state actors (Hunt 2021) – potentially due at least in part to a lack of resourcing (Pennington 2021b) – and this dynamic both highlights the problem with current approaches and offers opportunities for the future. Since vulnerable communities are already aware of online spaces from which threats against them emerge, it

should be possible to provide better resourcing and support for these community watchdogs alongside a formal expectation that government agencies check-in with them. Building structures and connections by which individuals and organisations can more easily communicate and provide evidence of their concerns to representatives of the state in ways that will be heard and investigated seem like efficient ways forward. Establishing such structures and connections would also take steps to mitigate prior problems where attempts from marginalised communities to notify representatives of the state of their concerns were ignored, as identified in the Royal Commission of Inquiry (NZ Department of Internal Affairs n.d.). With that said, the ideal situation is that members of vulnerable communities do not feel they *have* to engage in this form of surveillance, given the risks to them and the complexities involved. However, persuading them that their activity is unnecessary would involve demonstrating that they can trust the authorities to be handling the problem for them, and, given the systemic failures and lack of support they have experienced, this will be a challenge (Dreaver 2021; NZ Department of Internal Affairs n.d.; Pennington 2021a; 2021b). Supporting them in the work they are already doing in this area while working to establish that trust seems like a good initial step.

It is possible that there might be opportunities to cross-pollinate expertise and approaches from how the government and police manage the pursuit of child pornographers and those who consume child-porn in Aotearoa and abroad: hunting for both extremism and child-porn involves unsafe and often dark spaces of the internet, and the communities of criminal extremists and conversations unfolding in them. There are also substantial subcultural overlaps between hate-groups and the people who consume child-pornography, as we can see in the genesis of 8chan focusing on both child-porn and extremism, alongside specific cases where would-be terrorists have been found hoarding both weapons and child-exploitation material (Savage 2020).

Sites like Kiwi Farms, 8chan and others – alongside actively dark spaces of the internet – are not ones that can be touched by legislation or regulation. Their purpose is to break the law, and they have already proven that they will not cooperate with law enforcement.

The primary response left is to ensure that elements of the state are aware of how these environments provide fertile contexts for communities to promote real-world violence, and to develop approaches for surveillance that focuses on specific spaces and the communities within them as they move and metastasise online.

Caveats about automated surveillance tools

Documents released under the Official Information Act reveal that the police of Aotearoa have previously purchased software designed to help them search the dark web (Pennington 2021b). It is likely that those involved with the police, and government agencies involved, are already aware of some of these elements, but hate-groups and extremist communities range from the incredibly direct and unsubtle all the way through to groups concealing their communications via very basic but rapidly changing subcultural codes in order to escape this kind of tool (Veale 2020a, 97; Ehrenkranz 2016). As a result, it is important to be aware that any such tool makes the task of surveilling a space simpler, but at the cost of giving the impression it is showing everything that may be of concern. As such, these tools are most effective when applied alongside agents spending time in these spaces and observing conversational and community trends, which can then be applied to informing areas of possible observation and concern in more automated searching.

As always, it is vital to understand the role that software platforms play in shaping both online communities and our collective ability to monitor them.

CONCLUSION

The 'Counter-Terrorism Legislation Bill' introduced to the government of Aotearoa on the 13th of April 2021 seeks to improve safety through changes such as creating new offences tied to terrorist activity and planning, criminalising wider forms of material support for terrorist activities, and clarifying the definition of a terrorist act. However, public-facing discourse from members of the Government on the subject of the bill featured flawed elements that risk making the legislation less effective. In particular, the discourse focuses attention on problems that do not exist – 'lone wolves' – while missing opportunities to engage with those that do, such as online communities whose dynamics fuel terrorism and provide support, guidance and motivation for those who wish to enact it. These flawed discourses appear both in the Christchurch Call to Action Summit and discussions of its progress, alongside the new 'Counter-Terrorism Legislation Bill' and how it is discussed.

As such, it appears that the government of Aotearoa is uninformed about both the community dynamics of online hate-groups, and the ways online economies directly drive extremism by encouraging and rewarding the production of extremist material, and then by amplifying its spread. These economies then profit from its generation and amplification, and share some of the pro-

ceeds with the extremist communities producing it. At the same time, online platforms are financially rewarded for failing to use available tools to mitigate extremist content. As a result, the business models of social media platforms and online spaces are directly implicated in growing the size of hate-groups and extremist communities online, and, as the size of such groups grows, so too does the odds of one of their members committing violence against the members of marginalised groups. One of the costs of surveillance capitalism can be measured in lives lost to white-supremacist terrorism.

