IAN AXFORD
(NEW ZEALAND)
FELLOWSHIPS
in
PUBLIC POLICY

Social media monitoring by New Zealand agencies: policy and legal landscape, risks, and considerations

Prepared by
Rachel Levinson-Waldman

With funding from the sponsors of the
Ian Axford (New Zealand) Fellowships in Public Policy

June 2024

Established by the
New Zealand government in 1995
to facilitate public policy dialogue
between New Zealand and
the United States of America

Level 5, 26 The Terrace
PO Box 3465
Wellington 6011
New Zealand

Telephone +64 4 494 1506
E-mail info@fulbright.org.nz
axfordfellowships.org.nz/

Published by Fulbright New Zealand, June 2024

ISBN 978-1-7386094-8-2

Ian Axford (New Zealand) Fellowships in Public Policy

Established by the New Zealand Government in 1995 to reinforce links between New Zealand and the US, Ian Axford (New Zealand) Fellowships in Public Policy provide the opportunity for outstanding mid-career professionals from the United States of America to gain firsthand knowledge of public policy in New Zealand, including economic, social and political reforms and management of the government sector.

The Ian Axford (New Zealand) Fellowships in Public Policy were named in honour of Sir Ian Axford, an eminent New Zealand astrophysicist and space scientist who served as patron of the fellowship programme until his death in March 2010.

Educated in New Zealand and England, Sir Ian held Professorships at Cornell University and the University of California, and was Vice-Chancellor of Victoria University of Wellington for three years. For many years, Sir Ian was director of the Max Planck Institute for Aeronomy in Germany, where he was involved in the planning of several space missions, including those of the Voyager planetary explorers, the Giotto space probe and the Ulysses galaxy explorer.

Sir Ian was recognised as one of the great thinkers and communicators in the world of space science, and was a highly respected and influential administrator. A recipient of numerous science awards, he was knighted and named New Zealander of the Year in 1995.

Ian Axford (New Zealand) Fellowships in Public Policy have three goals:

- To reinforce United States/New Zealand links by enabling fellows of high intellectual ability and leadership potential to gain experience and build contacts internationally.
- To increase fellows' ability to bring about changes and improvements in their fields of expertise by the cross-fertilisation of ideas and experience.
- To build a network of policy experts on both sides of the Pacific that will facilitate international policy exchange and collaboration beyond the fellowship experience.

Fellows are based at a host institution and carefully partnered with a leading specialist who will act as a mentor. In addition, fellows spend a substantial part of their time in contact with relevant organisations outside their host institutions, to gain practical experience in their fields.

The fellowships are awarded to professionals active in the business, public or non-profit sectors. A binational selection committee looks for fellows who show potential as leaders and opinion formers in their chosen fields. Fellows are selected also for their ability to put the experience and professional expertise gained from their fellowship into effective use.

We acknowledge and thank the following sponsors that support the Ian Axford (New Zealand) Fellowships in Public Policy programme:

- Department of Internal Affairs
- Ministry of Defence
- Ministry of Education
- Ministry of Foreign Affairs and Trade
- Ministry of Health
- Ministry of Justice
- Ministry of Social Development
- New Zealand Customs Service
- Public Services Commission
- Victoria University of Wellington School of Government

Acknowledgments

This fellowship has been a life-changing experience, and I am grateful beyond measure to so many people and institutions. The Office of the Privacy Commissioner, the Board of the Ian Axford Fellowship in Public Policy, and Fulbright New Zealand collectively made this adventure possible. Privacy Commissioner Michael Webster took a chance on someone he met over a very distant zoom, bringing on the Office's first-ever Axford Fellow, for which I am forever grateful. Peter Mee was a constant steady hand as I developed my project and wrote this report, and I benefited from Liz MacPherson's and Jo Hayward's wisdom. Thank you, too, to the Comms pod for welcoming an American interloper, Kate Rickerby and the policy team for offering their insights, Frances Vaughan for helping me navigate, and the whole OPC family for introducing me to the delights of morning tea and the 3 pm quiz. I truly could not have asked for better colleagues.

