3

Becoming civic actors

Sally Wheeler

Here the Christchurch Call to Action is set in two contexts: the history of the livestreaming of violent events and the argument of technology companies that they are mere relayers of user-generated content. The second of these contexts is parlayed into an argument that technology companies should be seen as having the same responsibilities to the societies they operate in as all other large corporate actors. Despite being expressed at the international level with states as its audience, the response to the Christchurch Call will be, by structural necessity, at the domestic level. The call opens up an opportunity for technology companies to design and embed digital ethics in the societies in which they operate. This chapter closes by examining how this might be achieved.

Live footage of violence

The immediate background to the Christchurch Call of May 2019 was the livestreaming of a mass-shooting event that ended in considerable loss of life. It is worth remembering that the transmission of live footage of events of violence is not a particularly new phenomenon. It is something to which we have been exposed for a number of years and to some extent desensitised. Those of us in our mid-50s and older may well remember the fatal terrorist attack on the Israeli team at the Munich Olympics in early September 1972 that played out on television screens in real time across the northern hemisphere, and the killing of two British Army corporals
at a funeral in Northern Ireland, coverage of which interrupted the BBC’s Saturday afternoon sports program in March 1988 (Engle, 2018). The distinguishing feature of more recent events is that the second generation of the internet – Web 2.0 – enables user-generated content to be uploaded for global viewing. Livestreaming of terror-related events by unconnected bystanders has become depressingly familiar in recent years. The Brussels Airport and Metro attacks in March 2016 were uploaded live with commentary supplied by social media users in the vicinity. A gun battle between police and a sniper who had already shot five police officers that day in Dallas in July 2016 was relayed live on Facebook. The absence of a newscaster and the presence of a bystander as the link to the event makes it seem psychologically closer, even more so when the perpetrator controls the livestreaming.

In March 2019 the perpetrator of the Christchurch terrorist attack livestreamed his own actions across the world using a Facebook account. Facebook removed the footage of the attack as soon as it was alerted to its presence by the police; however, this was after the attack had ended, meaning that Facebook’s content-moderation software had not detected it. Before Facebook’s removal of the video, some 4,000 people had viewed it. Subsequently 300,000 versions of it were successfully uploaded and then removed by moderators and a further 1.2 million upload attempts were intercepted by Facebook software and blocked (Whittaker, 2019). While this shielding limited many Facebook users from viewing the event, it was still available on websites such as 4chan and 8chan (now 8kun) until mainstream ISP providers in Australia and Aotearoa New Zealand such as Telstra and Vodafone blocked it (Brennan, 2019; Brodkin, 2019). The Christchurch attack was a racially motivated, white supremacist attack. It has been followed by similarly motivated and executed attacks (each involving the posting of a racist manifesto to an internet forum followed by livestreaming the actual attack) in Poway in the US in April 2019 and in Halle in Germany in October 2019. We might conclude that whatever protocols were put in place regarding the takedown of material following Christchurch have yet to become successful.
Media corporations or technology corporations – does it matter?

The availability of this user-generated content is used to support the argument of social media platforms such as Twitter and Facebook, and digital media corporations such as Google and Apple, that they are not ‘media’ corporations in the sense that print and broadcast service providers are, but, rather, are technology corporations (Barns, 2020, pp. 35–52) and online service providers (OSPs). They do not produce original content but instead distribute the content made by others, whether those others are, inter alia, individual users, political parties or large corporations. The line between content creation and content distribution is not perhaps as clear as is being suggested; satellite broadcasters such as Sky in many of their operations might be seen as primarily distributors of content produced by others rather than content producers. Like mainstream print and broadcast media, advertising revenue is of huge strategic importance to the business model that OSPs are employing and this shared dependence brings the two much closer together.

This assertion that social media sites and ISPs are technology corporations is broadly supported by US legislation: the Telecommunications Act 1996 s. 230 protects them from liability for the speech of third parties that they host or distribute, as do Articles 12–14 of the foundational legal framework for online services in the EU, the Electronic Commerce Directive 2000. The European Court of Justice has confirmed in a recent decision (Judgment of the Court, 2021) that this directive does indeed set up a safe harbour by creating protection from liability as long as ‘neutrality’ is maintained; that is to say that conduct by the social media site or ISP is ‘merely technical, automatic and passive’ (Judgment of the Court, 2010). Once there is actual knowledge of illegal activity that might come from police or other users in relation to violent conduct or from rightsholders in relation to intellectual property rights infringement, then there needs to be a move towards blocking or removing the content in question.