There are actions that could be taken to have positive impacts on our collective safety, nationally and internationally, but foundationally these interventions require a better understanding of how the above dynamics work. Successful interventions also require getting resources to the right places and listening to vulnerable groups from the community who are often well-informed about at least some of the spaces from which threats against them emerge.

This article proposes a suite of possibilities that combine into a two-part process: firstly, surveilling the spaces favoured by extremist communities and hate-groups online ensures that the relevant authorities are aware of their activities and dynamics, alongside developing a window into the most extreme core of broader extremist communities. Secondly, although it is not possible to regulate away the spaces favoured by seriously bad actors in the primary tier of extremist communities, it *is* possible to work against the underlying business models that radicalise someone from environments like Facebook or YouTube, for example, and inspire them to go looking for 8chan. Although the roots of extremist communities can never entirely be removed, anything that can be done to disrupt the movement of new arrivals into hate-groups will disrupt the community dynamics around tiering and internal competition. In turn, this will limit their capacity to fundraise, and limit the pool of people who might be inspired to commit terrorist acts.

NOTES

1 Kevin Veale is fascinated with storytelling and popular culture, and most of his work explores the ways in which a media form changes the experience of the stories they mediate. His research into Alternate Reality Games (ARGs) highlighted the similarities between ARGs and communities of online extremists behind harassment campaigns. This connection lead to authoring *Gaming the Dynamics of Online Harassment* which came out with Palgrave in 2020. The book argues that online communities focused on harassment and abuse function as ARGs where the collective goal is to ruin the lives of those they target.

2 It is worth noting that 'white supremacy' and related ideas also do not appear in the document, while, in comparison, there are multiple well-developed paragraphs defining ideas tied to Da'esh, the Al-Qaida splinter group commonly referred to in Western media as ISIL or ISIS.

3 The initial nation-states who signed the Christchurch Call were Aotearoa-New Zealand, Australia, Canada, the European Commission, France, Germany, Indonesia, India, Ireland, Italy, Japan, Jordan, The Netherlands, Norway, Senegal, Spain, Sweden, and the United Kingdom. By September 2019, this had expanded to a total of 47 countries. The United States cited support for the summit, but claimed to be constrained by the First Amendment – a claim already challenged by Danielle Keats Citron, who argues that preventing hate speech and online harm is thoroughly consistent with the First Amendment (Citron 2014, 190–225).

4 The corporate signatories were Amazon, Daily Motion (owned by Vivendi), Facebook, Google, Microsoft, Qwant (a French search engine), Twitter and YouTube (a Google Subsidiary)

5 These dynamics are discussed in more detail in a book on the community dynamics of hate-groups online and the ways they are shaped by and abuse online economies (Veale 2020a).

6 See Sparrow 2019.

7 See Ali 2021; Dearden 2019; Ighoubah, Solberg, and Lorvik 2019.

8 See Conway, Scrivens, and Macnair 2019.

9 Interventions at other levels are certainly important, such as improving digital literacy and engagement with harm prevention across society at multiple levels, including school curricula. However, these interventions do not directly connect with the work associated with the 'Counter-Terrorism Legislation Bill', and are not discussed in detail within this article.

10 Thompson's (2019) work offers a substantial exploration of different angles and risks involved with regulating social media spaces and online environments. He flags that there is a historical tendency for big social media companies to offer to contribute to discussions around regulation in ways that would serve their strategic interests, and so their suggestions in this space are worthy of significant scrutiny.

11 The strength of this proposal is the fact it is a singular proposal across many countries. The downside is the same thing, in that it would be easier for corporations to respond to than a piecemeal approach, and thus less of a motivation to bring them to bargaining tables. There is no reason not to push for both, in that countries can use the international agreement as a floor to build their own bespoke bargaining position from.

12 My understanding from speaking to people who undertake such community-level surveillance of dangerous spaces is that they find simply being in those environments traumatic enough in itself, and would not consider posting or being active in the community as remotely safe. However, outliers may exist, and their existence will be important to consider going forward.

