On 15 March 2019, Facebook livestreamed a massacre. A lone gunman toting semi-automatic weapons killed 51 people and wounded 49 others.\(^1\) Two mosques in the small city of Christchurch were the physical location of the attack but this massacre was planned and executed for a much larger audience. As a prelude, the terrorist posted a ‘Great Replacement’ manifesto online and emailed a personal copy to the prime minister of New Zealand. Comprising 87 pages of racist memes and conspiracy theories, the manifesto was written for a global audience of violent extremists. The focus in this chapter is on the enabling relationship between social media and the rise of contemporary fascism, the so-called ‘alt-right’. Social media may not have caused the massacre but it has been central to: (1) shaping an alt-right imaginary in which the ‘White Races’ face extinction; (2) forging a global brotherhood espousing real-world, violent action; and (3) providing a global forum within which such atrocities may be planned, executed, distributed and consumed. My analysis is situated within the context of the mainstream political discourses of disinformation associated with populist politics, especially of US President Trump, and the monopoly position enjoyed by a small

\(^1\) Prime Minister Jacinda Ardern requested that the terrorist be nameless in all reports and commentaries on the Christchurch massacre. Her expressed motivation has been to thwart the terrorist’s goal of achieving personal fame. In respect of this request, in this chapter, the terrorist is not named in the text although references and quotations that use his name have not been altered (Walquist, 2019).
number of major social media companies. When, on 6 January 2021, Facebook finally banned President Trump from its platform, it had taken the invasion of Congress by a violent mob bent on insurrection to trigger that action.

The Christchurch massacre was a ‘made for social media’ event, designed to go viral on Facebook and spread rapidly across other platforms. To maximise audience size, the terrorist posted on 8chan that he would livestream the attack, and tweeted hints of the impending massacre. Then, with a GoPro camera strapped to his helmet, the terrorist framed his Facebook livestream to mimic a first-person shooter video game. Centred within the frame, fascist symbols and the names of mass shooters, Serbian war criminals and massacres were scrawled in white paint across his guns. The entire attack, including the drive-time between mosques, featured a soundtrack of martial music and fascist anthems. This livestreaming of mass murder may have been shocking but it was by no means original (Singer and Brooking, 2018). Nor is the idea of ‘terrorism as theatre’ new, with the phenomenon documented decades before Facebook was even founded (Jenkins, 1974). Rather, social media has amplified terrorist causes and is implicated at every level of its operations. Since 15 March, governments and international forums have focused on reducing the efficacy of social media as a tool for terrorism. Yet, the origins and implications of Christchurch extend far beyond Aotearoa New Zealand, all the way to Washington DC, and move us beyond social media to the fundamental principles and values of Western democracies.

The path to Christchurch

Since the Twin Towers attack of 9/11, Islamist extremism has been the primary focus of terrorism debates and measures in Western nations (Blee, 2016). During the same period, the West has also experienced the rapid rise of alt-right terror attacks by white nationalists. Indeed, the majority of terror attacks in the US itself have been perpetrated by alt-right extremists. Such attacks have been treated differently by Western governments and by the news media, which has tended to frame them as almost inexplicable acts committed by deranged individuals. For example, Britain’s Telegraph headlined the Christchurch massacre with the headline, ‘The “ordinary white man” turned mass murderer’ (Ward, 2019), while the Daily Mirror described the killer as an ‘angelic boy’, and both newspapers
2. THE MAKING OF A ‘MADE FOR SOCIAL MEDIA’ MASSACRE

carried a photo of the terrorist as a towhead child in the arms of his father (Ben Lazreg, 2019). In contrast, attacks by Islamist terrorists are less likely to be attributed to individual pathologies and more likely to be portrayed as the product of extremist ideologies (Blee, 2016). A recent study found that terror attacks by Islamist extremists attract significantly greater news media attention in the West than do those by other perpetrators (Kearns et al., 2019). This differential framing is consistent with the worldview that terror threats in the West are driven by external forces – an ‘othering’ of perpetrators – which aligns with an increased emphasis on border control. It also aligns with the rhetoric of US President Donald Trump, whose political statements and Twitter posts were marked by anti-Muslim sentiment, such as false claims that thousands of Muslims living in New Jersey had cheered on 9/11 as the Twin Towers came down (MPowerChange.Org, 2019).

President Trump backed his rhetoric with a series of measures to limit or ban Muslims from entering the US. His campaign manager and subsequent head strategist in the White House, Steve Bannon, was the former executive chairman of Breitbart News, a website known for its alt-right, anti-Muslim and anti-immigration content (Heft et al., 2019). In comparison to his consistent stance against Islamist terrorism, President Trump’s position on alt-right violence was, at best, ambivalent (Kaiser et al., 2019). Most notably, President Trump declared that there were ‘very fine people, on both sides’, following the murder of a women protesting against a white supremacist rally in Charlottesville, Virginia (Sparrow, 2018). The rally appears to have been organised in a chat group on the video-gamers’ site, Discord. It began on the University of Virginia campus where hundreds marched bearing tiki torches while chanting racist and fascist slogans such as ‘Blood and soil’, ‘White lives matter’ and ‘You will not replace us’ (Kelkar, 2017; Hanna et al., 2017). These same themes feature in the manifesto of the Christchurch terrorist and across the social media sites associated with contemporary fascism. Given the apparent mainstreaming of the alt-right under the Trump administration, the relative inaction of the major online service providers in the face of growing extremism becomes more understandable. For example, the two US social media giants, Facebook and Alphabet (owner of Google and YouTube), have been ongoing targets of criticism by US conservatives for their alleged left-wing bias (Singer and Brooking, 2018; Romm, 2019).
In an environment in which major companies are fearful of a legislative backlash that would hit profitability, the door was opened for alt-right extremism to proliferate across the internet.