Roy Ferguson and Penelope Borland, with Axford and Fulbright respectively, helped select me as a fellow and were enormously welcoming in both the United States and New Zealand. Fulbright Programme Manager Lauren Summersell was the day-to-day MVP, ensuring that we made it to New Zealand with visas in hand and smoothing the course to a final report over emails and coffees. Axford board member Pattrick Smellie was a generous source of information and support. Michael Macaulay, my academic mentor at Victoria University of Wellington, was a consummate advisor and made introductions that transformed my project. And as I finish this report, I am deeply appreciative to Daisy Coles for her careful editing and sound guidance.

The Axford alumni network was an instant welcoming committee in DC before I set foot in New Zealand. I am particularly grateful to Nate Swinton, who was a sounding board for me over several years, as well as to Alexa Daniels-Shpall, David Liebschutz and Lisa Lunt, former Axford fellows who helped steady me before the interview and celebrated with me once I was selected. Lisa and her husband Pat then exceeded all reasonable expectations by offering to keep our dog Jax during part of our time abroad. They say you are only as happy as your unhappiest child; in this case, we were only going to be as happy as our unhappiest dog, and Pat and Lisa's family – including their children Angus and Holly and their two dogs Sheba and Woody – helped ensure that humans and canines alike lived their best lives.

Aphra Green, New Zealand public servant extraordinaire, first told me about the Axford Fellowship when she was serving on a Harkness Fellowship in Washington, DC in 2017. She kept in touch in the subsequent years, encouraged me to apply, made the instrumental introduction to the Office of the Privacy Commissioner, fielded some panicked missives and was generally a constant champion for my success. Once we arrived in Wellington, she picked us up from the airport (possibly against doctor's orders) and was unhesitatingly generous in translating Kiwi-isms and making introductions to contacts across the government.

During my research, I spoke with dedicated public servants from across Wellington as well as practitioners, advocates and academics across Aotearoa New Zealand, who fielded my questions and requests for information and introductions with extraordinary generosity and patience. This is by no means an exhaustive list, but I owe special thanks to Sarah Adams-Linton, River Ayto, Tabby Besley, Claire Black, Dean Blakemore,

Trevor Bradley, Michael Daubs, Katrine Evans, Annabel Fordham, Angus Lindsay, Nessa Lynch, Emmy Rākete, Dawn Swan, Annette Sykes and Peter Tyson. Any errors that remain are mine alone.

Brennan Center for Justice President Michael Waldman and Vice President for Program Initiatives John Kowal were instrumental in enabling me to take six months away from my position as Managing Director of the Liberty and National Security Program. My LNS colleagues, particularly Liza Goitein and Faiza Patel, were unfailing cheerleaders as well, even when they had to shoulder the burden of being down one colleague.

Wellington itself is a truly special city. I will leave with gratitude for having had the opportunity to live here as well as regret at not having time to explore every corner of it. Our best decision was to live in walking distance of Aro Café and next door to the best neighbours in the southern hemisphere, Stefanie Lash and Luke Allen and their boys, Henry and Leo. Stef and Luke were purveyors of feijoas, grocery store chauffeurs, interpreters of Kiwi phrases, guides to New Zealand history, and patient recipients of countless requests for assistance and household tools. Living in Aro Valley also meant that we lucked into Te Aro School, a model of diversity and inclusivity; Te Aro's wonderful principal Sue Clemens helped ensure that our children had a seamless transition to a new school. And Temple Sinai Wellington and Habonim Dror Aotearoa provided our family with a Jewish community at a particularly meaningful time.

I could not have had a better co-fellow than Megan Seeds. In addition to becoming a fast friend, Megan acted as a sounding board and reality check more times than I can count. This experience also would not have been the same without the other Fulbright Welly WonderGals, Kira Omelchenko and Sheila Crowell.

None of this would have been possible without my family. I am grateful to my parents, Cynthia and Sandy Levinson, for their unconditional love and support, and for temporarily moving our family abroad when I was in sixth grade, a transformative experience that drove me to give our children the same opportunity. I am indebted to my sister Meira Levinson for offering critical input and supportive counsel on my fellowship application (and all other things). And I owe enormous thanks to my in-laws, Cathy Waldman and Paul Levi, who gathered our mail, drove our car, and — most importantly — cared for Jax during our six months away, except when they travelled to visit us.