REFERENCES

Ali, Kawsar. 2021. 'The Christchurch Massacre Continues to Haunt Muslims across the World–Online and Offline'. *The Guardian*, 16 March 2021. Accessed 23 April 2021 from http://www.theguardian.com/commentisfree/2021/mar/16/the-christchurch-massacre-continues-to-haunt-muslims-across-the-world-online-and-offline

Andelaine, Lana. 2021. 'Copycat Attack Planned on Anniversary of Christchurch Massacre Foiled in Singapore'. *Newshub*, 28 January 2021. Accessed 23 April 2021 from https://www.newshub.co.nz/home/world/2021/01/copycat-attack-planned-on-anniversary-of-christchurch-massacre-foiled-in-singapore.html

Ardern, Jacinda. 2019. 'Christchurch Call to Eliminate Terrorist and Violent Extremist Online Content Adopted'. *The Beehive*, 16 May 2019. Accessed 05 September 2020 from http://www.beehive.govt.nz/release/christchurch-call-eliminate-terrorist-and-violent-extremist-online-content-adopted

Bateman, Sophie. 2019. '4chan Users Furious Alleged Christchurch Shooter Brenton Tarrant No Longer Able to Receive Mail'. *Newshub*, 15 August 2019. Accessed 22 April 2021 from https://www.newshub.co.nz/home/new-zealand/2019/08/4chan-users-furious-alleged-christchurch-shooter-brenton-tarrant-no-longer-able-to-receive-mail.html

BBC. 2018a. 'Toronto Suspect Praised "incel" Killer'. BBC *News*, 25 April 2018. Accessed 12 December 2019 from https://www.bbc.com/news/world-us-canada-43883052

———. 2018b. 'How Rampage Killer Became Misogynist "Hero"'. BBC *News*, 26 April 2018. Accessed 12 December 2019 from https://www.bbc.com/news/world-us-canada-43892189

Bell, Stewart. 2020. 'RCMP Adding Incels to Terrorism Awareness Guide'. *Global News*, 8 June 2020. Accessed 06 September 2020 from https://globalnews.ca/news/7021882/rcmp-incel-terrorism-guide/

Boyd, Danah. 2011. 'Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications'. In *A Networked Self: Identity, Community and Culture on Social Network Sites*, edited by Zizi Papacharissi, 39–58. Abingdon: Routledge.

Bridle, James. 2017. 'Something Is Wrong on the Internet'. *James Bridle* (blog). 6 November 2017. https://medium.com/@jamesbridle/something-is-wrong-on-the-internet-c39c471271d2

———. 2018. *New Dark Age: Technology and the End of the Future*. London ; New York: Verso.

Butt, Mahli-Ann Rakkomkaew, and Thomas Apperley. 2016. 'Vivian James – The Politics of #Gamergate's Avatar'. In *From the 1st Joint International Conference of DiGRA and* FDG. Dundee: The School of Arts, Media and Computer Games, Abertay University.

Cecco, Leyland. 2020. 'Canada Police Say Machete Killing Was "incel" Terror Attack'. *The Guardian*, 19 May 2020. Accessed 21 May 2020 from https://www.theguardian.com/world/2020/may/19/toronto-attack-incel-terrorism-canada-police

'Christchurch Call'. 2019. The Christchurch Call. 15 May 2019. Accessed 06 December 2019 from https://www.christchurchcall.com/call.html

Citron, Danielle Keats. 2014. *Hate Crimes in Cyberspace*. Cambridge: Harvard University Press.

Conway, Maura, Ryan Scrivens, and Logan Macnair. 2019. 'Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends'. ICCT – *International Centre for Counter-Terrorism*, November. https://doi.org/10.19195/2019.3.12

Cox, Joseph, and Jason Koebler. 2019. 'Twitter Won't Treat White Supremacy Like ISIS Because It'd Have to Ban Some GOP Politicians Too'. *Vice* (blog), 25 April 2019. Accessed 15 May 2020 from https://www.vice.com/en_us/article/a3xgq5/why-wont-twitter-treat-white-supremacy-like-isis-because-it-would-mean-banning-some-republican-politicians-too

