The Political Economy of Communication
7(1), 83–104

http://www.polecom.org

Beware of Geeks Bearing Gifts: Assessing the Regulatory Response to the Christchurch Call

Peter A. Thompson, Victoria University of Wellington, Aotearoa-New Zealand

This commentary is an updated and expanded version of a May 2019 policy discussion document Beyond the Christchurch Call, prepared for the Better Public Media Trust (of which the author is board chair).

In May 2019, the Christchurch Call summit in Paris brought together the European Commission, 17 governments and eight major digital media corporations to discuss ways to combat the proliferation of violent extremist content online. Initiated by New Zealand prime minister, Jacinda Ardern, and French president, Emmanuel Macron, the summit was impelled by the terrorist attacks on two mosques in Christchurch in March 2019. Fifty-one people were murdered by a white supremacist who used GoPro to livestream his rampage on Facebook (literally from a first-person shooter perspective). The impetus for the Christchurch Call summit stemmed partly from the unexpectedness of such events transpiring in an ostensibly peaceful and developed country like New Zealand [1]. However, the use of social media to stream the attacks was a crucial factor in crystallizing concerns about the harmful consequences of leaving digital intermediaries unregulated. Although Facebook removed the terrorist video, this came only after they received notification from the police, by which time the live stream had already finished. This indicated that users were not reporting the video, and that Facebook's default algorithms were unable to recognise its nature (Chang, 2019). In the meantime, 4,000 people had watched the video feed and although Facebook's updated algorithms blocked 1.5 million uploads over the ensuing 24 hours, 300,000 versions were uploaded and had to be removed by moderators (RNZ, 2019a; see also Keall, 2019).

Predictably, the live-feed was also uploaded to a variety of websites tolerant of extremist content such as 4chan and 8chan, which lie outside New Zealand's legal jurisdiction and which were insulated from denial-of-service interference by network services such as Cloudflare (although this service was withdrawn after the El Paso Walmart massacre - see Taylor and Wong, 2019). The video was also disseminated through a wide range of mainstream media websites; excerpts appeared in *The Sun*, *The Daily Mail* and *The Daily Mirror* in the United Kingdom (Waterson, 2019), while in Australia Sky News, channels Seven and Nine and even SBS included some selected footage in their reports (Williams, 2019). Even a month after the attacks, re-edited versions with altered digital identifiers were still being discovered on Facebook, Instagram and YouTube,

one of which had 700,000 views (RNZ, 2019b). It was also played at a public rally for Turkish President, Tayyip Erdoğan.

Gaining support in principle for measures to prevent live-streaming terrorism is hardly controversial. Nevertheless, the Christchurch Call has opened up a space wherein the issue of social media regulation can be debated legitimately without the ideological default to neoliberal objections concerning state interference in the media. This commentary aims to contextualise the initiative with reference to policy developments in various countries (including the United Kingdom, France, Australia and New Zealand). It will identify some of the key policy complexities whereby competing vested interests are seeking to shape or circumscribe regulatory responses, and set out a broader framework of policy options for addressing issues raised by the activities of social media and digital intermediaries. It will then argue that although the Christchurch Call opens up an important space for multi-lateral policy deliberation, the high-level engagement of governments and corporations risks circumscribing the range of policy options which can be progressed. Consequently, the Christchurch Call needs to be complemented by robust regulatory responses which will hold social media and digital intermediaries accountable and defend civic interests against their incumbent power.

Reluctant self-regulation?

The size and scope of the social media and digital intermediaries coupled with the practical challenges of brokering international regulatory frameworks has historically persuaded governments to leave the tech companies unchallenged as the default agents of regulatory change. Unsurprisingly, the companies have selectively adopted modes of monitoring content while deflecting attempts to introduce statutory regulations at operational levels where their commercial interests are liable to be compromised (see Winseck, 2015).

Although Facebook is only one of many social media/ online intermediary companies, it has become the poster-child for proponents of stronger state-based regulation across the sector. Its role in enabling the live-streaming of the Christchurch terrorist attacks was preceded by a litany of ethically dubious practices. More recently, Facebook has been hit by a record US$5 billion fine from the Federal Trade Commission for privacy breaches, abuses of data and its role in the Cambridge Analytica scandal (Kelly, 2019b). Facebook certainly has a questionable track record in blocking extremist content. In 2018, Channel 4's *Dispatches* uncovered Facebook's 'shielded review' moderation system which permitted high-traffic right wing hate speech posted by groups such as the English Defence League and Britain First to remain online despite numerous complaints. It was only after the Christchurch terror attack that Facebook acquiesced and blocked the content in April 2019. Facebook also recently moved to block white nationalist content but as a Vice Motherboard investigation uncovered, its earlier response to the racially-motivated Charlottesville murder in 2017 was to block white supremacist content while expediently allowing white nationalist material to remain (Cox, 2018, 2019; Cox and Koebler, 2019b). Although Facebook has attracted the most criticism, Twitter and YouTube lag behind it in controlling extremist content. YouTube algorithms optimize traffic and user consumption by recommending increasingly extreme content in response to key-word searches. Another recent Motherboard report identified discrepancies between Twitter's robust policing of Islamic State content compared with their lax oversight of right wing content, and cites one executive's concern that controlling the latter would result in Republican politicians being blocked (Cox and Koebler, 2019a).

A UK government report was blunt in its assessment of digital intermediaries' willingness to act responsibly*:*

> We note that Google can act quickly to remove videos from YouTube when they are found to infringe copyright rules, but that the same prompt action is not taken when the material involves hateful or illegal content … The biggest and richest social media companies are shamefully far from taking sufficient action to tackle illegal and dangerous content (House of Commons/Home Affairs Committee, 2017, paras 3.1/3.3).

Interestingly, a week before the Christchurch attack, Facebook's Mark Zuckerberg outlined a privacy-oriented model for social networking; encrypted messaging tools, data storage and deletion options for all Facebook apps would give more control over communications to private individuals. Acknowledging the tension between protecting legitimate dissidents and affording privacy to 'bad actors', he went on to note "a growing concern among some that technology may be centralizing power in the hands of governments and companies like ours" (Zuckerberg, 2019a). A fortnight after the attack, however, Zuckerberg published an op-ed in the Washington Post, inviting *"*a more active role for governments and regulators" on issues like election integrity (e.g. transparency over political advertising), privacy, and data portability. He also called for more consistent guidelines on harmful content, remarking that *"*Regulation could set baselines for what's prohibited and require companies to build systems for keeping harmful content to a bare minimum*"* (Zuckerberg 2019b).

Apart from seeking to redress reputational damage from its facilitation of livestreamed terrorism and previous abuses of user data (e.g., permitting apps that harvested third party data and complicity with Cambridge Analytica's political machinations), Facebook's new-found openness to state regulation is founded on self-interest (Cadwalladr, 2017). It is apparent from Zuckerberg's remarks that, beyond clearer legal definitions of 'baselines', industry actors are still regarded as the principal agents of regulatory intervention.

Indeed, statutory regulation potentially offers strategic advantages for social media and digital intermediaries, especially if they are involved in its design and implementation. Media companies which enable content discovery and sharing between third parties currently operate within an unspecified regulatory environment between publishing and platform provision. In the absence of statutory definition of their obligations and liabilities in regard to content management, it is difficult to assess regulatory risk and the scope or scale of potential penalties, especially when these vary between jurisdictions.