Finally, to my husband Ariel and our children, Sarah and Eli. Living abroad as a family was a long-held dream of mine, and they gamely tolerated and then enthusiastically embraced it. Ariel took the leap to temporarily step away from his demanding job as founding executive director of Tzedek DC, which required Herculean coordination with his board and colleagues. Many former Axford fellows told us the only thing better than being a fellow is being the spouse of a fellow – and while that may well be true, it took no small measure of planning and sacrifice to pull this off. I could not have asked for a better partner in this adventure, as we transferred our lives to New Zealand, travelled all over the South and North Islands together and experienced life in a new city. Sarah and Eli, who are thoroughly splendid people, made every day of this experience better. They were fantastic travel companions, and I am awed by their adaptability, resiliency, good humour, and ability to find joy everywhere – which is, luckily, not a hard task in the most beautiful place in the world. I hope the richness of this experience benefits them for years to come.

Rachel Levinson-Waldman
Te Whanganui-a-Tara, Wellington, June 2024

Executive summary

We live in a golden age of data. There is a nearly incalculable quantity of digital information, including from social media, available at the click of a button. This data is valuable to government agencies for investigations, intelligence, regulatory enforcement, fraud detection and risk assessments. Much of this information is available with little more than a social media account at most, which is sometimes taken as licence to mine it without restraint.

But unfettered use of even publicly available data by the state may undermine core democratic and human rights values, from the ability to independently develop one's views to freedom of speech and association to the liberty to form intimate relationships. This information can implicate personal and collective privacy and is susceptible to misuse, abuse and misinterpretation, as Te Aka Matua o te Ture / the New Zealand Law Commission and Te Tāhū o te Ture / Ministry of Justice observed in their landmark report on the Search and Surveillance Act 2012 over half a decade ago.[1] The situation in Aotearoa New Zealand and globally has only become more acute since then. That is the subject of this report.

The report begins with an introduction to key pro-social uses of social media, from community building and organising to use for legitimate law enforcement purposes, as well as the sometimes toxic influence of social media in Aotearoa New Zealand. It highlights several elements of New Zealand history and culture that form the backdrop to the state's current use of social media, including New Zealanders' traditionally high level of trust in police and public institutions; the relationship between the state and Māori and the growing push for Māori data governance and sovereignty; the state's history of surveillance, particularly of Māori; and the tragic 2019 attacks on a Muslim community that had itself felt targeted by the Government.

The report then moves to an overview of the main pieces of legislation that enable and regulate the state's activities in this realm: the New Zealand Bill of Rights Act 1990, Policing Act 2008, Search and Surveillance Act 2012 and Privacy Act 2020. It identifies critical gaps in several of these laws that make New Zealanders more vulnerable to intrusions into their privacy, civil liberties and civil rights.

The report then offers a first-of-its kind compendium of the collection, use and monitoring of information from social media by over a dozen New Zealand public sector entities. Drawing from published policies, media reporting, correspondence and interviews, it reveals some details publicly for the first time, and includes in an appendix two never-before-published forms governing account takeovers by police. And it sets out a catalogue of the potential harms arising from state scrutiny of social media:

a) the ability to easily and cheaply create a comprehensive picture of an individual or collective
b) the susceptibility of social media to misinterpretation
c) the impact of social media monitoring on core personal and political expression
d) the implications for vulnerable or marginalised groups

[1] Law Commission and Ministry of Justice (June 2017), pp. 180–181

e) additional hazards of automated and AI-driven tools
f) the heightened risks of undercover online enforcement activity.

Based on the current legislative landscape, existing agency policies and practices, and potential harms, it offers three key recommendations:

1. The Search and Surveillance Act 2012 should be updated to direct agencies to develop and publish detailed policies, specifically covering their use of social media, and the Privacy Act 2020 should be updated to protect, to the maximum extent possible, against the potential harms of state exploitation of even publicly available information.
2. Regardless of whether a statutory obligation is implemented, all agencies using social media for investigative, enforcement, fraud detection, risk assessment or regulatory purposes should have publicly available policies governing these activities, as recommended by the 2017 joint report from the New Zealand Law Commission and Ministry of Justice, accompanied by robust oversight and transparency mechanisms to ensure compliance.
3. The entities undertaking this policy development and statutory update should endeavour to minimise the hazards associated with the use of information from social media, and should engage with the public to ascertain in more detail the level of social licence for current and potential future uses of social media. This report offers in closing a set of questions for agencies to consider in this process and as they undertake, expand or review their use of social media for data collection.