D'Anastasio, Cecilia. 2018. 'How YouTube Fueled The Anti-Social Justice Movement'. *Kotaku*, 20 September 2018. Accessed 21 September 2018 from https://kotaku.com/how-youtube-fueled-the-anti-social-justice-movement-1829207455

Dearden, Lizzie. 2019. 'Revered as a Saint by Online Extremists, How the Christchurch Shooter Inspired Copycat Terrorists around the World'. *The Independent*, 24 August 2019. Accessed 23 May 2021 from https://www.independent.co.uk/news/world/australasia/brenton-tarrant-christchurch-shooter-attack-el-paso-norway-poway-a9076926.html

Dena, Christy. 2008. 'Emerging Participatory Culture Practices: Player-Created Tiers in Alternate Reality Games'. *Convergence: The International Journal of Research into New Media Technologies* 14(1): 41–57. https://doi.org/10.1177/1354856507084418

———. 2009. 'Transmedia Practice: Theorising the Practice of Expressing a Fictional World across Distinct Media and Environments'. PhD, Sydney: University of Sydney. http://www.christydena.com/phd/

Dreaver, Charlie. 2021. 'Māori Party Question Police Response to White Supremacist Video'. RNZ, 2 June 2021. Accessed 05 June 2021 from https://www.rnz.co.nz/news/te-manu-korihi/443860/maori-party-question-police-response-to-white-supremacist-video

Ehrenkranz, Melanie. 2016. '4chan's New Racist Code: How Alt-Right Trolls Are Harassing Jews, Muslims and Black People'. MIC, 3 October 2016. Accessed 15 October 2016 from https://mic.com/articles/155739/4chan-new-racist-code-google-skype-skittle-alt-right-trolls-harass-jews-muslims-blacks#.fbZEctj4O

Eichenwald, Kurt. 2016. 'How Donald Trump Supporters Attack Journalists'. *Newsweek*, 7 October 2016. Accessed 08 October 2016 from http://www.newsweek.com/epileptogenic-pepe-video-507417

Faafoi, Kris. 2021. *Counter-Terrorism Legislation Bill 29-1(2021), Government Bill –*

New Zealand Legislation. Accessed 21 April 2021 from https://www.legislation.govt.nz/bill/government/2021/0029/latest/whole.html#LMS479298

Feiner, Lauren. 2019. 'Twitter Users Are Escaping Online Hate by Switching Profiles to Germany, Where Nazism Is Illegal'. CNBC, 3 August 2019. Accessed 30 May 2020 from https://www.cnbc.com/2019/08/02/twitter-users-switch-profiles-to-germany-to-escape-online-hate.html

Fogel, Stefanie. 2018. 'Video Game Developer Dies After Setting Herself on Fire'. *Variety* (blog), 26 June 2018. Accessed 13 September 2018 from https://variety.com/2018/gaming/news/chloe-sagal-death-1202858068/

Hankes, Keegan. 2018. 'Evidence of New Mexico School Shooter's Involvement in the Racist "Alt-Right" Is Overwhelming'. Southern Poverty Law Center, 8 February 2018. Accessed 12 December 2019 from https://www.splcenter.org/hatewatch/2018/02/08/evidence-new-mexico-school-shooter%E2%80%99s-involvement-racist-alt-right-overwhelming.

Hern, Alex. 2017. 'YouTube Accused of "violence" against Young Children over Kids' Content'. *The Guardian*, 7 November 2017. Accessed 29 September 2018 from https://www.theguardian.com/technology/2017/nov/07/youtube-accused-violence-against-young-children-kids-content-google-pre-school-abuse

———. 2018. 'Who Are the "incels" and How Do They Relate to Toronto van Attack?' *The Guardian*, 25 April 2018. Accessed 28 May 2020 from https://www.theguardian.com/technology/2018/apr/25/what-is-incel-movement-toronto-van-attack-suspect

Horwitz, Jeff, and Deepa Seetharaman. 2020. 'Facebook Executives Shut Down Efforts to Make the Site Less Divisive'. *Wall Street Journal*, 26 May 2020. Accessed 29 May 2020 from http://archive.is/GPO6b

Home Affairs Committee. 2017. 'Hate Crime: Abuse, Hate and Extremism Online'. Fourteenth Report of Session 2016–17. Accessed 25 May 2020 from https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/609.pdf

Hoverd, William James, Leon Salter, and Kevin Veale. 2020. 'The Christchurch Call: Insecurity, Democracy and Digital Media – Can It Really Counter Online Hate and Extremism?' *SN Social Sciences* 1(1): 2. https://doi.org/10.1007/s43545-020-00008-2.