Formal regulation (such as defining what content is deemed harmful) would allow digital intermediaries and social media to maintain a default defence of compliance with applicable laws (which could also specify the maximum penalties for violations) (see Isaac, 2019). As the pro-free market Mises Institute observes, increasing compliance costs (e.g., requiring social media to expand content monitoring) favours market incumbents like Facebook. Moreover, "By offloading decisions about harmful content, privacy rules, and elections onto third-parties, Facebook may not have to take as much of the heat when mistakes are made" (McMaken, 2019).

The return of the regulators?

The political momentum toward regulation of online/social media and other digital intermediaries was already well under way well before the terrorist attack in Christchurch and the subsequent

summit in Paris. Unsurprisingly, in the wake of the Christchurch attack, the resolve of governments to regulate social media and digital intermediaries has hardened, with a variety of responses. As Annany and Gillespie (2017) and Flew, Martin and Suzor (2019) have presciently observed, policy responses rushed through in response to 'public shocks' such as mass shootings risk being poorly designed and may deliver unintended outcomes. Indeed, there is a risk that policymakers under public pressure to take action on social media will focus on immediate symptomatic issues and misdiagnose deeper structural problems.

Some researchers and policy actors have sought to designate social media and digital intermediaries as media content publishers in order to bring them under existing regulatory frameworks, just as the corporations have often resisted such definitions (Napoli and Caplan, 2017). As New Zealand's prime minister, Jacinda Ardern recently observed, "We cannot simply sit back and accept that these platforms just exist and that what is said on them is not the responsibility of the place where they are published. They are the publisher. Not just the postman." (quoted in Small, 2019). Others have argued that defining digital intermediaries as media publishers invokes the wrong regulatory paradigm for many of the contemporary policy concerns. Winseck (2019), for example, suggests that the definition of content in these circumstances cannot be equated to the content of editorial work or publishing, and cautions that extremist content online can often be addressed adequately by existing laws. This view does not assume that digital intermediaries and platform providers are neutral channels of transmission with no content-related responsibilities. Their market scale and power certainly needs to be addressed through statutory measures. Winseck (2019) suggests functionally equivalent data-privacy protection measures across all layers of the value chain, including information fiduciary [2] obligations on platforms/intermediaries as well as requirements for algorithmic transparency and audits.

In the United States, senator Elizabeth Warren has called for anti-trust measures to break up dominant 'platform utilities' such as Amazon, Facebook and Google, arguing that they exert "too much power over our economy, our society, and our democracy. They've bulldozed competition, used our private information for profit … [and] hurt small businesses and stifled innovation" (quoted in Caplin, 2019). The European Commission, in conjunction with several major tech firms, introduced a Code of Conduct in 2016 to restrict the proliferation of online hate-speech. Germany, meanwhile, introduced the 2017 Network Enforcement Act (NetzDG) which requires the removal of hate speech within 24 hours and imposes fines for failing to respond (in fact Facebook now employs almost a sixth of its global content moderation staff in Germany) (see Flew et al., 2019). However, opponents have argued that NetzDG has led moderators to block contentious but legitimate expression (Kinstler, 2019).

In the United Kingdom, the 2017 House of Commons, Home Affairs Committee report on online hate speech and extremism identified the reliance of social media on the user community to police content as inadequate. More robust measures were needed because "the interpretation and implementation of the community standards in practice is too often slow and haphazard" (2017, para 3.9). The report also noted the inapplicability of traditional frameworks of media regulation to social media and digital platform operators.

In 2018, the government also announced the introduction (from 2020) of a 2 percent levy on the domestic turnover of digital intermediaries with global revenue of over £500m (BBC 2019a). Intended primarily as a remedial initiative to force global tech companies to pay the tax they otherwise avoid by declaring profits in offshore havens, the initiative is important because it reclaims online commercial turnover as domestic economic activity. The recent Online Harms

White Paper (Department for Digital, Culture, Media and Sport/ Home Office, 2019) sets out a series of "duty of care" responsibilities for digital intermediaries under a new regulatory body with the power to impose fines for violations. The onus would be on social media companies to limit harmful content (notably extremist/terrorist material and child sexual abuse). The duty of care also extends to increasing source transparency and reducing the propensity for filter-bubbles to proliferate disinformation (see sections 7.27-7.31).

France has also been pro-active in its response to social media regulation. President Emmanuel Macron, along with Jacinda Ardern, was, of course, instrumental in bringing state and industry together for the Christchurch Call summit in Paris. In May 2019, an interim report (commissioned before the Christchurch attacks) setting out the French framework for social media regulation was published. The regulatory team was granted six months of access to Facebook (France 24, 2019) and concluded that:

> Even if the abuses are committed by users, social networks' role in the presentation and selective promotion of content, the inadequacy of their moderation systems and the lack of transparency of their platforms' operation justify intervention by the public authorities, notwithstanding the efforts made by certain operators (Office of the Secretary of State for Digital Affairs, 2019: 10).

The report recommended a range of regulatory measures, including an "independent administrative authority, acting in partnership with other branches of the state, and open to civil society" (3). Three key transparency obligations were also cited: algorithmic ordering of content; terms of service and content moderation; and a requirement to defend user integrity (equivalent to a 'duty of care') (21). In July 2019, the French Parliament also approved a bill obliging digital intermediaries to remove content deemed to promote 'obviously hateful' speech. This included extremist, violent, racial and religious discrimination and child pornography with fines of up to €1.25 million if the content was not blocked within 24 hours (Kelly, 2019a). However, this initiative is subject to senate approval and some critics have suggested that it gives too much control over content to the intermediaries (The Guardian, 2019).

In a separate initiative, the government announced a 3 percent levy on the domestic turnover of major tech corporations with annual (global) turnover of over €750m. The specific targets were digital advertising and the sale of personal data to facilitate advertising. As with the United Kingdom's digital tax model, this effectively pre-empts a very similar European Commission proposal advanced earlier in 2019 (BBC, 2019a, 2019b). There has, thus far, been a highly negative response to these developments from the Trump administration because most of the digital intermediaries falling under the new regime are based in the United States.

In Australia, there was a swift legislative reaction to the Christchurch terror attack: The new Unlawful Showing of Abhorrent Violent Material Bill took barely a fortnight to be approved by Parliament (Attorney-General for Australia, 2019). Social media companies failing to remove extreme content (e.g., terrorism, murder and rape) in a timely manner after notification from a new e-Safety commissioner would be liable either for a fine up to 10% of their turnover or a sentence of three years imprisonment for the responsible executives. Minister for Communications, Mitch Fifield, explained the move thus:

> Mainstream media cannot live broadcast the horror of Christchurch or other violent crimes and neither should social media be able to do so … Where social media

> platforms fail to take action to stop the live streaming of such violent and abhorrent crimes, they should face serious penalties and that's what will now occur once this Bill receives Royal Assent (quoted in Attorney General for Australia, 2019).