These recommendations would help Aotearoa New Zealand take a major step towards protecting New Zealanders' privacy, civil liberties and civil rights in the digital age, and could act as a model for other governments worldwide.

Table of Contents

Introduction

Almost two decades after Facebook and Twitter (now X) entered the scene, social media[2] is a nearly constant presence in many New Zealanders' lives.[3] It connects friends and family, a particularly keen priority in Aotearoa New Zealand, which has one of the largest diaspora populations in the OECD. Families of origin are dispersed around the Anglo world, the Pacific Rim and Asia.[4] Social media also links members of marginalised and displaced communities, including indigenous groups and members of rainbow communities who may be isolated by virtue of being in rural areas, having families of origin who are not supportive of their sexual or gender identity, or coming of age during the COVID-19 pandemic.[5] And as the US Supreme Court has observed, it "allows users to gain access to information and communicate with one another about it on any subject that might come to mind."[6]

Used appropriately, social media can also be valuable to public sector agencies who use it to collect intelligence, enforce the law, investigate crimes, detect online threats, and allocate public safety resources. It may depict evidence of offline criminal activity, like ram raids,[7] stolen goods or possession of illegal firearms, and can itself be used to commit crimes, including online scams, identity theft, child exploitation and human trafficking. While the scope of social licence for law enforcement use of social media is not settled, there is, as the New Zealand Supreme Court has described, a "public interest in proper law enforcement, including the detection and prosecution of criminal behaviour", and this may encompass use of social media.[8] Outside the policing context, agencies may turn to social media to investigate violations of import laws, respond to online crises and enforce compliance with regulatory obligations, among other tasks.

Social media is a potent political tool as well. It can help nurture a "more democratic form of political participation" for marginalised communities who may be excluded from formal political structures.[9] This is a function not just of the connected space that

---

[2] This report adopts the definition of "social media monitoring" developed by the Ministry of Justice and the Law Commission in their joint review of the Search and Surveillance Act 2012, slightly modified to extend beyond law enforcement officers: social media monitoring should be understood to encompass access to social media by enforcement officers or other governmental agents "to obtain information about individuals or classes of individuals." Law Commission and Ministry of Justice (June 2017), p. 179. I draw on the definition of "social media" contained in the New Zealand Government's 2023 review of the Intelligence and Security Act 2017: "websites or applications that focus on communication, community-based input, interaction, content-sharing and collaboration, such as Facebook, Twitter, Telegram, Google, Instagram and so on." Arnold, Hon Sir Terence KNZM KC and Matanuku Mahuika (2023), p. 39 n. 46

[3] Arnold, Hon Sir Terence KNZM KC and Matanuku Mahuika (2023), p. 39 n. 47 (noting that four-fifths of all New Zealanders had a presence on at least one social media platform as of 2022); Matika, Correna et al (Dec. 2023), pp. 6, 11 (annual survey ranking social media the highest among activities on which New Zealand internet users spent their non-work time, with Facebook predominating)

[4] See Walters, Laura, *The Spinoff*, 10 Aug. 2021

[5] See, e.g., Waitoa, Joanne Helen (2013), pp. 17–34, 71–73; Black, Claire (2018), pp. 3, 16

[6] *Packingham v North Carolina* 582 US 98 (2017), p. 107

[7] See, e.g., Baker, James, *1News*, 27 April 2022

[8] *R v Ngan* [2008] 2 NZLR 48 at [104]

[9] Green, Jordan (July 2020), p. 25; see also ibid. p. 1 (referring to "Māori Instagram"); Wilson, Alex, et al (2017), p. 1 (observing, with respect to indigenous use of social media, that "Facebook and other social media facilitate … interaction and allow users to maintain relationships across vast distances and time

social media creates, but also of specific platform affordances; hashtags, for instance, can be used to organise, to elevate particular issues and even to challenge dominant media narratives.[10] Facebook and Instagram were used to mobilise both online and in-person support for the Ihumātao land occupation, which culminated in a successful push to keep the land from being developed by a private outfit.[11] Participants were able to use social media to craft the story and to keep public attention, as well as to reveal uses of force by law enforcement against protestors.[12] And Instagram was a critical organising space for the successful 2022 campaign to ban gay conversion therapy in New Zealand; activists used it to build community, elevate public awareness and raise the pressure on politicians.[13]