The term ‘alt-right’ was popularised by a ‘webzine’ created in 2010 by Richard Spencer and is now loosely applied to individuals and groups espousing neo-Nazi, fascist, white nationalist, anti-Semitic, anti-feminist and anti-immigration views. While anti-globalisation is a core theme for the alt-right, the movement itself is globally connected through a network of websites, social media pages and chat spaces. Some of these spaces are on the dark web, which is an encrypted part of the internet and not accessible through search engines. However, much alt-right communication – like the organisation of Charlottesville – is undertaken in plain sight on, for example, Facebook, YouTube and Twitter (Chaudhry and Gruzd, 2019).

In their 2018 book, LikeWar: The Weaponization of Social Media, Singer and Brooking (2018, pp. 169–70) argue that:

As it has with so many other movements, social media has revolutionized white nationalist, white supremacist, and neo-Nazi groups, spiking their membership and allowing their views to move back into mainstream discourse. In the United States, the number of Twitter followers of such groups ballooned 600 per cent between 2012 and 2016, and the Southern Poverty Law Center now tracks some 1,600 far-right extremist groups.

Those who identify with alt-right ideology and causes appear to move between the public internet and dark net, reserving much but by no means all of their most extreme content and hate speech for the latter. This pattern is evident in the reported postings of those who have gone on to commit attacks, including the Christchurch terrorist and the attackers he inspired, in El Paso, Texas, and Poway, California.

The alt-right movement might be characterised as what Bennett and Segerberg (2012, p. 760) have termed a ‘connective’ rather than a ‘collective’ network. Connective networks are self-organising across social media platforms and do not require formal membership of organisations. They function as trusted social networks for the sharing of political content that is readily personalised and semantically open, enabling people with a broad range of motivations and levels of commitment to participate. Memes feature strongly in connective networks, representing both a common trope within the community and an opportunity for individual expression. Connective networks therefore provide a space
for identity formation and performance. While such networks often celebrate real-world achievements aligned with their core beliefs, there is no expectation that participants will translate their own online engagement into real-world action. Indeed, as will be discussed below, continued tolerance of extremist connective networks is often justified on free speech grounds.

The content that circulates within alt-right networks is a mash-up of facts, lies, conspiracy theories, misinformation, memes and historical analysis (Kaiser et al., 2019). A fresh stream of material that reinforces alt-right ideology and gives it currency is provided by media sites ranging from the partisan *Fox News* to the extremist *Daily Stormer* chat board, which is openly neo-Nazi. In their analysis of the links between these sites, Kaiser and colleagues found that the more extreme the site, the more it was focused on identity-defining issues, such as Islam and immigration (Kaiser et al., 2019). While identity politics are normally associated with the left, the alt-right may also be seen as a form of identity politics (Sparrow, 2018; Stump and Dixit, 2016). Identity politics is centred on the oppression experienced by groups of people based on their characteristics, such as race, gender or sexuality. Core to the identity politics of the alt-right is the belief that the so-called ‘white races’ are oppressed by multiculturalism and faced with ‘extinction’ due to immigration and abortion. There is even a core group within the alt-right who label themselves ‘incels’ or involuntarily celibates, and blame feminism for their inability to find sexual partners. The ‘Identitarian’ label is now used widely within European alt-right networks, where Muslims are portrayed as an oppressive, invading force to be resisted and pushed back to their own ‘homelands’ (Ebner, 2017).

Identitarian ideology, which circulates via alt-right social media, is evident throughout the Great Replacement manifesto. This online material was reinforced for the Christchurch terrorist by a self-guided study tour of Asia and Europe, where he learned firsthand about the version of anti-Islamist history promoted by Identitarians. His focus appears to have been on the defeat of the Ottoman Empire, and included visits to the sites of historic battles between Serbians and invading Ottoman armies. He also sought meetings with people active in the European ‘Identitarian’ movement. His Great Replacement manifesto represents a combination of these real and virtual world experiences, and serves multiple functions including justifying violent action against Muslims, aligning the terrorist with the alt-right and Identitarian politics, and framing the massacre as a political act.
An Australian national, the terrorist migrated to Dunedin in 2017. Aotearoa New Zealand does not seem the logical choice for a person who professed in his Great Replacement manifesto to believe both in white supremacy and in the concept of ethnic groups remaining in their so-called ‘homelands’. The country is renowned for its strong commitment to biculturalism based on a partnership between the indigenous Māori and the Crown that originates in the nation’s founding document, the Treaty of Waitangi. Moreover, those professing the Muslim faith – the terrorist’s primary target – made up only 1 per cent of the population according to the 2013 Census. That same census showed that the largest source of immigrants to Christchurch was England (Stats NZ, 2013). While there is limited information about the terrorist’s reasons for choosing Aotearoa New Zealand, it is clear that the country’s relatively lax gun laws were a factor. In Dunedin, he was able to legally purchase semi-automatic rifles and practise the rapid firing of multiple rounds at his local gun club. However, the terrorist’s goals included maximising the number of Muslim people killed and Dunedin had few Muslim residents (Malley, 2019). In contrast, Christchurch offered three mosques located within easy driving distance. The city also boasted excellent mobile broadband. With the alt-right agenda of taking violent action against Muslim immigrants as the motivating force, the site of the attack may have been less important than the ease with which a large massacre could be carried out and livestreamed through social media.