Although the legislation targeted a narrow range of particularly extreme content, the Digital Industry Group Inc. (representing Facebook, Google and Twitter) has argued that the bill was rushed through with insufficient deliberation and that United States law prevented these groups from sharing content data (Bogle, 2019). Three months later, the report of the Australian Competition & Consumer Commission (ACCC) Digital Platforms Inquiry (July 2019) was published, recommending a wider range of measures to redress the market power of digital intermediaries. These include developing a harmonized regulatory framework for digital media on a platform-neutral basis alongside a code of conduct to promote a fairer balance of relations between digital intermediaries/platforms and news media. Flew (2019) suggests that the ACCC's platform-neutral approach is important, as is its recognition that digital intermediaries require specific measures that currently fall between competition and platform-neutrality measures and Australian Communications and Media Authority's (ACMA) content regulation regimes. The ACCC report also notes the need for large digital platform providers with over a million users to develop a code of practice to address disinformation and fake news. However, unlike the Abhorrent Violent Material Bill, this appears to place the onus back on the digital intermediaries to develop their own criteria for managing online content. The proposals also contain measures to strengthen privacy protections, including consumer consent for data sharing, more rights for consumers to opt out and/or seek legal redress for breaches.

In Aotearoa-New Zealand, the complexities of digital convergence have been recognised by successive governments, but to date there has been no fundamental overhaul of the regulatory framework since the neoliberal reforms of the late 1980s (although the 2008 Review of Regulation initiative attempted this before being canned) (Thompson, 2019). The 2015 Exploring Digital Convergence consultation (Ministry for Culture and Heritage/ Ministry of Business Innovation and Employment, 2015) sought to resolve the gaps in the Telecommunications and Broadcasting Acts (including online services and content standards) but the ensuing legislation never progressed. In New Zealand, it is apparent that policy initiatives addressing the issues surrounding social media and digital intermediaries (along with other communication policy issues) have become somewhat fragmented across different government departments. As Mason and Errington (2019) observe, the regulation of social media is "being addressed in a piecemeal fashion by an array of government agencies, including the Privacy Commission, the Ministry of Justice, the Department of Internal Affairs, and Netsafe" (2019:4).

Nevertheless, the 2015 Harmful Digital Communications Act (see Ministry of Justice, 2017), does address cyber-bullying and harassment, with measures to restrict harmful, threatening and offensive messages. However, the framework mainly targets peer-to-peer abuse and does not encompass broader issues concerning hate speech facilitated by digital intermediaries and social media.

The immediate regulatory response to the Christchurch attack was a move by the chief censor to classify the terrorist's live-streamed video and accompanying manifesto as "objectionable". The penalties for possession or distribution are fines of up to NZ$10,000 or imprisonment of up to 14 years (Department of Internal Affairs/Te Tari Taiwhenua, 2019a). Thus far, one neo-nazi has been jailed for 21 months for illegally distributing the video.

A Royal Commission of Inquiry into the attack on the Christchurch mosques was also announced in April (Department of Internal Affairs/Te Tari Taiwhenua, 2019b). This is focused primarily on investigating why state agencies were unable to anticipate or prevent the Christchurch attack, but it is likely that the use of social media by extremists (and police monitoring thereof) will be highlighted. It is also significant that, in April 2019, the government pushed through a bill banning military-style semi-automatic firearms and moved to set up a buy-back scheme despite protestations from the local gun lobby (a legal initiative that still seems unthinkable in the United States notwithstanding the recent El Paso and Dayton mass shootings).

Several New Zealand-based NGOs and think tanks also published extensive commentaries and reports in advance of the Christchurch Call. InternetNZ, facilitated a "civil society" statement on the Christchurch Call response informed by the Voices for Action meeting in Paris the day before the Paris Summit (InternetNZ, 2019). Focusing on human rights issues, the report argues for a free and open internet as core principles. Although supportive of regulation on terrorist and other extremist content, the report highlights the need to define such terms carefully and avoid inadvertently inviting authoritarian responses which could harm civic interests:

> It is of vital importance that governments participating in the Christchurch Call commit to robust accountability and oversight to ensure that laws, mechanisms, and other initiatives to combat terrorism online do not result in disproportionate human rights violations of political critics, human rights defenders, journalists, ethnic or religious minorities, refugees, asylum seekers, and migrants (InternetNZ, 2019: 1)

The report also emphasised the need to differentiate between social media and infrastructure providers and insisted that regulatory measures not impinge on open access to the infrastructures of the internet (see also Carter and Komaitis, 2019). The Helen Clark Foundation (Mason and Errington, 2019) noted that, even if the social media companies did not intend to promote extremist content per se, they are highly motivated to optimise traffic through the sharing and discussion of controversial material. Cautioning against a regulatory default to the United States framework of media regulation, the report supports a new regulatory body along with a statutory "duty of care" for social media platforms (including reasonable measures to develop technologies and mechanisms to minimise harm). Another report from the Workshop (Elliott, Berentson-Shaw, Kuehn and Salter, 2019) identified three overarching regulatory challenges: platform monopolies; algorithmic opacity; and the constraints of the attention economy. The report supports regulating digital intermediaries and social media to control extremist content, but stresses the need for clear definitions. Importantly, it highlights the need for a response that extends beyond content regulation to consider a wider range of structural issues in the digital media ecology. To this end, it also calls for technological solutions in the design of digital platform architectures to encourage civic participation.

The Christchurch Call: tip of the iceberg?

New Zealand's prime minister, Jacinda Ardern, gained international attention and praise after her empathetic support for the Christchurch Muslim community in the aftermath of the attacks. Images of her wearing a hijab and hugging one of the survivors were published in news media around the globe. Jacinda Ardern, working alongside the French president, Emmanuel Macron, attracted global media attention and provided a persuasive pretext for government and industry to attend the

Christchurch Call summit. In addition to the European Commission, government actors included Australia, Canada, France, Germany, Indonesia, India, Ireland, Italy, Japan, Jordan, the Netherlands, New Zealand, Norway, Senegal, Spain, Sweden and the United Kingdom (the United States was conspicuous by its absence, although a White House statement later endorsed the anti-terrorist aims of the Christchurch Call - see White House, 2019). Meanwhile, the industry actors present were Amazon, Daily Motion (Vivendi), Facebook, Google, Microsoft, Qwant (French search engine provider), Twitter and YouTube (also a Google Subsidiary).

The ensuing pledge document (the Christchurch Call, 2019) is only three pages long and non-binding. It is obviously unrealistic to expect more from a one-day summit. Indeed, the achievement of getting government and key industry actors to sit together at the table and agree on basic principles arguably matters more than the content of the ensuing pledge, insofar as it sets the stage for future deliberations and multilateral engagement among government actors and industry. However, the fact that civic actors were left to meet separately is perhaps indicative of the narrow scope of debate. Had the Paris summit failed to produce any sort of multilateral agreement, it might well have backfired and served to reinforce the perception that the global tech firms cannot be effectively regulated. The document outlines broad commitments and principles in three areas, the edited highlights of which are listed below (the Christchurch Call, 2019):

Governments

- Counter the drivers of terrorism and violent extremism by strengthening the resilience and inclusiveness of our societies.
- Ensure effective enforcement of applicable laws that prohibit the production or dissemination of terrorist and violent extremist content.
- Encourage media outlets to apply ethical standards when depicting terrorist events online.
- Support frameworks, such as industry standards, to ensure that reporting on terrorist attacks does not amplify terrorist and violent extremist content.
- Consider appropriate action to prevent the use of online services for the purposes of disseminating terrorist and violent extremist content.