This distinction is also implicitly recognised by the recent digital platforms inquiry in Australia, the Competition and Consumer Commission Digital Platforms Inquiry (ACCC, 2019). There it was proposed that certain specified ‘digital platforms’ were to implement a voluntary code facilitated by the Australian media regulator, the Australian Communications and Media Authority, to govern their relationships with ‘media businesses’.
This voluntary code has recently become the subject of an intense disagreement between the Australian Government and Facebook in particular. Being classified as technology rather than media corporations also means that regulatory obligations in relation to content that are imposed on media providers in a variety of nation-state settings such as the requirement, for example, to follow particular guidelines in relation to religious affairs broadcasting (UK), giving adequate time to educational material (US) and ensuring that impartial news content rules (UK) do not apply to them (Napoli and Caplan, 2017).

Of course, pressuring for consideration or classification by the state and commentators as technology corporations rather than media corporations does not mean that there is no legislative or regulatory purview of technology corporations with resulting restrictions or compliance obligations; it simply means that these will not be the same as those applied to media corporations (Moe, 2008) and that there is a lobbying opportunity for technology corporations to shape their regulatory environment. There is an expectation from what might broadly be termed civil society that all corporations, whatever their industry classification, undertake voluntary, socially oriented activities that go beyond the obvious enhancement of corporate profits (Carroll, 2016) under the label of corporate social responsibility (CSR). Additionally, civil society expects that corporations will behave ethically and responsibly towards their stakeholders, notwithstanding the rather nebulous definition that the term ‘stakeholder’ enjoys, even if that means corporations going beyond what is required in a strict regulatory sense (Gunningham et al., 2004). This captures the idea of corporations holding a ‘social license to operate’. The difference between CSR and the social license is that corporations choose their CSR interventions but fulfilling their social license requires meeting societal expectations and so involves dialogue with stakeholders around the corporate response to regulation and the corporate decision-making process (Moffat et al., 2016). There is an argument that corporate commitment to demonstrable CSR activities and the maintenance of social license increases inexorably for individual corporations in a position of dominance or where they are so central to the lives of citizens that they might be seen as public utility corporations or essential service providers (Andrejevic, 2013). This increased commitment might be viewed as akin to one of civic responsibility.
The idea that technology corporations occupy a position of dominance and/or operate an essential service, in terms of both their infrastructure and activities, is often adopted by those who advocate that antitrust or competition legislation should be applied to them (Wu, 2018). Indeed, this linkage between monopoly or dominant market power, civic or public responsibility, and competition or antitrust regulation is exactly the position taken by two recent state level inquiries (Flew and Wilding, 2021): the Cairncross Review in the UK (Cairncross, 2019) and the aforementioned Australian Inquiry (ACCC, 2019). The idea of using existing regulatory structures or designing new anti-competitive structures (Lawrence and Laybourn-Langton, 2018) to deal with the perceived monopoly position of technology corporations is one that is well rehearsed from within the disciplines of, inter alia, media studies and law (Thierer, 2013; Ghosh, 2019). There is an assumption made that technology corporations once subjected to antitrust regulation will automatically become civic actors operating in the public interest. However, little consideration is given to what these civic responsibilities might be in the context of technology companies and how they might be arrived at.