Hunt, Elle. 2021. 'New Zealand Police Charge Man over Online Threat to Christchurch Mosques'. *The Guardian*, 4 March 2021. Accessed 27 April 2021 from http://www.theguardian.com/world/2021/mar/04/new-zealand-police-arrest-two-over-alleged-threat-to-christchurch-mosques

Ighoubah, Farid, Trine Solberg, and Nina Lorvik. 2019. 'Dette vet vi om drapssiktede Philip Manshaus'. *Nettavisen*, 11 August 2019. Accessed 23 April 2021 from https://www.nettavisen.no/12-95-3423826953

Kayyem, Juliette. 2019. 'There Are No Lone Wolves'. *Washington Post*, 4 August 2019. Accessed 28 May 2020 from https://www.washingtonpost.com/opinions/2019/08/04/there-are-no-lone-wolves/

Kovacs, Anja. 2017. 'Reading Surveillance through a Gendered Lens: Some Theory'. Gendering Surveillance, February 2017. Accessed 01 June 2021 from https://genderingsurveillance.internetdemocracy.in/theory/

Lewis, Rebecca. 2018. 'Alternative Influence: Broadcasting the Reactionary Right on Youtube'. *Data & Society*. Accessed 21 September 2018 from https://datasociety.net/output/alternative-influence/

'lightninggrrl'. 2016. 'I Am Being Stalked and Harassed by Kiwi Farms and SA'. *Wrong Planet*, 24 March 2016. Accessed 13 April 2016 from http://wrongplanet.net/forums/viewtopic.php?t=308671

Lomas, Natasha. 2017. 'Here's How to Kick Nazis off Your Twitter Right Now'. *TechCrunch* (blog), 14 October 2017. Accessed 13 October 2018 from http://social.techcrunch.com/2017/10/14/heres-how-to-kick-nazis-off-your-twitter-right-now/

Macklin, Graham. 2019. 'The Christchurch Attacks: Livestream Terror in the Viral Video Age'. *Combating Terrorism Center at West Point* (blog), 18 July 2019. Accessed 26 February 2020 from https://ctc.usma.edu/christchurch-attacks-livestream-terror-viral-video-age/

Martin, Allen. 2017. 'Twitter Can Automatically Hide Neo-Nazis and White Supremacists, but Chooses Not To'. *Alphr*, 19 October 2017. Accessed 02 February 2018 from http://alphr.com/go/1007424

Marwick, Alice E. 2021. 'Morally Motivated Networked Harassment as Normative Reinforcement'. *Social Media+Society* 7(2): 20563051211021376. https://doi.

org/10.1177/20563051211021378

Myrow, Rachel. 2019. 'How Hate-Filled Groups Incite Violence From the Extreme Corners of the Internet'. KQED, 7 August 2019. Accessed 22 April 2021 from https://www.kqed.org/news/11765841/how-hate-filled-online-groups-encourage-budding-psychopaths-to-kill-others

Neiwert, David. 2015. 'Illinois Woman With Neo-Nazi Leanings Charged in Canadian Mass Murder Plot'. Southern Poverty Law Center, 18 February 2015. Accessed 12 December 2019 from https://www.splcenter.org/hatewatch/2015/02/18/illinois-woman-neo-nazi-leanings-charged-canadian-mass-murder-plot

Newshub. 2019. 'Kiwi Farms Website Refuses to Help Police in Christchurch Terror Case'. *Newshub*, 18 March 2019. Accessed 23 April 2021 from https://www.newshub.co.nz/home/new-zealand/2019/03/kiwi-farms-website-refuses-to-help-police-in-christchurch-terror-case.html

NZ Department of Internal Affairs. n.d. 'Home'. Royal Commission of Inquiry into the Attack on Christchurch Mosques on 15 March 2019. Accessed 3 May 2021 from https://christchurchattack.royalcommission.nz/

NZ Herald. 2019. 'Christchurch Mosque Shootings: Website Kiwi Farms Refuses to Surrender Data Linked to Accused'. *NZ Herald*, 19 March 2019. Accessed 23 April 2021 from https://www.nzherald.co.nz/nz/christchurch-mosque-shootings-website-kiwi-farms-refuses-to-surrender-data-linked-to-accused/YYMW2OF5GE3C7EYAMJAPSDANKI/

NZSIS. n.d. 'Domestic and International Partnerships'. New Zealand Security Intelligence Service. Accessed 23 April 2021 from https://www.nzsis.govt.nz/our-work/our-methods/working-with-other-organisations/.