Livestreaming a massacre

In the days leading up to 15 March, the Christchurch terrorist was active on Facebook, Twitter and 8chan. The 8chan website hosted the notorious /pol/ message board, the home of fascists and white supremacists of all affiliations. It was to this receptive audience that the terrorist made his last 8chan post

Well lads, it’s time to stop sh*tposting and time to make a real life effort post. I will carry out and [sic] attack against the invaders, and will even livestream the attack via facebook. (McBride, 2019)

Note: ‘sh*tposting’ is the practice of posting material online – often large quantities of material – that is poor quality and may be offensive. The practice is intended to annoy or provoke those who are not ‘in on the joke’ and can be used to disrupt online discussions. It is a favoured tool of the alt-right and of internet trolls more generally (Gorman, 2019).
2. THE MAKING OF A ‘MADE FOR SOCIAL MEDIA’ MASSACRE

The link to Facebook enabled supporters to watch the massacre live, comment enthusiastically on its progress and, most importantly for the terrorist’s purposes, capture the video and post a link to a file-sharing site so that it could go viral once Facebook had removed the footage (Gorman, 2019). According to Facebook Newsroom (2019a), fewer than 200 people watched the livestream video and none of them made a complaint to Facebook or notified the police. It was only after the gunman had been arrested that Facebook received an official police request to remove the video. By this time, multiple copies were in existence and propagated across the internet. Facebook reported thwarting approximately 1.2 million upload attempts and removing 300,000 copies in the first 24 hours. YouTube did not report the total number of uploads but called the attempts ‘unprecedented’ in scale (Fussell, 2019).

Social media companies rely heavily on users to report objectionable content and employ large workforces devoted to the task of moderating such reports and removing content that violates company policies (Facebook Newsroom, 2019b). The traumatic nature of this work is detailed in a 2018 film, The Cleaners, which documents the lives of thousands of lowly paid social media content moderators based in Manila (Wilson, 2018). The documentary highlights the mental health toll on workers who face a daily parade of horrors. In addition to their ever-growing workforce of content moderators, internet safety advisers and counterterrorism experts, social media companies have invested heavily in developing technologies to automatically block, for example, child pornography, suicides, murders, beheadings and terrorist acts from their platforms. Facebook alone claims that its automated systems enabled the removal of more than 26 million pieces of terrorism-related content in the two years to September 2019 (Facebook Newsroom, 2019d). This figure highlights the scale of the problem, and also points to the size of the workforce on the ‘other side’ of the problem, producing and disseminating extremist content, including through the use of increasingly sophisticated technologies of their own (Singer and Brooking, 2018). Facebook senior executives, including Zuckerberg and Sandberg, have boasted repeatedly of a 99 per cent pre-emptive removal rate of extremist content. More recently, however, whistleblower Frances Haugen has exposed internal Facebook documents suggesting that the actual removal rate may be as low as 5 per cent (Nix and Etter, 2021).
In the face of all the money, technology and human time devoted to preventing such events, the viral success of the Christchurch massacre video – produced using cheap, basic technology by one person – provides a stark illustration of the challenges faced by social media companies. Artificial intelligence (AI) and ‘hashing’ technology are the main tools available and they are successful in blocking significant amounts of content (Facebook Newsroom, 2019c). ‘Hashing’ is akin to taking a digital fingerprint of an image or video. When such content violates the policies of a social media company, a hash is added to a database and is used to automatically block future uploads of that content. In mid-2019, YouTube announced that it had loaded more than 200,000 unique hashes into the database that it shares with other major social media platforms (YouTube Official Blog, 2019). While hashing is adept at blocking the automated reloading of images, there are major weaknesses in the technology. The initial upload of any image will not be in the database and it is this upload that must be prevented if the goal is to prevent livestreaming or reposting to other image-sharing sites. Further, any small alteration to an image, such as adding a watermark or making a video of a video, may fool the system into believing it is assessing a different image.

In the case of the Christchurch footage, there was a further technical issue for AI systems: it was framed as a first-person shooter video game, similar to thousands of other games livestreamed on social media every day. It is difficult for AI to tell the difference between simulated slaughter and actual slaughter. Facebook Newsroom (2019a) reported that there was a ‘core community of bad actors working together to continually re-upload edited versions of this video in ways designed to defeat our detection’. In total, they detected 800 distinct versions of the Christchurch massacre video. Not all of those who reposted the video were, however, ‘bad actors’, with users who may have been horrified by its content nonetheless motivated to share the graphic footage. Sharing newsworthy content with friends is, after all, a highly valued activity on social media platforms. Social media algorithms also tend to promote popular content, rendering them the automated allies of propagandists. The underlying logic of the platforms themselves, along with a whole range of technological and human failings, therefore conspired to ensure that the social media goals of the Christchurch terrorist were achieved.
2. THE MAKING OF A ‘MADE FOR SOCIAL MEDIA’ MASSACRE

Shaping and sharing an alt-right legend

Despite the efforts of mainstream social media platforms, material from the Christchurch massacre continues to circulate. Online posts give prominence to the number of deaths – the ‘kill count’ – and to the killer himself, who is portrayed as a hero and inspiration for the alt-right internationally (Evans, 2019). Given that the video mimicked a first-person shooter game, it is not surprising that shortly after the attack, the footage was reworked into a number of actual video games set in mosques. One game offers the Christchurch terrorist, along with Hitler and President Trump, as a possible avatar (Duffy, 2019). Another version, found on Facebook, combined a game with raw footage of the shootings and appears to have been designed to fool the company’s AI systems (Keall, 2019). The game reportedly eluded detection for some two months before being removed following an alert from a journalist.