Online Service Providers

- Take transparent, specific measures to prevent the upload of terrorist and violent extremist content and its dissemination on social media and similar content-sharing services.
- Provide greater transparency in the setting of community standards or terms of service.
- Enforce those community standards or terms of service in a manner consistent with human rights and fundamental freedoms.
- Implement immediate, effective measures to mitigate the specific risk that terrorist and violent extremist content might be disseminated through livestreaming.
- Implement regular and transparent public reporting.
- Review the operation of algorithms and other processes that may drive users towards terrorist and violent extremist content in order to identify possible intervention points.
- Work together to ensure cross-industry efforts are coordinated and robust.

Governments and online service providers

- Work with civil society to promote community-led efforts to counter violent extremism in all its forms.
- Develop effective interventions based on trusted information sharing in regard to algorithmic and other processes (so as to redirect users away from terrorist and violent extremist content).
- Accelerate research into the development of technical solutions which will detect and immediately remove terrorist and violent extremist content online.
- Support research and academic efforts to better understand, prevent and counter terrorist and violent extremist content online.
- Ensure appropriate cooperation with and among law enforcement agencies for the purposes of investigating and prosecuting illegal online activity in regard to terrorist and violent extremist content.
- Support smaller platforms as they build capacity to remove terrorist and violent extremist content.
- Collaborate with, and support partner countries in the development and implementation of best practice in preventing the dissemination of terrorist and violent extremist content online.
- Develop processes allowing governments and online service providers to respond rapidly, effectively and in a coordinated manner to any major event which involves the dissemination of terrorist or violent extremist content.
- Avoid directly or indirectly contributing to adverse human rights impacts through their business activities and by addressing such impacts as and when they occur.
- Recognise the important role of civil society concerning the issues and commitments in the Christchurch Call.

The predominant focus on measures curtailing terrorist and extremist content, while understandable in the short-term, also underlines the narrow premises of agreement among government and tech sector actors. The cursory acknowledgement of human rights and the role of civil society do nothing to guarantee that future deliberations will not be quarantined within a narrow content-oriented framework.

There are three important arguments for pursuing a more extensive approach to the regulation of social media and digital intermediaries, both within domestic jurisdictions as well as through the multilateral Christchurch Call framework.

1. The concerns over online hate-speech and extremism, while important, are symptomatic of deeper structural patterns in the digital media ecology, including:

    a) Intensified financialisation and commercial competition (with commensurate increases in market failures and the opportunity costs of maintaining civic and cultural obligations).
    b) Disruption of traditional value chains and business models through convergence.
    c) New forms of network dominance stemming from digital intermediaries' control over the architectures and algorithms of content discovery (and thereby audience traffic and associated revenues).

2. The response to the Christchurch terror attack and the ensuing Christchurch Call summit has opened up a space of policy deliberation wherein proposals to regulate social media and digital intermediaries and hold them accountable to the public interest can be tabled without inviting preemption of such initiatives. Such a response could take the form of wholesale opposition either from vested commercial interests within the tech sector or from governments and state departments sceptical of regulatory intervention in markets.
3. Although the Christchurch Call framework has brought several governments and key industry actors to the table, the domestic regulatory responses to the growing power of social media and digital intermediaries in respective domestic jurisdictions remain vital because:
    a) The probability of substantial, binding, multi-lateral agreements on social media/digital intermediary regulation in the short term is negligible. The prospect of developing such a framework beyond protocols for removing extremist/terrorist content is, at best, uncertain. Delaying domestic interventions on the pretext that the global tech companies can only be meaningfully regulated through a multilateral accord risks further entrenching their incumbent dominance. Future claw-backs to make them accountable to civic interests will be even more difficult.
    b) Many forms of regulatory intervention that might ensue from a multilateral forum will still need to be implemented and enforced on a domestic level. The scope of the possibilities for intervention at a multilateral level are likely to be informed by working examples of existing interventions (as well as associated lobbying from the global tech companies).
    c) It is likely that the threat of various regulatory measures implemented through different state agencies reflecting different policy rationales has compelled the global tech companies to sit down at the bargaining table. They face the prospect of levies on turnover to redress tax avoidance with fines for inadequate monitoring of extremist content and duty of care obligations to protect user privacy. These companies would rather negotiate a consistent framework at a multilateral forum than confront a multitude of regulatory measures which might compromise different parts of their business model in different countries.

A framework for policy deliberations

The scope of this discussion does not extend to specific policy prescriptions, not least because their shape and form needs to be articulated within the institutional arrangements associated with the media ecologies of each jurisdiction. I will, however, outline a heuristic framework for working through the regulatory issues and potential policy responses. To this end, a ‘value chain’ model is set out, identifying different layers of the media sector which represent potential points of intervention. Importantly, this differentiates between the levels of content distribution and content discovery. This is a crucial point where the platforms and algorithms of social media and other digital intermediaries have become dominant (see Figure 1).