O'Connor, Alice. 2019. 'New Zealand Banned a Mass Shooting Game as a "Terrorist Publication"'. *Rock, Paper, Shotgun* (blog), 1 November 2019. Accessed 12 December 2019 from https://www.rockpapershotgun.com/2019/11/01/new-zealand-banned-a-mass-shooting-game-as-a-terrorist-publication/

Pennington, Phil. 2021a. 'NZSIS Counterterror Focus on White Supremacists Found New Targets Quickly'. RNZ, 26 April 2021. Accessed 27 April 2021 from https://www.rnz.co.nz/news/national/441232/nzsis-counterterror-focus-on-white-supremacists-found-new-targets-quickly

———. 2021b. 'Police Had No Dedicated Team to Scan Internet before Mosque Attacks'. RNZ, 27 April 2021. Accessed 27 April 2021 from https://www.rnz.co.nz/news/national/441270/police-had-no-dedicated-team-to-scan-internet-before-mosque-attacks

Pless, Margaret. 2016. 'Kiwi Farms, the Web's Biggest Stalker Community'. *New York Magazine*, 19 July 2016. Accessed 06 October 2016 from http://nymag.com/selectall/2016/07/kiwi-farms-the-webs-biggest-community-of-stalkers.html

Puar, Jasbir, and Lewis West. 2014. 'Regimes of Surveillance'. *Cosmologics Magazine*, 4 December 2014. Accessed 01 June 2021 from https://web.archive.org/web/20150204072732/http://cosmologicsmagazine.com/jasbir-puar-regimes-of-surveillance/

RNZ. 2021a. 'Counterterrorism Laws Expansion Bill Follows up Mosque Attacks Report'. RNZ, 13 April 2021. Accessed 21 April 2021 from https://www.rnz.co.nz/news/political/440373/counterterrorism-laws-expansion-bill-follows-up-mosque-attacks-report

———. 2021b. 'Ridding Internet of All Concerning Content Would Be "unrealistic Goal" for Christchurch Call–Ardern'. RNZ, 14 April 2021. Accessed 21 April 2021 from https://www.rnz.co.nz/news/political/440435/ridding-internet-of-all-concerning-content-would-be-unrealistic-goal-for-christchurch-call-ardern

———. 2021c. 'Rich Nations Back Deal to Tax Multinationals'. RNZ, 6 June 2021. Accessed 07 June 2021 from https://www.rnz.co.nz/news/world/444134/rich-nations-back-deal-to-tax-multinationals

Robertson, Adi. 2014. 'Trolls Drive Anita Sarkeesian out of Her House to Prove Misogyny Doesn't Exist'. *The Verge*, 27 August 2014. Accessed 12 December 2019 from https://www.theverge.com/2014/8/27/6075179/anita-sarkeesian-says-she-was-driven-out-of-house-by-threats

Rowe, Don. 2019. 'The Online Cesspits Where Hate Found a Home'. *The Spinoff* (blog), 19 March 2019. Accessed 12 December 2019 from https://thespinoff.co.nz/media/19-03-2019/the-online-cesspits-where-hate-found-a-home/

Sarkeesian, Anita. 2014. 'I Usually Don't Share the Really Scary Stuff. But It's Important for Folks to Know How Bad It Gets [TRIGGER WARNING]'. Tweet.