While gamification of the Christchurch massacre is disturbing, albeit predictable, perhaps the more dangerous development is the rapid ‘beatification’ of the terrorist on the dark web, where, despite being very much alive, he is routinely referred to as a ‘saint’. The Poway Synagogue gunman reportedly posted online that the Christchurch terrorist ‘was a catalyst for me personally. He showed me that it could be done. And that it needed to be done’ (Dearden, 2019a). The following week, a Norwegian gunman also cited the Christchurch terrorist as the inspiring ‘saint’ behind his failed attack on a mosque (Dearden, 2019a). The perpetrator of the El Paso massacre, in which 18 people were shot in a Walmart store, referenced both the Christchurch gunman and his manifesto in 8chan posts. While the 8chan community embraced and celebrated El Paso, they were openly critical of what one poster termed the gunman’s ‘0 effort manifesto’, comparing his four-page document unfavourably with the 87-page, Great Replacement manifesto (Evans, 2019). Christchurch has become both a motivation and a high bar to match for subsequent alt-right terror attacks.

Given the centrality of 8chan as a host for alt-right terrorists in many nations, it is worth exploring how the website was able to continue for so long. The day after El Paso, Evans (2019) posted on the open-source intelligence site, Bellingcat, that:
In the wake of the Christchurch shooting I published my first Bellingcat article about 8chan. I was interviewed by numerous media agencies about the website, and I warned all of them that additional attacks would follow – every month or two – until something was done. This prediction has proven accurate. Until law enforcement, and the media, treat these shooters as part of a terrorist movement no less organized, or deadly, than ISIS or Al Qaeda, the violence will continue. There will be more killers, more gleeful celebration of body counts on 8chan, and more bloody attempts to beat the last killer’s ‘high score’.

The ability of 8chan to continue to operate lay in the services, including crucial protection from DDOS\(^3\) attacks that the site received from the internet infrastructure company, Cloudflare. After the Christchurch attack and for two days after El Paso, the company continued to defend its support of 8chan on the basis that moderating content was not Cloudflare’s responsibility (Wong, 2019). When Cloudflare did drop 8chan as a client, other companies followed suit and the site suspended services. However, within months it was back, rebranded as ‘8Kun’ but without the /pol/ message board. Some of the extremist chatter of /pol/ migrated to the online gamers’ chat app, Discord, while the ‘dark libraries’ of, for example, Nazi videos, moved to the encrypted messaging app, Telegram (Glaser, 2019). Prominent on 8Kun are the conspiracy theories of QAnon, which were lent support by President Trump even after the FBI had labelled this network a domestic terror threat. The role and libertarian rhetoric of the network of internet companies that enable extremist websites and apps to operate will be explored below. First, however, the multilateral and national responses to Christchurch are examined.

**Multilateral responses**

The viral success of the Christchurch massacre amplified existing concerns about the central role of social media in the spread of violent extremism online (VEO) and motivated some governments to take further, united action. In May 2019, Prime Minister Jacinda Ardern joined with French President Emmanuel Macron to produce the Christchurch Call to

---

\(^3\) Distributed denial of service (DDOS) attacks are attempts to disrupt a website by flooding it with web traffic.
Action, which sought cooperation between governments and technology companies to eliminate VEO. The opening section of the Christchurch Call states:

The Call outlines collective, voluntary commitments from Governments and online service providers intended to address the issue of terrorist and violent extremist content online and to prevent the abuse of the internet as occurred in and after the Christchurch attacks. All action on this issue must be consistent with principles of a free, open and secure internet, without compromising human rights and fundamental freedoms, including freedom of expression. It must also recognise the internet’s ability to act as a force for good, including by promoting innovation and economic development and fostering inclusive societies. (MFAT, 2019)

A central theme within the Christchurch Call – balancing human rights and free speech protections with the prevention of VEO – is evident in this statement. However, citing First Amendment concerns, the US was noticeably absent among the signatories to the call, which included social media giants, Facebook, Twitter and YouTube along with the EU and 17 nations. Subsequently, a further 33 signatories were added to the call, bringing the total number of nations to 47.

A statement released by the US Embassy in New Zealand at the time of the Christchurch Call condemned VEO but asserted:

We maintain that the best tool to defeat terrorist speech is productive speech, and thus we emphasize the importance of promoting credible, alternative narratives as the primary means by which we can defeat terrorist messaging. (US Embassy and Consulate in New Zealand, 2019)

However, the day after the Christchurch Call was released, the White House released its own call, which appeared to move in the opposite direction. Through the White House Twitter account, @WhiteHouse, users were invited to submit details of instances in which they had been ‘censored or silenced online’. This invitation built on allegations made two weeks earlier by Donald Trump Junior of a left-wing bias on social media, including in the following Twitter post:
The purposeful & calculated silencing of conservatives by @facebook & the rest of the Big Tech monopoly men should terrify everyone.

It appears they're taking their censorship campaign to the next level.

Ask yourself, how long before they come to purge you? We must fight back. (Trump Jr, 2019)

This post followed the decision taken by Facebook, as part of its stated commitment to removing hate speech, to place a permanent ban on the alt-right conspiracy site, InfoWars, and on the pages of several prominent figures associated with hate groups.

Despite its subject matter, the Christchurch Call is a softly worded document that contains specific, though non-binding, commitments by governments and online service providers to work individually and collectively to combat VEO. While the primary focus is on the internet, it is noteworthy that the first government commitment relates not to the internet but to social cohesion: ‘Counter the drivers of terrorism and violent extremism by strengthening the resilience and inclusiveness of our societies to enable them to resist terrorist and extremist ideologies’. This statement reflects the actions of Prime Minister Ardern who was widely praised when she asked that the nation come together in support of the Muslim community. When President Trump called to offer his condolences and ask what assistance the US might provide, Prime Minister Ardern reportedly asked that he demonstrate ‘sympathy and love for all Muslim communities’ (Cooke, 2019).