Social media is not, of course, an unqualified good. As Māori lawyer and activist Annette Sykes (Te Arawa, Ngāti Makino, Ngāti Pikiao) notes, while social media can help facilitate political engagement among Māori rangatahi (youth), it can also disengage rangatahi and the community as a whole from discussion that would historically happen at the marae, or meeting ground.[14] Indeed, where indigenous groups turn to social media for internal community building, this is typically due in part to the realities of displacement caused by colonialism.[15]

Social media also facilitates behaviours that pose broad challenges to a peaceful, democratic society, including recruitment to extremist causes, dissemination of hateful rhetoric and distribution of mis- and disinformation.[16] The Royal Commission of Inquiry into the 2019 Christchurch masjidain attacks observed that social media platforms have become the main locus of organising, recruitment and education for right-wing extremist groups; both mainstream and more fringe platforms have played a role.[17]

---

zones, thereby increasing social and political connectivity and impact"); Waitoa, Joanne Helen (2013), pp. 74–77 (documenting the Mana Party's five key goals for using Facebook)

[10] See, e.g., Green, Jordan (July 2020), p. 23; see also Lindgren, Simon and Coppélie Cocq (2017), pp. 131–150 (documenting the use of social media in indigenous protest movements for information sharing, network building and support)

[11] See McKenzie, Peter, *The Spinoff*, 1 Aug. 2019; Green, Jordan (July 2020), p. 59; Roy, Eleanor Ainge, *The Guardian*, 17 Dec. 2020; see also Green, Jordan (July 2020), p. 72 (documenting other resistance efforts inspired by social media, including protests against child removals from Māori whānau)

[12] Green, Jordan (July 2020), p. 77

[13] See Lal, Shaneel (2023); Conversion Practices Prohibition Act 2022

[14] Waitoa, Joanne Helen (2013), p. 74. Throughout this report, I define terms that will be familiar to a New Zealand audience but may be less so to readers outside New Zealand. For those interested in exploring te reo Māori (the Māori language) further, the Māori Dictionary, at https://www.maoridictionary.co.nz/, is an excellent reference.

[15] Green, Jordan (July 2020), p. 33

[16] Disinformation and extremism are increasingly enmeshed; while disinformation far predates the development of social media, social media has supercharged its speed and reach, and it plays an increasingly important role in New Zealand's online ecosystem. See, e.g., *New Zealand's Security Threat Environment 2023* (Aug. 2023), p. 38; Hattotuwa, Sanjana, et al (April 2023), p. 11; *Nine to Noon*, 18 May 2022. An analysis of the state's role in monitoring and combating disinformation and the political and privacy implications of what is deemed mis- or disinformation are, however, beyond the scope of this report.

[17] "Chapter 5: Harmful behaviours, right-wing extremism and radicalisation" (8 Dec. 2020); see also Halpin, James and Chris Wilson (2022), pp. 21, 23, 30–31

The harms of these kinds of antisocial behaviours are not evenly distributed. The vast majority of New Zealand online extremists align with far-right ideologies, suggesting that the targets of far-right hate — including indigenous groups, immigrants of colour, women, individuals identifying as or appearing to be LGBTQ+ and members of minority religious groups — will bear the brunt of their rhetoric.[18] And research shows that while 18 per cent of New Zealanders have experienced online harm or harassment, those numbers are higher for Māori and those with long-term disabilities.[19]

These multifaceted uses of social media make it a rich, sometimes overwhelming, and potentially risky source of information for state agencies seeking to combat crime and hate speech, conduct investigations, enforce regulations, detect fraud and assess risk. While social media monitoring — and data collection overall[20] — do not yet appear to be as pervasive in Aotearoa New Zealand as they are in the United States, this report reveals that social media is in use by a number of New Zealand agencies with investigative, regulatory or enforcement functions. With the American experience illuminating the hazards of expanding social media monitoring in the absence of adequate guardrails or public engagement, New Zealanders have an opportunity for earlier intervention to ensure that the use of these capabilities reflects principled human rights values.[21] Overall, the research underlying this report suggests that New Zealand agencies are approaching their use more cautiously, influenced by ethical considerations and sensitivity to public acceptance.