The ‘ask’ of the Christchurch Call

By asserting their identity as technology corporations, reinforced by descriptions of themselves as ‘platforms’ with stated missions to deliver ‘sharing, community and empowerment’ (Etlinger, 2019, p. 24), ISPs and social media corporations are ultimately seeking to escape from the idea that they can (or should) exercise editorial control over the content that they host (Gillespie, 2010). The Christchurch Call, at its heart, is a demand that this is exactly what they should do in an open and transparent manner by developing both content screening methodologies and the appropriate technical expertise supported by governments and civil society to filter out material that is supportive of, and advocates for, terrorism and violent extremism. In its three pages of text, the call sets out the paradoxes that surround the internet as a forum for communication. The call is at one and the same time an appeal to protect ‘collective security’ and recognise the potential impact that the unchecked availability of violent content might have on that, and an assertion that it is possible to do this while respecting and supporting free speech and the role that the internet plays in creating an inclusive and connected society. As a general goal, this is much more difficult to achieve than the call acknowledges.
The events of Christchurch itself apart, the call comes at a difficult juncture for technology companies. Some of those difficulties around the occupation of monopoly positions and liability for distributed content have already been alluded to, but they are really symptomatic of a bigger issue that confronts OSPs: the role of the internet in political life, more generally at the nation-state level, that OSPs facilitate. The internet has gone from being seen as an open public space, an ideal that OSPs have carefully curated through their portrayal of themselves as social libertarians, playing a crucial part in the organisation of protests against authoritarianism and the advance of democracy (Google executive, Wael Ghonim’s comment that ‘if you want to liberate a society, just give them the internet’ comes to mind [Hofheinz, 2011]) to one in which political manipulation through the platforming of fake news in the form of disinformation and the silencing of voices in anti-democratic manner through ‘takedown’ activities are said to occur (Hoverd et. al, 2021). The longstanding view of OSPs as mere ‘relayers’ of content has begun to break down, particularly in the EU and in its member states where values such as privacy and respect are seen as at least the equal of the US First Amendment idol of free speech, and are often protected by the criminal law of member states.

The cultural battle around ‘cancel culture’ is a useful illustration of the general dilemma that OSPs and wider society face. Social media allows a protest movement around a particular institutional activity or person to grow in strength organically thus allowing the resulting collective view to exert, often successfully, pressure for the cancellation of an activity or personal appearance. In this instance the voiceless have been given voice but at the expense of the expression of a perfectly legal view or the conduct of a legitimate activity. In more specific terms, having been lauded as the organising forum for the Arab Spring a decade ago (Clarke and Kocak, 2020), OSPs, particularly Facebook, are now under pressure around a number of alleged misconduct issues: misuse of personal data via Cambridge Analytica during the 2016 US Presidential Election; the manipulation of platform algorithms (aka filter bubbles and echo chambers), to allow the targeting of particular categories of British voters during the Brexit referendum in breach of UK electoral law; and the failure to prevent, through content removal and individual suspensions of users, the organisation of acts of violence by Myanmar military officials against the minority Rohingya people.
This last infraction was compounded by Facebook's subsequent refusal to cooperate in a document production request to support The Gambia's action for genocide against Myanmar in relation to the Rohingya before the International Court of Justice (2020). The Oxford Internet Institute reported that there is evidence of organised campaigns of social media manipulation in 70 countries in 2019; this figure has increased steadily from the institute's first report in 2017 (Bradshaw and Howard, 2019). There is no suggestion that OSPs endorse this manipulation but it does indicate that their ‘takedown’ policies (or absence thereof) allow it to happen. Both Facebook and Twitter, as platforms, seem to give more latitude to elected officials, or authority figures at least, than to other individuals in terms of when they apply takedown policies (York, 2021). Presumably, their thinking is that those who have been elected have had their perspectives democratically endorsed and that their speech is per se newsworthy (Kang and Isaac, 2019). Given that the utterances and actions of politicians and elected officials will garner more interest within the community, it is to be hoped they are not inciting violence or projecting hate speech. Recent events in the US and parts of Europe would call this assumption into question as we see the rise of violent white nationalism and populist authoritarian political regimes, both of which are thought to be potential triggers for the occurrence of online violent and extremist content (Kaakinen et al., 2018). Even the ‘elected official’ position can break down; Hezbollah, for example, holds seats in the Lebanese Parliament but is banned on Facebook because in the US, Hezbollah is a designated foreign terror organisation under the Immigration and Nationality Act 1965, s. 219.