One month after the Christchurch Call, the G20 (2019, Japan) issued a multilateral statement of its own, the ‘G20 Osaka Leaders’ Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism’. Although the G20 statement did not differ substantially from the Christchurch Call in its balancing of free speech and VEO limitations, this time the US was a party to the statement. The US involvement may be due to other differences between the two documents. The G20 statement is shorter, at just 578 words compared with the Christchurch Call’s 1,376 words, and much less specific in relation to the commitments of governments themselves, while ‘urging’ action on the part of online platforms. Perhaps the most notable difference, however, is that the G20 statement makes no mention of the need for governments
to work on community ‘inclusivity’ or social cohesion as a key strategy for combating terrorism. Rather, the G20 statement places responsibility for action onto the major internet companies.

In addition to the multilateral responses embodied in the Christchurch Call and the G20 statement, there have been a number of unilateral actions by nations concerned with regulating the impact of the internet on their societies. The actions of the two nations arguably most affected by Christchurch – Aotearoa New Zealand, the site of the massacre, and Australia, its nearest neighbour and country of citizenship for the terrorist – are briefly outlined below, followed by an overview of industry responses.

**National responses: Aotearoa New Zealand**

There are four main strands to Aotearoa New Zealand’s domestic response to Christchurch: increasing gun control; emphasising the inclusivity of society; preventing the spread of VEO through improving the policies, practices and technologies of online service providers, especially social media companies; and assessing the performance of state agencies in light of the attack. Within 72 hours of the massacre, the government announced plans to tighten the nation’s relatively lax gun control laws. Legislation to ban military-style semi-automatics and assault rifles was passed three weeks later by an overwhelming majority of 119 to one. This rare, united stance of parliament reflects a broader national unity that followed the attack. In her speech to the National Remembrance Service, themed as ‘We Are One’, Prime Minister Ardern spoke of the collective responsibility to combat hate by embracing the humanity of all people (Ardern, 2019a).

While the immediate focus for Aotearoa New Zealand was dealing with the aftermath of the massacre, there was recognition that the context for the attack extended well beyond national borders. Prime Minister Ardern expressed the view that addressing the complexities of VEO would require collaboration within and between multiple nations and across multiple sectors:
In the wake of the March 15 attacks New Zealanders united in common purpose to ensure such attacks never occur again. If we want to prevent violent extremist content online we need to take a global approach that involves other governments, tech companies and civil society leaders. (Ardern, 2019b)

This ‘global approach’ took the form of the Christchurch Call discussed above. It also led Aotearoa New Zealand to work with the Global Internet Forum to Counter Terrorism (GIFCT), an existing consortium founded by Facebook, Microsoft, Twitter and YouTube. Through GIFCT, major online service companies shared knowledge of terrorist activities, collaborated on the development of technologies to combat VEO and undertook joint research. Following the Christchurch Call, and citing it as its inspiration, GIFCT took the further step of becoming an independent agency with an enlarged remit to work in collaboration with civil society and government stakeholders (GIFCT, 2019).

Aotearoa New Zealand’s vehicle for assessing the role of state agencies in relation to the massacre took the form of a Royal Commission of Inquiry. The focus of the Royal Commission was on state agencies and it was tasked with identifying ways of reducing the likelihood of future attacks. Following release of the Royal Commission’s report in December 2020, Prime Minister Ardern apologised for failings on the part of intelligence agencies, which, like those in other Western nations, had failed to pay appropriate attention to right-wing extremism. Subsequently, the government established an Office for Ethnic Communities, appointed a minister for inclusion, diversity and ethnic communities inside Cabinet, launched a new police program to combat hate crime and criminalised the planning of a terrorist attack.

National responses: Australia

For Australia, the Christchurch massacre represented the nation’s first experience of having exported alt-right terrorism to a close ally. Mirroring the US example discussed above, the Australian Government’s discourse on terrorist threats had, since 9/11, centred on Islamist extremist groups with relatively little attention paid to the alt-right. Given the exceptional nature of the massacre, the nationality and ideology of the terrorist might have seemed a natural new focus of attention for Australia. Instead, at least from an Australian Government perspective, attention has
been directed to the US-based social media companies. On the day of the massacre, Australian Prime Minister Scott Morrison spoke of mounting a joint counterterrorism operation with Aotearoa New Zealand in acknowledgement of the fact that the perpetrator was an ‘Australian-born citizen’ and a ‘right-wing extremist, violent terrorist’ (PM of Australia Media Centre, 2019a). However, mention of the terrorist’s Australian nationality or of right-wing extremism quickly disappeared from Prime Minister Morrison’s statements. Just two weeks after the massacre, when the Prime Minister was attending the National Remembrance Service in Aotearoa New Zealand, he went so far as to deny that the terrorist should be regarded as Australian in the following exchange with a journalist:

Journalist: Is there a sense of guilt, a sense of responsibility [inaudible] given that the [inaudible] Australian citizen?

Prime Minister: The crime was perpetrated by an extremist terrorist and extremist terrorists have no nationality. (PM of Australia Media Centre, 2019b)

Other than in his initial statements, Prime Minister Morrison consistently framed the export of terrorism as a failure not of Australia but of social media companies, and as a problem best addressed by technological solutions. He spoke of ‘calling out social media companies on their responsibilities’, asserting that:

They have a responsibility when they put these platforms into public use, to make sure they are safe and that they cannot be weaponised by terrorists. Similarly, they shouldn’t be able to be weaponised for other forms of harm that can affect the youngest of us around here today, through to the most serious of criminal offences. (PM of Australia Media Centre, 2019c)

Prime Minister Morrison also suggested that the problem was a lack of will or commitment to action by the social media companies:

If they can write an algorithm to make sure that the ads they want you to see can appear on your mobile phone, then I’m quite confident they can write an algorithm to screen out hate content on social media platforms. (Laschon and Dalzell, 2019)

In line with this framing, and just three weeks after Christchurch, an Amendment to the Criminal Code regarding the ‘Sharing of Abhorrent Violent Material’ was rushed through both houses of parliament.
The amendment, which is analysed in detail in Chapter 6, was aimed at holding internet service providers, content service providers and hosting service providers accountable for abhorrent material (Keller, 2019).