The expanding use of social media also comes against the backdrop of Aotearoa New Zealand's history and national culture. The country is known for having a high level of trust in its institutions, and that trust is extended in large part to police as well, despite some recent drops.[22] New Zealand police have historically taken pride in showing a friendly public face; officers typically do not carry guns on their person and the service emphasises the importance of consent and positive community relations for its operations.[23]

At the same time, the history of law enforcement and surveillance in New Zealand is complex, as it is around the world. Dr Richard Hill, the preeminent historian of New Zealand's police service, has noted that surveillance and coercion are at the heart of policing — including in New Zealand, where the police service was birthed from the Irish constabulary and, by extension, the London Metropolitan police, with the goal of suppressing the expression of tino rangatiratanga (indigenous sovereignty) during the colonial period.[24] Filmmaker and activist Valerie Morse has documented surveillance

---

[18] Comerford, Milo, et al (2021), p. 11

[19] Matika, Correna et al (Dec. 2023), p. 32

[20] See "Chapter 2: The three ways the individual may have been detected" (8 Dec. 2020) (suggesting that "large-scale data aggregation" is being carried out by foreign countries but not New Zealand, at least as of December 2019)

[21] See Levinson-Waldman, Rachel, et al (7 Jan. 2022) for an overview of the use of social media by federal agencies in the United States

[22] See "OECD: High level of trust in the Public Service" (n.d.); cf. "Social cohesion straining at the seams" (13 June 2023) (noting erosion in social cohesion and high-trust culture)

[23] See Greener**,** Bethan, *The Conversation*, 24 Feb. 2021; see also Cooke, Henry, *Stuff*, 25 Feb. 2021 (documenting a 2021 parliamentary committee hearing in which Police Commissioner Andrew Coster defended policing by consent)

[24] Hill, Richard (2008), pp. 39, 44; see also Morse, Valerie (2019b), p. 199 (observing that "state institutions of surveillance, coercion and dispossession were central to the birth" of New Zealand)

as a central theme of state power since the country's founding, with a shifting crew of targets from anarchists, communists and pacifists to union leaders to activists for racial and social justice to Māori, who are subject to both policing and punitive measures at far higher rates than Pākehā (white European New Zealanders), eroding the social contract that underlies the consent model.[25, 26] The state has formally acknowledged some of these lapses, such as the 1970s Dawn Raids targeting immigrants from the Pacific, for which Prime Minister Jacinda Ardern apologised in 2021.[27]

Surveillance and data collection are intertwined as well. As Māori scholars Donna Cormack (Waitaha, Kāti Mamoe, Kai Tahu), Tahu Kukutai (Ngāti Tīpā, Ngāti Mahanga, Ngāti Kinohaku, Ngāti Ngawaero, Te Aupōuri) and Chris Cormack (Kāi Tahu, Kāti Māmoe, Waitaha) have observed:

> [The] imperative to accumulate large amounts of data facilitates the ongoing surveillance of Indigenous peoples that has long been central to the colonial project. … Oversurveillance of Māori, in particular by police, Corrections and other punitive and disciplinary institutions, means that data about Māori are more likely to be included in government datasets ….[28]

This history also contributes to the push for Māori indigenous data governance and data sovereignty, which together seek to recognise Māori rights in their own data and to establish structures and policies enabling Māori control over their data.[29] Māori data is broadly defined to include "digital or digitisable data, information or knowledge … that is about, from or connected to Māori".[30] This definition would include social media information relating to Māori individuals or collectives.

Two events in recent New Zealand history offer important contextual touchpoints for the intersection of state power, surveillance and marginalised communities, highlighting both concerns about misdirected surveillance and a desire for the state to play some role in stemming the tide of online hate that can magnify real-life threats.