The Christchurch Call features several joint undertakings from governments and OSPs to end or at least control the presentation of terrorist-supported content online. There have been other attempts to do this through, for example, the UN Security Council Resolutions (UNHRC, 2018), the EU-supported Internet Forum and technology company-generated initiatives such as Tech Against Terrorism and the Global Internet Forum to Counter Terrorism, but they have concentrated on position-taking, sector by sector, and underwriting their

---

1 See European Internet Forum, www.internetforum.eu/
2 See Tech Against Terrorism, www.techagainstterrorism.org/about/; Global Internet Forum to Counter Terrorism, gifct.org/. As a result of the Christchurch Call, the GIFCT announced in September 2019 that it would become an NGO, rather than an industry-based body, and would offer a platform for multi-stakeholder engagement.
efforts on what is not necessarily a cooperatively negotiated starting point. What differentiates the Christchurch Call from these previous efforts is the level within both governments and technology companies at which there is engagement, the idea of a partnership approach between not just state and corporate interests but also civil society actors and the clear definition given to its goals (Heldt, 2019). The origin of the Christchurch Call in Aotearoa New Zealand, with the personal investment in it of its prime minister, Jacinda Ardern, is pivotal to creating a new impetus and new space for a familiar discussion. The refusal of the Aotearoa New Zealand administration to use the attacker's name ensured that the focus of media attention remained on the attack itself (Lankford and Tomek, 2018). Aotearoa New Zealand is an unlikely incubator environment for terrorism and all New Zealanders can be seen as victims of this intrusive violence. Aotearoa New Zealand had hitherto not been a state where technology companies were battling against proposed antitrust intervention, privacy legislation and demands to take down fake news and at the same time give protection to free speech rights. This absence of prior history makes the Christchurch Call all the more emotive.

The modalities of this partnership approach commit states to building societal resistance to terrorism and extremism as well as to using regulation in a variety of formats (hard law, soft law, policy tools) to discourage the making and reporting of material and events that support the same. The commitment of OSPs is to transparency of action in general and in particular to the terms of service they operate under in relation to content upload. There is an expectation that those terms of service will be used to achieve a balance between freedom of expression and content removal in the context of the behaviour that the call relates to. In other words, the expectation placed on OSPs for industry-based action is quite a narrow one. The algorithms that drive users with particular activity histories on the internet to violent or extremist content are to be kept under review. In terms of their joint undertakings, there are obligations to civil society around the support of community efforts to counter extremism, obligations to assist smaller internet platforms in developing the capacity to deal with terrorist and extremist content, and obligations to support each other in exchanging information and research that will encourage the development of automatic technical intervention to remove such content (Pandey, 2020).
Answering the Christchurch Call

The Christchurch Call offers three pillars of intervention: the social, the regulatory and the technical. These cannot be seen in isolation from each other. Content moderation is a good example of this interlinking. The call is looking to governments and OSPs to develop content-moderation strategies to combat the uploading of extremist and violent content. This is presented as a technocratic solution to be applied in the event of the failure of the cultural strategies around social inclusion to combat inequality and build resilience to extremist discourses and the regulatory solutions around preventing the production and dissemination of this type of material. Much faith is being placed in technology as an end-game solution to the extent that there are pledges to make algorithmic solutions available across OSPs on the basis of a commercial sharing of innovation. It is possible that in the future machine learning will have evolved sufficiently so that it can do this consistently (Hall et al., 2020) but problems of transparency in what is in many instances the policing of free speech will still occur (Gowra et al., 2020). The events of Christchurch, while not unique, are very much at one end of a long spectrum of potential content-moderation activity.