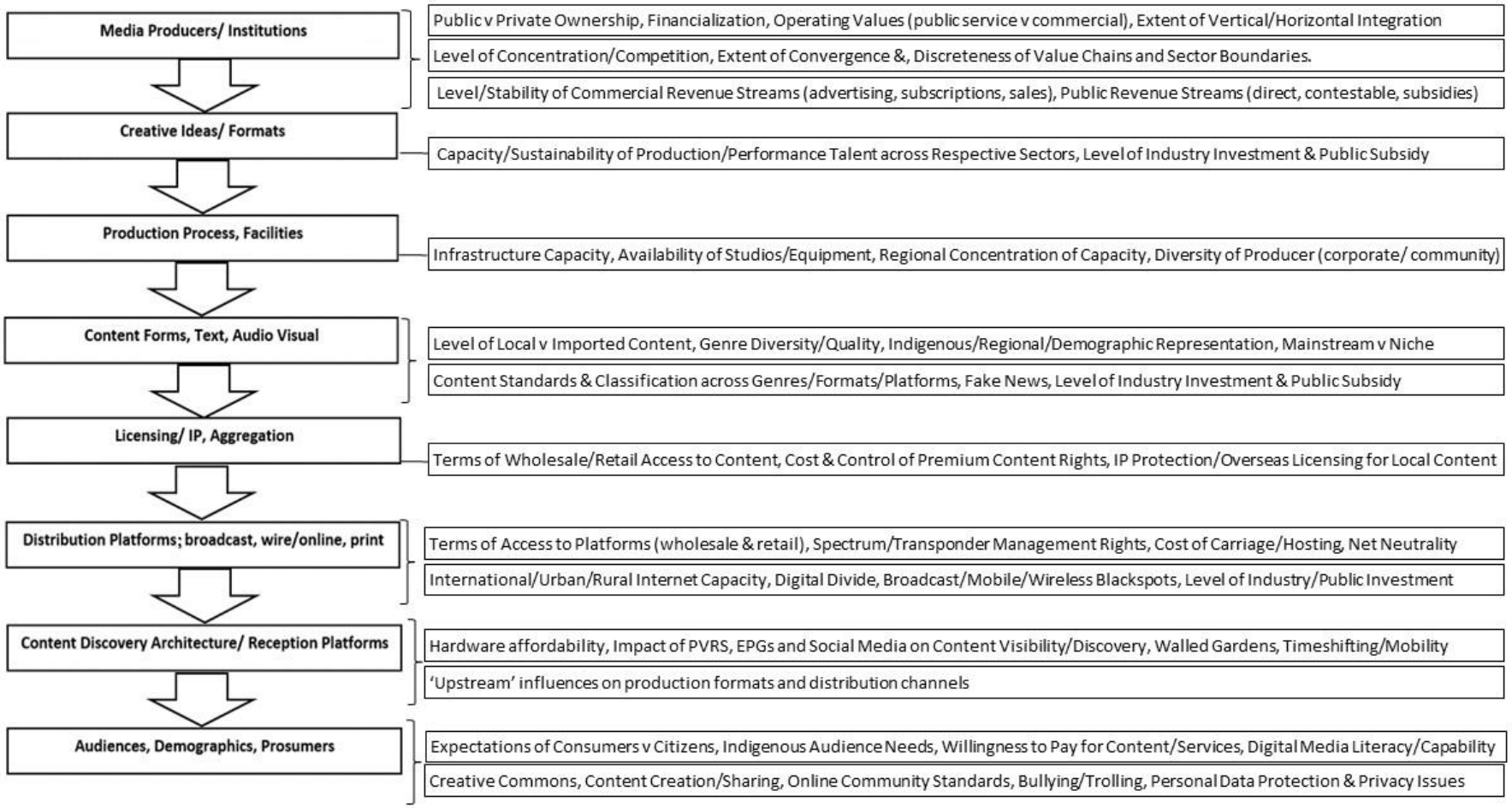

Figure 1. A value-chain model of regulatory intervention points

One important implication of the model here is that 'upstream' levels can affect 'downstream' levels (and in some cases vice-versa). Thus, the shape of ownership and level of market concentration will affect content priorities (such as driving news providers to seek online traffic through 'clickbait'). New forms of content discovery via mobile/online platforms may fragment audiences and influence content formats and distribution channels (e.g., 'digital first' policies).

Concomitantly, regulatory interventions at one level may have implications (whether intentional or inadvertent) for others. For example, imposing copyright restrictions on online content sharing or imposing a levy on online advertising spending would influence the business models of digital intermediaries. Similarly, subsidising the expansion of broadband networks affects consumer take-up of on-demand content streaming services. Obviously, this model does not make predictions about the efficacy of specific policy interventions. That depends on the configuration of the media market and the institutional priorities of the media actors comprising it. However, the model does invite a more holistic approach to identifying regulatory interventions.

Applying the framework to social media after the Christchurch Call

Even if there is a broad consensus that something needs to be done about extremist, terrorist and hate speech online, generic calls to 'regulate Facebook' and other social media are, in themselves, unhelpful. The nature and source of the problems must be correctly identified and regulatory interventions targeted appropriately and proportionately. Four key questions arise here:

1) What exactly is the issue to be resolved and what policy outcome is desired?
2) At what point of the value chain should regulatory intervention be focused?
3) Which agents are responsible for implementing and enforcing regulatory measures?
4) What mechanisms for delivering the policy outcomes are to be employed?

A table outlining some of the policy issues, points of intervention, agents of regulation and potential mechanisms on social media issues is presented in Figure 2. Preliminary discussion is needed to illustrate some of the technical and normative tensions which are liable to arise.

As noted earlier, the Christchurch Call's primary focus is to control the dissemination of terrorist/extremist content through online media and there appears to be a fundamental consensus that regulatory intervention is needed. However, the point at which content could or should be subject to regulation can be debated, especially if the ultimate policy outcome of the Christchurch Call is to reduce terrorist activity itself, not just its livestreaming. A major tension arises here: if law enforcement agencies were permitted access to social media data to pre-emptively identify potential terrorists and extremists, this would inevitably infringe personal privacy and civil liberties (while extremists still inhabited the 'dark web').

Facebook's call for regulatory guidance on its content moderation also reflects the intrinsic complexity of deciding what criteria can be incorporated into algorithms or moderator practices. Facebook's decision to block groups like Britain First is arguably justified on the basis that they actively promoted racial and religious intolerance. However, the United Kingdom government does not currently class Britain First as a banned organisation (even though this is the case for militant far right group National Action). One might therefore contend that unless *all* the views expressed by people affiliated with such groups were intrinsically objectionable, free speech is imperiled when popular sentiment or political correctness drives social media companies to impose wholesale bans

on otherwise legal public organisations. The question arises, who should arbitrate the views that are permitted online?

As noted earlier, the willingness of social media companies to comply with official demands for content removal has often been limited. If self-regulatory measures are insufficient then regulators could require internet service providers (ISPs) to block access to websites designated as objectionable. However, controlling content discovery by restricting internet access is opposed by some civic groups as a step toward controlling the infrastructure and as a threat to open access. Technically speaking, it is not unduly difficult and can target specific URL addresses. The risk is that such measures could become a heavy-handed default in lieu of more nuanced policy measures. Of course, countries with authoritarian media policy frameworks such as China have gone even further by restricting public access to entire platforms such as Facebook and Google. Singapore recently introduced legislation to control disinformation which gives the government the power to order the blocking or retraction of content that it deems to be fake news. In effect, therefore, Singaporean government agencies determine what is or isn't true (see Fullerton, 2019).

Another complexity in policing extremist content is that it is easier to respond retro-actively than pre-emptively. The measures needed to pre-emptively stop the livestreaming of actions such as the Christchurch attacks could impinge on other democratic freedoms. For instance, the pre-vetting and registration of all livestream users would not necessarily exclude a heretofore unknown terrorist, but could be used to stop known democracy activists from livestreaming a protest. One could improve regulatory oversight of the algorithms used by social media and online intermediaries to harvest user data and prioritise content in social media feeds or search engines. This would, however, require an unprecedented level of transparency from a sector reluctant to allow outside scrutiny. Analysing the code to identify those factors liable to trigger recommendations of extremist content is not simple, but it might ensure that such material was not easily discovered by users. The possibility of governments deciding what kind of content should be deprioritized could raise democratic concerns. Moreover, a wholesale restriction on algorithms designed to magnify the visibility and discoverability of 'trending content' would affect the business models of digital intermediaries.

Calls for the regulation of social media and digital intermediaries often assume that they are more than just platform providers but content aggregators, curators, distributors and/or publishers. The implied dichotomy between media companies which produce and publish content and those which provide the 'pipes' for the common carriage of other's content is often unhelpful for the understanding of digital media ecology. However, the primary operations of search engines and social media and other digital intermediary services do not entail provision of either the distribution infrastructure or the content forms themselves. Rather, they provide the intermediary architecture and navigation platforms which enable third parties to share and discover content (in order that they can monetise the online traffic thereby generated). This is also why the core operations of social media and search engines tend to fall between the traditional regulatory provisions for telecommunications and broadcasting. Further, this suggests that the prevailing regulatory frameworks need more than cosmetic reform to address concerns related to the practices of social media and digital intermediaries.

Table 1 presents a breakdown of several regulatory issues arising from concerns about social media and digital intermediaries. Potential responses are categorized in terms of the point of intervention on the value-chain, possible agents of intervention and the potential mechanism for addressing the issue. The identification of certain regulatory agents and mechanisms is intended to

offer a framework for considering a broader potential regulatory response, *not* to endorse any option as desirable or feasible.