The Criminal Code Amendment was immediately and widely criticised, including by the UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression, and by the UN special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. In a joint letter to the Australian minister for foreign affairs, the rapporteurs expressed doubt over the amendment’s apparent faith in unproven technological solutions, which might lead companies to adopt a heavy-handed approach in order to avoid significant penalties. They also expressed:

Serious concerns that the approach, particularly the haste of presentation and adoption of the legislation and key elements of the Law itself, unduly interferes with Australia’s obligations under international human rights law. (Kaye and Ní Aoláin, 2019)

Legal academic Nicola McGarrity has speculated that the Australian tendency to resort to restrictive legislation may be due to a lack of constitutionally enshrined, free speech protection:

Australia is the only country in the western democratic world that lacks a national constitutional or statutory bill of rights, and that has meant where other countries exercise restraint because they’re unsure whether measures will impact on freedom of speech or freedom of association or the right to privacy … Australia can just adopt a really gung-ho approach. (Burgess, 2019)

Regardless, the rapporteurs’ concerns were dismissed by the Australian ambassador and permanent representative to the UN on a number of grounds, including that the scope of the legislation was very narrow and that it was necessary to limit the sharing of ‘abhorrent violent material’ that ‘can threaten national security, perpetuate further criminal activity, prejudice the dignity of victims and has the potential to cause harm and distress to various sections of the community’ (Mansfield, 2019). Subsequently, there has been limited explanation of how the legislation will operate in practice and no additional resources have as yet been announced in support of its enactment.
In addition to pushing through legislation at home, Prime Minister Morrison called for the upcoming G20 meeting to discuss social media governance, which resulted in the G20 Osaka Leaders Statement described above. He also convened an Australian summit with major digital platforms, internet service providers and government agencies and ministers, which established the Australian Taskforce to Combat Terrorist and Extreme Violent Material Online. Reporting on 21 June, the taskforce recommended a series of voluntary measures for industry action, including in collaboration with the GIFCT and Australian Government agencies (ATCTEVMO, 2019). These measures included ‘proactive technical intervention’, ‘enhanced moderation’ and ‘live-streaming controls’ along with ‘periodic reporting’ by industry to government. The taskforce report also partially addressed the enlarged role of Australia’s eSafety commissioner who, following the passage of the Criminal Code Amendment, had found her remit expanded from cyber bullying of children and ‘image-based abuse’ of adults, to combating terrorism. This sudden pivot, from cybersafety to cybersecurity, enlarges the remit of the commissioner quite significantly, and in ways that may overlap or conflict with the remit of national security agencies.

Industry responses

In livestreaming the Christchurch massacre, Facebook unintentionally placed a large spotlight on itself and the governance, reach and influence of internet companies more generally. Arguably, the industry has achieved its phenomenal success partly because the regulatory and policy environments within which it operates were designed before it was invented and are ill-suited to its governance. In the wide spaces between the rules, Facebook has grown from a rather disreputable website run out of Mark Zuckerberg’s student dorm, into a Fortune 500 corporation with around 2.4 billion users and annual revenues exceeding US$60 billion. In the absence of externally imposed rules, companies like Facebook have made up their own, often on an ad hoc basis and in response to a new crisis or scandal. The many gaps in the self-regulation of internet companies is partly due to the speed of their development. However, from the very beginning these companies have been highly resistant to the imposition of regulation or any oversight by governments. Instead, the unprecedented
rise of the major internet companies, from startups to globally dominant, multinational corporations, has occurred in the context of a strongly libertarian internet culture.

Since the launch of the World Wide Web, when the internet became available to individuals and the private sector, key figures in the internet’s development have been critical of any form of government control. For example, in his oft-quoted Declaration of the Independence of Cyberspace, a co-founder of the Electronic Frontier Foundation, John Perry Barlow (1996), declared:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone … I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Their utopian vision for the World Wide Web was of an anarchic, global paradise of individual freedom. This vision was blown apart in 2013 by the revelations of whistleblower Edward Snowden who revealed the extent to which internet traffic was being monitored by the US Government (Motion et al., 2016). Since then, there have been multiple instances in which the internet has been harnessed for the surveillance and manipulation of whole populations by state and criminal actors. Rather than being a domain of individual freedom, the internet has been systematically walled off, concentrated and privatised by a small number of companies who have emerged as a new form of monopoly capitalism and market failure. As governments have sought to gain control over the internet, especially in areas related to national security, taxation and crime, its international character has been compromised by increasing fragmentation along national boundaries, most notably by China and North Korea (Singer and Brooking, 2018).

Public trust in the major internet companies was further damaged by their role in the 2016 US presidential election. Following the surprise defeat of Hillary Clinton, Facebook was found to be the source of personal data used illegally by British political consulting firm Cambridge Analytica in support of the Trump campaign, including with so-called ‘fake news’ posts (Margetts, 2019). Facebook also sold advertising to a Russian-based ‘troll factory’, the Internet Research Agency, which was later indicted by a US
Grand Jury on charges of interfering with a US election. Facebook first denied, then downplayed, the possibility that misuse of its platform could play a significant role in voter choices. By late 2017, Facebook was under such pressure that CEO Zuckerberg backtracked from his earlier position, and admitted that it was not ‘a crazy idea’ that the scale of the platform was such that it might be deployed to change the outcome of an election (Levin, 2017).