However, the current reality of content moderation is that it seems to work most efficiently if there is a substantial element of human screening and intervention alongside automated review (Einwiller and Kim, 2020). Human screening or commercial content moderation has its limitations around the quantum and type of material that needs to be viewed. It is a low status, poorly remunerated and stressful job that exposes workers to disturbing words and images (Roberts, 2019). Increasingly, content moderation means the establishment of user-driven moderation tools such as flags, muting ability and the hiding of material (Crawford and Gillespie, 2016). Technology in all its guises reflects its social setting; it is impossible for a technocratic solution not to be embedded in human agency (Katzenbach and Ulbricht, 2019). User-driven content moderation pits user against user without offering any guidance or scaffolding around the appropriate social norms to be applied. There is an increased risk of echo chambers occurring as those not aligned to the position at hand are silenced; some users might find themselves isolated in particular spaces and there might be severe curtailment of free speech opportunities as potential over-censoring takes place by those without a broader view.
The Christchurch Call recognises the presence of an ecosystem between users, content, OSPs and the global reach of their business in the sense that any possible solution requires the sharing of innovation and new expertise. What the call does not explicitly deal with are the problems posed by the fragmented nature of the tech stack that underpins internet activity. Six very large technology companies are signatures to the call: Amazon, Facebook, Google, Twitter, YouTube and Microsoft (what we might call the usual suspects), and they are joined by two French companies, Qwant, a search engine, and Dailymotion, a video-sharing platform. Behind these platforms and search engines sit layers of other specialised technical service firms, inter alia, domain name registrars, hosting services, content delivery networks, internet service firms and security firms. Any web presence depends on the seamless interlocking of these services. The firms in the different layers of the tech stack will have terms of service around the screening of content, the takedown of content and ultimately a denial of service. Following their own policies places these firms in the position of deciding what material appears on the internet, who can view that material, and, ultimately, what groups are represented and which voices are heard.

The complexity of the tech stack allows the creators and purveyors of violent and extremist material to burrow further into the recesses of the internet. We might assume that the largest OSPs, like the ones that signed the Christchurch Call, operate in similar ways and on reasonably similar terms of service. We know comparatively little about how the smaller, single service firms, without which the internet could not function, operate (Gillespie et al., 2020). At times we might be pleasantly surprised; Facebook may have eventually removed the video of the Christchurch attacker and by doing so made it inaccessible to many casual users but it was the action of a small content delivery network firm (Cloudflare) that resulted in the shutdown of more sinister sites dedicated to racist outpourings that were also carrying it (Donovan, 2019). However, as a general principle, to be successful in their aim of preventing the upload of violent, extremist material the signatories to the call are hoping that the engine room of the internet embedded in the tech stack endorses and follows their approach.

The Christchurch Call lacks a geographic or regulatory anchor to the nation-state. It is an aspirational document aimed at inter-state cooperation as evidenced by its internal references to ‘partner countries’, and future inter-governmental meetings such as the G20 and the G7.
This is unsurprising in that the Christchurch Call was assembled on the back of the Paris Call that had been launched by President Macron of France in the days following the centenary of the 1918 armistice. The Paris Call focused on acknowledging the need of individuals for cyber security and how they should be seen essentially as non-combatants in any cyber attacks (the new warfare) launched by rogue governments or hackers and afforded assistance by technology companies and states. The crossover with the Paris Call explains why two French technology companies were signatures to the Christchurch Call. Taken together, these two interventions by national leaders with their appeals to multilateralism across a broad range of stakeholders can be seen as the beginning of techdiplomacy (Smith and Browne, 2019, pp. 109–30). The Christchurch Call has called OSPs to account in a very public way and opened up a dialogue space that, from a reputational standpoint, is impossible for them to resist.

However, there is unlikely to be supranational agreements of substance around removing violent and terrorist material from the internet emerging from these sorts of discussions in the short to medium term. Multilateral agreements in any area require extensive negotiation and frequently, even then, require implementation and enforcement, post-interpretation, at the domestic state level. There is no internationally agreed definition of terrorism (Hardy and Williams, 2011). National legal systems have very different definitions of hate speech and no agreement on what is harmful (Nemes, 2002). The possibility of either of these things becoming the subject of international agreement is very low indeed. Civil society as the Christchurch Call uses the term is a reference to the broad polity rather than a suggestion of any structured representative engagement with particular interest groups. Interventions are likely to work rather better if they carry an element of co-design or endorsement from the user sector.