@femfreq (blog). 27 August 2014. Accessed 12 December 2019 from https://twitter.com/femfreq/status/504718160902492160/photo/1

———. 2015. 'One Week of Harassment on Twitter'. *Feminist Frequency*, 27 January 2015. Accessed 21 April 2016 from https://feministfrequency.com/2015/01/27/one-week-of-harassment-on-twitter/

Savage, Jared. 2020. '"Terrorist Attack": How Police Thwarted Heavily Armed Teen's Plan to Shoot Teachers, Classmates in South Island School'. *NZ Herald*, 13 November 2020. Accessed 27 April 2021 from https://www.nzherald.co.nz/nz/terrorist-attack-how-police-thwarted-heavily-armed-teens-plan-to-shoot-teachers-classmates-in-south-island-school/UIBDQEDPD5OCWPJLYN34DSI53U/

Schipp, Debbie. 2018. 'Toxic Content Their "Crack Cocaine": Facebook's Disturbing Moderator Secrets'. news.com.au., 7 August 2018. Accessed 05 November 2018 from https://www.news.com.au/entertainment/tv/current-affairs/toxic-content-their-crack-cocaine-facebooks-disturbing-moderator-secrets/news-story/e03358922d893e49286fe514b11fe504

Sierra, Kathy. 2014. 'Trouble at the Koolaid Point'. *Serious Pony*, 7 October 2014. Accessed 30 March 2016 from http://seriouspony.com/trouble-at-the-kool-aid-point

Silverman, Robert. 2016. 'Twitter Is Deleting Olympics Videos. Harassment? Nah'. *Vocativ*, 15 August 2016. Accessed 21 January 2018 from http://www.vocativ.com/350674/twitter-is-deleting-olympics-videos-harassment-nah/

Sparrow, Jeff. 2019. 'What Induces Men to Imitate the Christchurch Massacre?' *The Guardian*, 5 August 2019. Accessed 23 April 2021 from http://www.theguardian.com/commentisfree/2019/aug/05/what-induces-men-to-imitate-the-christchurch-massacre

Tait, Maggie. 2019. 'Two Terrorist Publications Banned'. NZ Office of Film & Literature *Classification*, 31 October 2019. Accessed 12 December 2019 from https://www.classificationoffice.govt.nz/news/latest-news/two-terrorist-publications-banned

Thompson, Peter A. 2019. 'Beware of Geeks Bearing Gifts: Assessing the Regulatory Response to the Christchurch Call'. *The Political Economy of Communication* 7(1). http://www.polecom.org/index.php/polecom/article/view/105/314

Tufekci, Zeynep. 2018. 'Opinion | YouTube, the Great Radicalizer'. *The New York Times*, 10 March 2018. Accessed 19 April 2020 from https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html

Veale, Kevin. 2013. 'Capital, Dialogue, and Community Engagement—'My Little Pony: Friendship Is Magic' Understood as an Alternate Reality Game'. *Transformative Works and Cultures* 14(September). https://doi.org/10.3983/twc.2013.0510.

———. 2020. *Gaming the Dynamics of Online Harassment*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-60410-3.

Warzel, Charlie. 2016a. '"It Only Adds To The Humiliation" — How Twitter Responds To Harassers'. *BuzzFeed*, 22 September 2016. Accessed 17 April 2020 from https://www.buzzfeednews.com/article/charliewarzel/after-reporting-abuse-many-twitter-users-hear-silence-or-wor

———. 2016b. '90% Of The People Who Took BuzzFeed News' Survey Say Twitter Didn't Do Anything When They Reported Abuse'. *BuzzFeed*, 23 September 2016. Accessed 02 February 2018 from https://www.buzzfeed.com/charliewarzel/90-of-the-people-who-took-buzzfeed-news-survey-say-twitter-d

Wegener, Friederike. 2020. 'The Globalisation of Right-Wing Copycat Attacks'. *Global Network on Extremism & Technology*, 16 March 2020. Accessed 22 April 2021 from https://gnet-research.org/2020/03/16/the-globalisation-of-right-wing-copycat-attacks/

West, Lindy. 2014. 'Twitter Doesn't Think These Rape and Death Threats Are Harassment'. *Daily Dot,* 23 December 2014. Accessed 06 April 2016 from http://www.dailydot.com/opinion/twitter-harassment-rape-death-threat-report/

Yeo, Amanda. 2020. 'One Twitter Account Is Reposting Everything Trump Tweets. It Was Suspended within 3 Days.' *Mashable*, 3 June 2020. Accessed 07 June 2020 from https://mashable.com/article/twitter-donald-trump-suspend-tweets-policy-violence/