The view that major social media platforms might be ‘weaponised’ by bad actors for political and criminal purposes took hold. After an extensive investigation by the US Federal Trade Commission (FTC) into the misuse of the private data of 87 million users, Facebook was fined US$5 billion. This statement by the FTC chairman highlights the extent of alleged wrongdoing in relation to data privacy:

In 2012, Facebook entered into a consent order with the FTC, resolving allegations that the company misrepresented to consumers the extent of data sharing with third-party applications and the control consumers had over that sharing … Our complaint announced today alleges that Facebook failed to live up to its commitments under that order. Facebook subsequently made similar misrepresentations about sharing consumer data with third-party apps and giving users control over that sharing, and misrepresented steps certain consumers needed to take to control [over] facial recognition technology. Facebook also allowed financial considerations to affect decisions about how it would enforce its platform policies against third-party users of data, in violation of its obligation under the 2012 order to maintain a reasonable privacy program. In addition to these order violations, today’s complaint alleges that Facebook violated the FTC Act by engaging in a new set of deceptive practices relating to the collection and use of consumer phone numbers provided by consumers to enable security features such as two-factor authentication. (USFTC, 2019)

The FTC statement alleges that internet companies cannot be relied upon to voluntarily ‘do the right thing’ in the absence of legal constraints and in the face of significant and conflicting financial incentives. More than this, the statement alleges both ‘misrepresentations’ and ‘deceptive practices’ in relation to data privacy, which suggests active intent rather than accidental violations.
The Snowden revelations and the FTC judgement had focused public attention on data privacy and data protection. The Christchurch massacre raised a whole new set of concerns centred on the lack of accountability by internet companies for the content posted by users, with an additional level of concern in relation to the livestreaming of atrocities. In the US, s. 230 of the Communications Decency Act of 1996 protects internet companies from any responsibility for the content posted by users (Harvard Law Review, 2018). For example, Zeran v. America Online, Inc. found that s. 230 ‘creates a federal immunity to any cause of action that would make service providers liable for information originating with a third party user of the service’ (Harvard Law Review, 2018). Under s. 230, internet platforms have enjoyed legally immunity from prosecution – at least in the US – for the publication of prohibited forms of speech, including defamation. Indeed, despite becoming the world’s largest publishers of content and gatekeepers to the content of others, Facebook and Alphabet have not been legally defined as publishers at all. At the time of writing, and following the storming of the US Capitol Building by a mob intent on preventing the confirmation of President Biden, a Bill that would place limits on s. 230 is before the US Congress. Outside the US, governments have also begun to hold internet companies responsible for their user-generated content, including through the Australian Amendment to the Criminal Code discussed above and in subsequent chapters by Wheeler and by Nolan and Dalla-Pozza.

In the face of growing pressure to act, the major internet companies have been active participants in global discussions around combating VEO, including becoming signatories to the Christchurch Call. The arguments of the libertarian past have been all but abandoned as companies struggle to deal with the attempted invasion of their platforms by a myriad of bad actors including terrorists, paedophiles, fraudsters and troll farms propagating ‘fake news’ (Coleman, 2015). Two weeks after Christchurch, Facebook CEO, Zuckerberg, stated:

Every day we make decisions about what speech is harmful, what constitutes political advertising, and how to prevent sophisticated cyberattacks. These are important for keeping our community safe. But if we were starting from scratch, we wouldn’t ask companies to make these judgments alone. I believe we need a more active role for governments and regulators. By updating the rules for the internet, we can preserve what’s best about it – the freedom for people to express themselves and for entrepreneurs
to build new things – while also protecting society from broader harms. From what I’ve learned, I believe we need new regulation in four areas: harmful content, election integrity, privacy and data portability. (Kimball, 2019)

The statement both invites government intervention and attempts to steer the attention of governments and regulators in particular directions. As discussed above, the major social media platforms are already spending billions on voluntary content moderation, and on safety and security more generally. One of the biggest threats these companies face to their global business model is the increasing ‘balkanisation’ of the internet that is occurring in response to, for example, terror attacks and foreign interference in elections. After self-regulation in an environment of zero liability for their content, the next best option for internet companies would be globally agreed rules that they had had a major role in drafting.

Being seen to act as good and concerned corporate citizens is also a defensive strategy in the face of an additional threat to the business model of the major players, such as Facebook, Alphabet and Amazon. In an opinion piece entitled ‘It’s time to break up Facebook’, the company’s co-founder, Chris Hughes (2019), argued that: ‘Facebook isn’t afraid of a few more rules. It’s afraid of an antitrust case and of the kind of accountability that real government oversight would bring’. The sheer size and reach of platforms such as Facebook, Google, YouTube and Twitter underpins their profitably. It also enhances their utility for fraudsters, terrorists, election hackers and other bad actors. In the face of numerous scandals and crises, such as the livestreaming of the Christchurch massacre, governments are under increasing pressure to address the growing power of the major internet companies.

In July 2019, the US Department of Justice announced that it was ‘reviewing whether and how market-leading online platforms have achieved market power and are engaging in practices that have reduced competition, stifled innovation, or otherwise harmed consumers’ (USDoJ, 2019). A month earlier, the Australian Competition and Consumer Commission (ACCC) had released its own Digital Platforms Inquiry, which focused on the detrimental impacts of major platforms on conventional news media. Despite the fact that they do not produce news, and are therefore exempt from the complex regulatory frameworks governing media companies, Facebook and Google emerged as major players in the Australian news media market (ACCC, 2019, p. 101). Advertising revenues have shifted
accordingly, leading to the reduced production of Australian news content by cash-strapped media companies. The ACCC found that such news was ‘important for the healthy functioning of the democratic process’ and that there was no evidence of a ‘business model that can effectively replace the advertiser model’ for media companies (p. 1). A new ‘platform-neutral regularity framework’ that would level the playing field was recommended (p. 31). This recommendation is in sharp contrast with the s. 230 protections and advantages enjoyed by internet companies in the US.