Table 1. Value chain model applied to social media and digital intermediaries in the Christchurch Call context

Regulatory issues	Potential points of intervention	Possible agents of intervention	Potential mechanisms/modes of intervention
Proliferation of harmful extremist content including online hate-speech and live-streaming of terrorist acts (e.g. Christchurch mosque attacks)	• Content production • Content form • Distribution platforms • Content discovery & algorithms • Audience reception	• Police/law enforcement (domestic or multilateral) • Content standards regulators • Advertisers • Internet Service Providers • Digital Intermediaries (social media, search engines) • Algorithms • Audience	• Prosecution of terrorist/extremist groups • Increased policing of 'dark web' • Pre-vetting, classification & restriction of content pre-distribution to resrict objectionable material • Pre-vetting for live-streaming access • Development of codes of online practice for digital intermediaries • Content standards codes vetted post-distribution in response to complaints and/or via algorithms • Content providers self-police content or regulators issue take-down notices • ISP website blocking • Advertiser boycotts of non-compliant social media (or possible restrictions on advertising) • Algorithmic oversight & accountability • Audience media literacy & self-monitoring, also complaints to regulators and authorities, consumer boycotts
Algorithms underpinning search engines and social media news-feeds promote extremist echo chambers & filter-bubbles), undermining rational dialogue/ community solidarity.	• Distribution platforms • Content discovery/algorithms • Audience reception	• Digital intermediaries • Independent regulators • Government • Audience	• Increased self-monitoring of algorithms by social media and search engines • Independent regulator access to and vetting/ oversight of algorithms/code (e.g. requiring prioritisation of independent public interest media in news-feeds and web searches) • Government support for public interest media inlcuding public service broadcasters and independent journalism • Audience media literacy
Collation and (a)buses of personal data/ breaches of privacy either by social media or third parties to whom data is made available (e.g. Facebook traded user data to Amazon in return for advertising business)	• Content licensing/IP • Content discovery/reception • Algorithms • Audience reception	• Police/law enforcement • Independent regulators • Internet Service Providers • Digital Intermediaries (social media, search engines) plus associated 'App' providers • Audience	• Legislation to protect privacy of audience personal data as inalienable intellectual property. • Require active consent for data sharing with third parties and rights to revoke consent and delete stored data. • Imposition of information fiduciary duty of care on social media companies' use of personal data • Permit law enforcement agencies to access personal data in order to anticipate extremist/terrorist activity • Enhanced audience rights to block undesired advertising • Audience media literacy, consumer boycotts

Regulatory issues	Potential points of intervention	Possible agents of intervention	Potential mechanisms/modes of intervention
Co-option of social media (and/or search engines) and user data by political agencies for targeted dissemination of propaganda and/or fake news (e.g. Cambridge Analytica)	• Distribution platforms • Content discovery • Audience reception	• Police/law enforcement • Independent regulators • Digital Intermediaries (social media, search engines) • Internet Service Providers • Audience	• Legislation to criminalise concerted efforts to manipulate elections through abuse of social media • Expanded fact-checking and fake news detection/removal systems by social media and/or regulators • Blocking of identified fake news proliferators from social media and other online platforms • Audience media literacy
Impact of digital intermediaries on traditional media (e.g. newspapers) by dominating advertising revenue from online traffic through facilitating discovery of third party content (e.g. it is estimated that Google and Facebook account for 70% of online advertising)	• Content licensing/IP • Distribution platforms • Content discovery/reception • Audience reception	• Government • Independent regulator • Content producers • Digital Intermediaries • Advertisers	• Regulation obliging social media and search engines which facilitate third party audience discovery to contribute to the cost of producing the content thereby discovered/shared. • Impose a marginal levy on domestic advertising spend directed toward domestic audiences at point of transaction, with the revenue redirected to content providers. • Subject existing relationships between digital intermediaries, content providers and audiences to market competition/ market power rules.
Concentration, Network effects & monopolisation of the means of online content discovery (e.g. it is estimated that Google and Facebook account for 80% of online referrals)	• Media institutions • Content discovery/reception • Distribution platforms	• Government (multi-lateral/ domestic) • Independent regulator	• Redesignate digital intermediaries as public utilities with civic obligations beyond private shareholders. • Subject existing relationships between digital intermediaries, content providers and advertisers to market competition/ market power rules. • Require formal break-up or partial nationalisation of digital intermediaries which exert disproportionate market power or fail to operate in the public interest. • Government support for public interest media inlcuding public service broadcasters and independent journalism
Concentration, Network effects & monopolisation of the platforms for e-commerce.	• Media institutions • Distribution Platforms	• Government (multi-lateral/ domestic) • Independent regulator	• Redesignate online-e-commerce providers as public utilities with civic obligations beyond private shareholders. • Subject e-commerce platform providers to market competition/ market power rules. • Require formal break-up or partial nationalisation of e-commerce providers which exert disproportionate market power or fail to operate in the public interest.

Concluding points

The Christchurch Call pledge represents a very initial step toward the formation of a multilateral regulatory framework for controlling online terrorist and extremsit content, along with other practices of social media and online intermediary operators. It would be premature to declare the initiative either a success or a failure at this stage, but it needs to be understood in the context of a broader policy trajectory which has been unfolding over the past decade. Many of the regulatory initiatives being implemented were either in the policy pipeline or under deliberation well before the Christchurch terror attacks and the ensuing Paris summit. It would, therefore, be wrong to characterise these measures as being driven by the shock of these events (although the Australian Unlawful Showing of Abhorrent Violent Material legislation may be the exception).

The Christchurch Call proposal itself is significant insofar as it brought a range of state and industry actors together and managed to find sufficient common ground for developing a multilateral, mutli-stakeholder agreement on future principles and responsibilities. As such, it provides a basis for progressing deliberations on regulatory measures for social media and digital intermediaries in the future. It is important to bear in mind that the Christchurch Call pledge document is not sufficiently specific to be enforceable, even if it were enacted into some form of legally-binding treaty. It also makes only cursory reference to broader questions of human rights and civic accountability, the regulatory import of which extends well beyond the immediate question of curtailing online extremism. What the Christchurch Call does do though is legitimate future regulatory interventions in the digital media sector. They can no longer be casually dismissed by vested interests or ideological opponents of state intervention in markets.

A consistent, international multilateral framework of regulation must be the ultimate goal of the Christchurch Call, but the corporate interests must not be be allowed to circumscribe its scope. The parallel domestic regulatory initiatives stemming simultaneously from different government departments in different jurisdiction may be somewhat disparate, but deferring domestic level regulation in the hope of an imminent multilateral regulatory framework would be both politically naïve and risky. Indeed, the groundswell of support for statutory regulation of social media and digital intermediaries in different jurisdictions has probably helped to bring the global tach companies around the bargaining table.

Meanwhile, one must be cautious of the new-found willingness of social media corporations and digital intermediaries to engage with governments and regulators after years of evading and denying responsibility or liability. Indeed, the strategic interests of these corporations may actually be served by a loose, fragmented international framework in which they remain the primary regulatory agents of intervention. Such an outcome is likely if social media corporates are able to obstruct or narrow the call for clearer legal guidelines on industry self-moderation of extremist content. We should beware of geeks bearing gifts.

Author bio

Peter Thompson is a senior lecturer in the Media Studies programme at Victoria University of Wellington. In addition to co-editing the Political Economy of Communication journal, he is co-vice-chair of the Political Economy section of the International Association for Media and Communication Researchers (IAMCR). He has published extensively on media policy in Aotearoa-New Zealand and is chair of the Better Public Media trust.