For technology companies, an understanding of each national context in which they operate in terms of their own market position and wider political and cultural norms is essential, as it is that national context that will inform regulatory solutions, the possibilities for self-regulation and civic responsibility, and the potential for amelioration by CSR activities (Thompson, 2019). In terms of a general example of national context, we know that unrestricted free speech as a right has much more support in the US than it does in Germany (Wike, 2016) because each has a very different cultural setting around the exercise of individual
rights. In more specific terms, Facebook does not allow postings from the UK group Britain First, which has a right-wing political orientation, because much of their discourse is around the promotion of racial and religious hatred. However, Britain First, no matter how distasteful one finds the positions they advocate for, is not a proscribed organisation in the UK. A denial of platform by the UK’s most popular social media site, judged by commercially available statistics (Statista, 2020), risks giving credence to claims of victimisation and differential treatment from their supporters. It pushes these sorts of users into darker, less accessible places on the internet, such as Gab, Parler and Telegram, and towards the business actors that support them (Murphy and Venkataramakrishan, 2021). It also makes their rhetoric more attractive to some sections of UK society that see themselves as disconnected from the political mainstream.

The Christchurch Call in domestic settings

MGAFA (Microsoft, Google, Apple, Facebook and Amazon) are the world’s largest companies by market capitalisation, and all headquartered on the west coast of the US. There are significant differences between them in terms of their business scope (e.g. Amazon has a large physical distribution network and Apple is mainly a hardware business, while Google and Facebook are largely an online presence only) but each dominates in their particular segment: for example, Google in the global search market, Facebook in the digital advertising market, Amazon in the e-commerce market (Barwise and Watkins, 2018). The shift observed around the internet moving from, at worst, a benign intervention creating a new and free public space based on shared values of non-profit making and little state interference to the internet as a purveyor of harmful and dangerous material, a harvester and seller of personal data and a denier of free speech controlled by this small number of globally powerful companies assembling huge profits (a narrative that is not entirely true as demonstrated by the discussion of the tech stack but plausible enough to raise concerns [Noam, 2016]), places the activities of these companies under scrutiny in nation-states.

The Christchurch Call secures that national-level scrutiny wonderfully well, as Aotearoa New Zealand, like Australia and much of the rest of the world, does not have a domestic OSP industry. If US-located technology
companies can be used to promote a terrible event happening in a place known mostly for rugby union and tourism, then these technology companies can be drawn into the promotion of extremist violence anywhere. This ability to promote and support undesirable activities in individual states across the world must be reined in (Smith, 2018). This negative perception of technology companies (termed techlash) at the national level sits alongside popular concerns about the activities of the corporate sector more generally. The retreat of the state under a philosophy of New Public Management in many developed countries has pushed the provision of previously state-led services into the hands of private sector corporations. Access to these services is frequently dictated by technology corporations through devices and digital platforms. Public scrutiny of corporate activities has followed and particular ire has been directed at, inter alia, low taxation revenue raised from non-domiciled corporations with apparently large profits, a description that certainly fits MGAFA when they operate outside the US (Davidson, 2014); rising executive pay in a climate of largely stagnant wage remuneration for rank and file employees; and the need for demonstrably responsible innovation and behaviour to ameliorate harmful activities.

A number of states have embarked upon public inquiries, or their equivalent, into the power and influence of OSPs in recent years, both before and after the Christchurch Call, and how best to achieve effective governance of them on the national stage: India, Aotearoa New Zealand, Germany, France, the UK, Canada, The Netherlands, Switzerland, the US and Australia. Australia’s direct response to the events of Christchurch was to pass the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (Cth) in April 2019, which means, of course, that this legislation was not informed by the Christchurch Call or the discussions around it (Douek, 2020). The ‘right to be forgotten’ litigation between Spain and Google, as well as explaining the rights of EU citizens in relation to private facts (Rallo, 2018), demonstrates that OSPs can accommodate segmentation of their services on geographic lines and so can tolerate different governance settings in different jurisdictions. The presence of the Christchurch Call, state-based responses to it and national inquiries, both extant and new, have seen OSPs rush to model themselves as responsible self-governing organisations through the adoption of voluntary codes and oversight mechanisms. The Facebook Oversight Board is one such response. It is a body of 40 or so lawyers, academics and commentators drawn from around the world by Facebook. Its remit is to
act independently of Facebook, reviewing a sample of the organisation’s decisions around content-moderation oversight to see if it complies with its own policy (Klonick, 2020). While it is an interesting venture into the feasibility of crowd-sourcing public opinion in the international arena, it is unlikely to have much practical effect in an area where the feasibility of global governance is severely challenged.