The ACCC inquiry found that ‘disinformation’, which was widespread on the major platforms, was being used to ‘influence public opinion’, and was a ‘significant public policy concern’ (ACCC, 2019, p. 358). In the interests of protecting Australian democracy, the ACCC recommended a raft of measures to address the perceived market failure, including increased funding for public broadcasters and for media literacy programs in schools and the broader community. While finding evidence that the algorithms deployed by major digital platforms tended to direct users to increasingly extreme content, the ACCC concluded that more research was required to understand ‘echo chambers’ effects. They did not make any specific recommendations in relation to the role of social media in the radicalisation of terrorists or the creation of a more divided polity. At the time of writing, a Bill is before the Australian Parliament that would require Google and Facebook to pay Australian media for the use of their content. Given that the Bill could potentially set a global precedent, it has been met with fierce opposition from Google, which has threatened to turn off its ‘search’ function, and Facebook, which has threatened to block Australian content.

The lessons of Christchurch

Despite all the media attention, agreements signed and commitments to action made by governments and industry since Christchurch, there have been multiple copycat attacks by suspected alt-right terrorists. One such attack, on a German synagogue, was livestreamed on Amazon’s Twitch without any human or AI intervention, and the video was subsequently shared across multiple platforms (Haselton and Graham, 2019). As with Christchurch, the shooter had posted a hate-filled manifesto outlining
his white nationalist ideology, this time on the German-language site, Kohlchan (Dearden, 2019b). On other extremist sites, the attack is already being celebrated in the name of the ‘sainted’ Christchurch terrorist.

Amazon is a signatory to the Christchurch Call, including to the pledge to implement ‘immediate, effective measures to mitigate the specific risk that terrorist and violent extremist content is disseminated through livestreaming’ (MFAT, 2019). The major lesson to be learned from the Christchurch massacre may be the confronting reality of how difficult it is to prevent the attacks themselves along with their global dissemination through social media. However, internet platforms play a far broader role than that of mere broadcasters. They appear to be implicated in multiple, overlapping ways, including as a contributing cause and source of motivation for terror attacks. The platforms have become a standard part of the terrorist’s toolkit for marketing ideology, recruiting followers, advertising successful massacres and canonising perpetrators. Through social media, the alt-right has become a globally connected community, united against perceived threats to the dominance of white men. Feminists, Muslims, Jews and refugees are all targets of their hate speech. The Christchurch terrorist and his imitators all used social media to encourage direct, violent action against these targets. Social media did not cause the terrorists to embrace extremism in any straightforward way, but it did provide a community of like-minded people who reinforced the validity of mass murder in the name of white nationalism. The community furnished role models to emulate and provided advice on terror methodology. A helmet-mounted camera with an internet connection is now a key part of this methodology. In short, social media figures in every aspect of the Christchurch terror attack: in its inspiration, planning, preparation and execution, and in perpetuating its iconic status within the alt-right community.

This chapter has outlined some of the responses to Christchurch on the part of governments and industry that were intended to prevent future massacres. Unfortunately, these responses have raised a myriad of related, complex issues that reduce the likelihood that the responses will succeed. From the start, government statements on the massacre emphasised the importance of an inclusive society that embraced Muslims. However, this framing conflicted with the mainstream media’s portrayal of Muslims as a source (not a target) of terrorism (Blee, 2016). It also conflicted with the discourse of US President Trump who was elected on a platform that resonated with alt-right fears of immigration and Islamist terror.
This mainstreaming of alt-right ideas was reinforced by President Trump when he rejected the Christchurch Call, and by Donald Trump Jr who openly attacked the so-called ‘Big Tech monopoly men’ on the basis that they endangered ‘conservatives’ (Trump Jr, 2019). The word ‘monopoly’ played directly to the biggest fear of major internet companies, which is an antitrust suit that would lead to their dismantling. Much of the delicate work of blocking or countering extremist content while not impinging on free speech falls to US-based multinationals, such as Facebook, Alphabet and Amazon. The companies are seriously conflicted in making these fine judgements by their desire to avoid offending those capable of threatening their market dominance.

Internet companies are not alone in their struggle to balance free speech with internet safety. The Australian Government faced this same dilemma when it amended the Criminal Code to make internet companies liable if they failed to remove ‘abhorrent violent material’ swiftly from their platforms. The legislation was criticised for incentivising internet companies to engage in heavy-handed censorship in order to avoid hefty penalties. Australia is signatory to a number of international agreements that would seem to prohibit such censorship. The spectre rises of China’s digital Great Wall, which protects citizens from terrorist propaganda but also isolates them from ideas and information not sanctioned by the state. Each fresh tragedy lends further impetus to calls for the erosion of human rights in the name of safety. Technology features in all these debates both as a problem to be solved and as the solution.

The inability of technology, at least in its current phase of development, to perform the tasks we now ask of it is evident. The Australian prime minister was mistaken in his view that automating terrorism detection was akin to automating an advertising feed in social media. Only in the former is the tolerance for errors set at zero due to the massive consequences of mistakes. Even one livestreamed massacre is a catastrophe. While they work on technological solutions, internet companies default to employing thousands of staff dedicated to content moderation. This private army engages in daily battle with terrorists and criminals – driven by a range of ideological and economic motivations – as well with individual hackers who view the battle as sport (Gorman, 2019). Its very existence raises issues of where the public–private divide ought to sit between industry self-governance and government regulation and policing. When individual governments decide to act alone their options are limited by the global character of the internet. When they seek international cooperation, the
resulting agreements tend to default to voluntary industry compliance. Meanwhile, the internet itself is a continuously shapeshifting entity that grows in power and reach every day. There are no simple solutions to combating violent extremism online and the complexity is only increasing.

References


Trump, Donald Jr. (2019, 4 May). @DonaldJTrumpJr, 1.46 am. Twitter.com.