Endnotes

[1] It is worth noting that the Ogassagou and Welingara massacre of 160 Futani herders in Mali, just one week after the Christchurch attack, received very little western media attention. Although the Easter bombings in Sri Lanka the following April which claimed 259 lives did gain considerable coverage, its profile as a news story reflected the fact that tourist hotels were a primary target.

[2] The notion of 'information fiduciaries' suggests an obligation like a financial or legal professional's duty of care to protect personal data and use it only to serve the interests of the client- see Balkin and Zittrain (2016)

References

ACCC (2019) Digital Platforms Inquiry: Final report. Available at: https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf (accessed July 27 2019).

Annany M and Gillespie T (2017) Public platforms: Beyond the cycle of shocks and exceptions. Paper presented to *the 67th Annual Conference of the International Communications Association, Interventions: Communication Research and Practice*. San Diego, 25–29 May. Available at: http://blogs.oii.ox.ac.uk/ipp-conference/sites/ipp/files/documents/anannyGillespie-publicPlatforms-oii-submittedSept8.pdf (accessed 24 June 2019).

Attorney General for Australia (2019) Tough new laws to protect Australians from live-streaming of violent crimes. *Government press release*, 4 April. Available at: https://www.attorneygeneral.gov.au/Media/Pages/Tough-New-Laws-to-protect-Australians-from-Live-Streaming-of-Violent-Crimes.aspx (accessed 27 June 2019).

Balkin JM and Zittrain J (2016) A grand bargain to make tech companies trustworthy. *The Atlantic*, 3 October. Available at: https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ (accessed 23 June 2019).

BBC (2019a) France tech tax: What's being done to make internet giants pay more? *BBC Business*, 11 July. Available at: https://www.bbc.com/news/business-48928782 (accessed 13 July 2019).

BBC (2019b) France passes tax on tech giants despite US threats. *BBC World News*, 11 July. Available at: https://www.bbc.com/news/world-europe-48947922 (accessed 13 July 2019).

Bogle A (2019) Laws targeting terror videos on Facebook and YouTube 'rushed' and 'knee-jerk', lawyers and tech industry say. *ABC News*, 4 April. Available at: https://www.abc.net.au/news/science/2019-04-04/facebook-youtube-social-media-laws-rushed-and-flawed-critics-say/10965812 (accessed 24 June 2019).

Cadwalladr C (2017) The great British Brexit robbery: how our democracy was hijacked. *The Guardian*, 7 May. Available at: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy (accessed 25 June 2019).

Carter, J. and Komaitis, K. (2019) How to regulate the internet without shackling its creativity. *Stuff*, May 15. Available at: https://www.stuff.co.nz/national/christchurch-shooting/112704241/how-to-regulate-the-internet-without-shackling-its-creativity (accessed 20 June 2019).

Chang D (2019) Social media crackdown: How New Zealand is leading the global charge. *NZ Herald*, 27 April. Available at: https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1andobjectid=12224140 (accessed 13 June 2019).

Channel 4 (2018) Dispatches investigation reveals how Facebook moderates content. *C4 News*, 17 July. Available at: https://www.channel4.com/press/news/dispatches-investigation-reveals-how-facebook-moderates-content (accessed 16 June 2019).

Corbin K (2019) Warren wants to break up Amazon, Facebook, Google. *Forbes*, 8 March. Available at: https://www.forbes.com/sites/kennethcorbin/2019/03/08/warren-wants-to-break-up-amazon-facebook-google/#30492fe16a6a (accessed 24 June 2019).

Cox J (2018) These are Facebook's policies for moderating white supremacy and hate. *Vice Motherboard*, 30 May. Available at: https://www.vice.com/en_us/article/mbk7ky/leaked-facebook-neo-nazi-policies-white-supremacy-nationalism-separatism (accessed 20 June 2019).

Cox J (2019) Twitter and YouTube won't commit to can white nationalism after Facebook makes policy switch. *Vice Motherboard*, 3 April. Available at: https://www.vice.com/en_us/article/mbzz8x/twitter-youtube-wont-ban-white-nationalism-facebook (accessed 20 June 2019).

Cox J and Koebler J (2019a) Why won't Twitter treat white supremacy like Isis? Because it would mean banning some republican politicians too. *Vice Motherboard*, 26 April. Available at: 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 (accessed 20 June 2019).

Cox J and Koebler J (2019b) Facebook bans white nationalism and white separatism. *Vice Motherboard*, 28 March. Available at: https://www.vice.com/en_us/article/nexpbx/facebook-bans-white-nationalism-and-white-separatism (accessed 20 June 2019).

Department for Digital, Culture, Media and Sport/Home Office (2019) UK to introduce world first online safety laws. *Government press release*, 8 April. Available at: https://www.gov.uk/government/news/uk-to-introduce-world-first-online-safety-laws (accessed 22 June 2019).

Department of Internal Affairs/Te Tari Taiwhenua (2019a) The department's response to the Christchurch terrorism attack video – Background information and FAQs, March. Available at: https://www.dia.govt.nz/Response-to-the-Christchurch-terrorism-attack-video (accessed 18 June 2019).

Department of Internal Affairs/Te Tari Taiwhenua (2019b) *The Royal Commission of Inquiry into the Attack on Christchurch Mosques.* April. Available at: https://christchurchattack.royalcommission.nz/about-the-inquiry/ (accessed 14 June 2019).

Elliott M, Berentson-Shaw J, Kuehn K and Salter L (2019) Digital threats to democracy. *The Workshop*, May. Available at: https://static1.squarespace.com/static/5cbe92fcaf4683f10f6c8de5/t/5cd241278d34250001741b01/1557283123703/DD-single-report-combined-WEB.pdf (accessed 19 June 2019).

European Commission (2016) The EU Code of Conduct on Countering Illegal Hate Speech Online. Available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/countering-illegal-hate-speech-online_en (accessed 23 June 2019).

Flew T (2019) Australian media regulators face the challenge of dealing with global platforms Google and Facebook. *The Conversation*, 6 August. Available at: https://theconversation.com/australian-media-

regulators-face-the-challenge-of-dealing-with-global-platforms-google-and-facebook-121430?fbclid=IwAR0M6szNbq7bzfWDpmDCzMTzxzydNgv4PT0vzc812sJgt9ktP9VbDXFhG0E (accessed 6 Auhust 2019).

Flew T, Martin F and Suzor N (2019) Internet regulation as media policy: Rethinking the question of digital communication platform governance. *Journal of Digital Media and Policy* 10(1): 33-50. Available at: https://www.ingentaconnect.com/contentone/intellect/jdmp/2019/00000010/00000001/art00005# (accessed 2 April 2019).

France 24 (2019) *French report calls for more access to Facebook algorithms as Macron meets Zuckerberg*. 5 May. Available at: https://www.france24.com/en/20190510-france-facebook-law-mark-zuckerberg-president-macron-internet-regulation-internet (accessed 22 June 2019).

Fullerton J (2019) Singapore to introduce anti-fake news law, allowing removal of articles. *The Guardian*, 1 April. Available at: https://www.theguardian.com/world/2019/apr/01/singapore-to-introduce-anti-fake-news-law-allowing-removal-of-articles (accessed 21 June 2019).

House of Commons/ Home Affairs Committee (2017) Hate crime: Abuse, hate and extremism Online. *Fourteenth Report of Session 2016–17.* Available at: https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/609.pdf (accessed 23 June 2019).