The Facebook Oversight Board is a classic example of self-regulation in that it is an entirely responsive mechanism by the company that attracts much attention but actually requires Facebook to do very little over and above what it already does in the area of content moderation. It has no specific deliverable in terms of stimulating behavioural change. Facebook’s shareholders have no need to panic that corporate profits will be impacted by the decision to adopt this strategy. In most jurisdictions, regulation is used to signal the lowest level of performance or conduct that is considered to be consistent with current societal cultural norms and acceptable to the state in terms of the enforcement mechanisms that need to be in place (Bunting, 2018). Domestic jurisdictions recognise that their regulatory enforcement powers do not go beyond their territorial borders and that in both legislative content and enforcement, technological innovation is frequently ahead and will only move further ahead (Hemphill, 2019).

Regulation, particularly the currently fashionable principles-based regulation, is used to stimulate corporate actors to operate over and above it in a way that it is consistent with civic responsibility. This civic responsibility is often ‘soft-signalled’ by the adoption of a co-designed ‘code of ethics’. This is particularly important in the context of OSPs, which are the ultimate societal gatekeeper in terms of the control they have over access to information, communication and services (Metoyer-Duran, 1993). In these circumstances, gatekeepers have a responsibility to support the public interest (Shapiro, 2000). As Taddeo (2019) expresses it:

[Civic] responsibilities require OSPs to consider the impact of their services … on the societies in which they operate, take into account … ethical benefits and risks, and act so [as] to maximize the former and mitigate the latter. Ethical considerations need to become a constitutive part of their … business model.

Regulatory compliance by OSPs is necessary but on its own it is insufficient to create an environment where OSPs respond continuously and positively at pace with technological developments and in societal
BECOMING CIVIC ACTORS

interests to create better outcomes (Floridi, 2018). Other industries, for example those in the banking and finance sector in the aftermath of the global financial crisis, have similarly rehabilitated themselves.

The rights set out in the Universal Declaration of Human Rights and the expression they are given in a society is an obvious starting point to determine what values should shape OSP practices in pursuit of civic responsibility. Human rights are obligations of the state but in 2011 the UN adopted the Guiding Principles on Business and Human Rights, which calls on corporations as private actors to respect human rights (UNHRC, 2011). We might think that it is important to protect users’ privacy, to correct and prevent biases in information and safeguard the democratic process. Core human rights to be respected would include expression, personal security and dignity, freedom from all forms of discrimination and freedom of exposure to harm and harmful content (Suzor et al., 2018). Transparency of action by OSPs underpins all these values. Accountability and structures for accountability are something that public and quasi public institutions must exhibit. It is within the ambit of these fundamental rights that policies on content moderation should sit. This tie to fundamental rights is an aspirational starting point for a discussion around OSPs and civic responsibility. Few democratic states have a complete articulation of a human rights–compliant framework in their constitutional setting or in supporting legislation. This is true of the US with its grand republican constitution and Germany with its concern for the prevention of hate speech and, in the aftermath of World War II, the protection of the truth (Article 19, 2018). Australia starts from the position of a constitutional settlement, which contains only five limited individual rights and no meaningful domestic discourse about rights or ethics at the nation-state level (Wheeler, 2020).

Constitutional recognition of a particular right is important in assessing its place in society but it is not definitive. Deciding on the values that underpin civic responsibility and how conflicting values should be weighed against each other will be a process of negotiation that involves political actors, civil society and users on a national basis. Users are particularly important contributors to this negotiation as much of OSPs’ activity involves interaction with user content. If OSPs think of these fundamental rights at all, it is in a context that is informed by corporate norms (Jørgensen, 2017). We know that these corporate norms are likely to come from a fundamentally libertarian standpoint that draws on the American individualist tradition (van Dijck et al., 2018). The ways in
which OSPs organise to construct their civic responsibilities will be dependent on how democratic dialogue operates within individual states. The occurrence of serious events makes society-wide discussions, megalogues in Etzioni’s (2002) terms, which span different levels of informal and formal governance more possible. The terrorist attack of March 2019 in Christchurch is one such event.

References


3. BECOMING CIVIC ACTORS


3. BECOMING CIVIC ACTORS