InternetNZ (2019) Civil society positions on Christchurch Call pledge. 14 May. Available at: https://docs.google.com/document/d/10RadyVQUNu1H5D7x6IJVKbqmaeDeXre0Mk-FFNkIVxs/edit (accessed 19 July 2019).

Isaac M (2019) Mark Zuckerberg's call to regulate Facebook, explained. *New York Times Technology*, 30 March. Available at: https://www.nytimes.com/2019/03/30/technology/mark-zuckerberg-facebook-regulation-explained.html (accessed 2 July 2019).

Keall, C (2019) As Jacinda Ardern prepares social media crackdown, alleged gunman's video reappears - and gets huge traffic. *NZ Herald*, 23 April. Available at: https://www.nzherald.co.nz/business/news/article.cfm?c_id=3andobjectid=12224469 (accessed 14 June 2019).

Kelly M (2019a) France wants to fine Facebook over hate speech. *The Verge*, 4 July. Available at: https://www.theverge.com/2019/7/4/20682513/french-parliament-facebook-google-social-network-hate-speech-removal (accessed 22 July 2019).

Kelly M (2019b) FTC hits Facebook with $5 billion fine and new privacy checks. *The Verge*, 24 July. Available at: https://www.theverge.com/2019/7/24/20707013/ftc-facebook-settlement-data-cambridge-analytica-penalty-privacy-punishment-5-billion (accessed 26 July 2019).

Kinstler L.(2018) Germany's attempt to fix Facebook is backfiring. *The Atlantic*, 19 May. Available at: https://www.theatlantic.com/international/archive/2018/05/germany-facebook-afd/560435/ (accessed 24 June 2019).

Mason C and Errington K (2019) Anti-social media: Reducing the spread of harmful content on social media networks. *Helen Clark Foundation Report*. Available at: https://www.helenclark.foundation/wp-content/uploads/2019/05/thcf-social-media-report-min.pdf (accessed 18 June 2019).

McMaken R (2019) 3 Reasons Why Facebook's Zuckerberg wants more government regulation. *Mises Institute Wire*, 1 April. Available at: https://mises.org/wire/3-reasons-why-facebooks-zuckerberg-wants-more-government-regulation (accessed 2 July 2019).

Ministry for Culture and Heritage (2008) *Digital Broadcasting: Review of Regulation, Vols. 1-2*. Available at: https://mch.govt.nz/research-publications/our-research-reports/digital-broadcasting-review-regulation-january-2008 (accessed 13 June 2019).

Ministry for Culture and Heritage/ Ministry of Business, Innovation and Employment (2015) *Exploring Digital Convergence: Issues for Policy and Legislation.* Available at: https://mch.govt.nz/sites/default/files/Exploring%20Digital%20Convergence%20Issues%20for%20Policy%20and%20Legislation%20(D-0740630).PDF#overlay-context=exploring-digital-convergence (accessed 22 June 2019).

Ministry of Justice (2017) *Harmful Digital Communications.* Available at: https://www.justice.govt.nz/justice-sector-policy/key-initiatives/harmful-digital-communications/ (accessed 19 June 2019).

Napoli PM and Caplan R (2017) Why media companies insist they're not media companies, why they're wrong, and why it matters. *First Monday* 22(5), May. Available at: https://journals.uic.edu/ojs/index.php/fm/article/view/7051/6124 (accessed 3 July 2018).

Office of the Secretary of State for Digital Affairs (2019) Creating a French framework to make social media platforms more accountable: Acting in France with a European vision. *Interim Mission Report,* May (English version). Available at: http://thecre.com/RegSM/wp-content/uploads/2019/05/French-Framework-for-Social-Media-Platforms.pdf (accessed 25 June 2019).

RNZ (2019a) 4000 people watched Facebook video before anyone reported it. *RNZ News,* 19 March. Available at: https://www.rnz.co.nz/news/national/385127/4000-people-watched-facebook-video-before-anyone-reported-it (accessed 19 June 2019).

RNZ (2019b) Christchurch terror attacks: Videos still on social media – expert. *RNZ News*, 24 April. Available at: https://www.rnz.co.nz/news/national/387656/christchurch-terror-attacks-videos-still-on-social-media-expert (accessed 20 June 2019).

Small Z (2019) 'Global alliance': Jacinda Ardern joins world leaders calling for tech giant accountability. *Newshub*, 20 March. Available at: https://www.newshub.co.nz/home/politics/2019/03/global-alliance-jacinda-ardern-joins-world-leaders-calling-for-tech-giant-accountability.html (accessed 19 June 2019).

The Christchurch Call (2019) *The Christchurch Call to Action To Eliminate Terrorist and Violent Extremist Content Online*. Available at: https://www.christchurchcall.com/christchurch-call.pdf (accessed 1 July 2019).

The Guardian (2019) France online hate speech law to force social media sites to act quickly. *Guardian World News via AFP*, 9 July. Available at: https://www.theguardian.com/world/2019/jul/09/france-online-hate-speech-law-social-media (accessed 20 July 2019).

Thompson PA (2019) The return of public media policy in New Zealand: New hope or lost cause? *Journal of Digital Media and Policy* 10(1): 89-107. Available at: https://www.ingentaconnect.com/contentone/intellect/jdmp/2019/00000010/00000001/art00008;jsessionid=1ojcjkfsz6w4e.x-ic-live-01 (accessed 10 June 2019).

Waterson J (2019) Facebook removed 1.5m videos of New Zealand terror attack in first 24 hours. *The Guardian*, 17 March. Available at: https://www.theguardian.com/world/2019/mar/17/facebook-removed-15m-videos-new-zealand-terror-attack (accessed 4 June 2019).

Williams D (2019) Terror on TV news: Lessons from Australia. Newsroom, 1 August. Available at:: https://www.newsroom.co.nz/2019/08/01/710147/terror-on-tv-news-lessons-from-australia# (accessed 23 June 2019).

White House (2019) Statement on Christchurch Call for action. Office of Science and Technology Policy. Press release from US Embassy in New Zealand, 15 May. Available at: https://nz.usembassy.gov/statement-on-christchurch-call-for-action/ (accessed 15 July 2019).

Winseck DR (2015) Intermediary responsibility. In: Mansell R and Ang PH (eds) *International Encyclopedia of Digital Communication and Society, Vol.1*. Boston: Wiley-Blackwell. pp 488–502.

Winseck DR (2019) Ready, fire, aim: Why digital platforms are not media companies and what to do about them. Presentation to the *2019 IAMCR Conference, Communication, Technology and Human Dignity: Disputed Rights, Contested Truths*, 7-11 July, Madrid.

Taylor J and Wong JC (2019) Cloudflare cuts off far-right message board 8chan after El Paso shooting. *The Guardian*, 5 August. Available at: https://www.theguardian.com/us-news/2019/aug/05/cloudflare-8chan-matthew-prince-terminate-service-cuts-off-far-right-message-board-el-paso-shooting?fbclid=IwAR0tC_ibLpFZSKd_1tPnC4h-_fPyMiQAiFCvQ80sRU9-MKiS4lP4w9dtdDk (accessed 5 August 2019).

Zuckerberg M (2019a) A privacy-focused vision for social networking. *Facebook Comment*, 6 March. Available at:: https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/ (accessed 20 July 2019).

Zuckerberg M (2019b) The internet needs new rules - let's start in these four areas. *Washington Post*, March 30. Available at: https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.4d379f685de9 (accessed July 2 2019).