First, in 2007, New Zealand Police undertook Operation 8, a campaign inflicting roadblocks, raids and arrests in the rugged North Island region of Te Urewera and nationwide on Māori activists and their families — including children — that became emblematic of overreaching police power and use of surveillance authorities.[31] Māori law scholars Khylee Quince (Ngāpuhi, Te Roroa, Ngāti Porou, Ngāti Kahungungu) and Jayden Houghton (Ngāti Maniapoto) situate Operation 8 within a broader context, asserting that the "surveillance of Māori, both individually and collectively, has often centred on political dissidents and their activities", and noting that the raids were "a

---

[25] Morse, Valerie (2019b), pp. 201, 210
[26] See Hurihanganui, Te Aniwa, *RNZ*, 26 March 2021; Quince, Khylee, *Stuff*, 6 March 2021
[27] See Cooke, Henry and Bernadette Basagre, *Stuff*, 14 June 2021
[28] Cormack, Donna, et al (2020), pp. 74–75; see also Royal Society Te Apārangi (Dec. 2023), p. 39 (noting the "long history of the state using intrusive racial surveillance and monitoring to control and categorise Māori, often as a threat"); Edwards, Lilian and Lachlan Urquhart (11 Dec. 2015), p. 4 (examining "dataveillance", the management of "populations through collection, sorting, management and risk assessment of data")
[29] Kukutai, Tahu, et al (2023-b), p. xi; see also Royal Society Te Apārangi (Dec. 2023), p. 19; Ruckstuhl, Katharina (2023); Taiuru, Karaitiana (2022), p. 9; "Co-designing Māori data governance" (2 Feb. 2021)
[30] Kukutai, Tahu, et al (2023-b), p. xi
[31] See Law Commission and Ministry of Justice (June 2017), p. 47

breach of both … individual and collective privacy".[32] While the raids largely predated the rise of social media, the police conducted extensive network analysis of the kind that would now draw heavily on online sources.[33] A Māori-focused chat room, Aotearoa Café, was shut down during the raids, suggesting early attention to the significance of digital spaces.[34]

Second, on 15 March 2019, a white supremacist committed a mass shooting of Muslim worshippers at two mosques in Christchurch. The perpetrator posted online, albeit often anonymously, in the leadup to his attack.[35] Less than half an hour before he opened fire, he posted publicly on 8Chan, a social media platform popular with the far-right, and then live-streamed the attack on Facebook in a video that migrated to YouTube, Twitter and other social media platforms.[36] The attack spawned horrific copycats, including at a predominantly African-American supermarket in Buffalo, New York, and a synagogue in Poway, California.[37] The massacre prompted a national reckoning, as scores of people told the resulting Royal Commission of Inquiry that the state had targeted Muslim communities as a threat while ignoring the online threats directed at them from white supremacists, laying the groundwork for some of the efforts described below to address online extremism.[38]

It is with this background in mind that this report explores the use of social media for information and intelligence collection, investigations, risk assessment and fraud detection by New Zealand public sector bodies, through the lens of the governing legal and policy framework, the potential harms posed by these practices and ways to mitigate them.[39]

---

[32] Quince, Khylee and Jayden Houghton (2023), pp. 74, 79
[33] See "Operation 8: The evidence and police spying methods" (Nov. 2013)
[34] Waitoa, Joanne Helen (2013)
[35] See Wilson, Chris, et al, *New Zealand Herald*, 21 Feb. 2024
[36] Wakefield, Jane, *BBC*, 17 March 2019; see also "Chapter 6: Planning the terrorist attack" (8 Dec. 2020) (documenting his Facebook and Twitter activity in the immediate lead-up to the attack)
[37] Comerford, Milo, et al (15 March 2024)
[38] "Ch. 5, What people told us about the national security system and counter-terrorism effort" (26 Nov. 2020); see also Tolley, Philippa, *RNZ*, 8 March 2020. Notably, one of the main recommendations from the inquiry, the development and promotion of a reporting system enabling members of the public to report concerning behaviours, which gained substantial support from Muslim and other faith communities, has not yet been implemented. Pennington, Phil, *RNZ*, 9 Nov. 2023-b
[39] It does not address the use of analytic tools embedded into government agency websites. See, e.g., Hill, Ruth, *New Zealand Herald*, 11 April 2023

1 Legal Framework

New Zealand is one of a small number of countries without a written constitution. Instead, the state's power — and New Zealanders' fundamental rights — are defined and regulated by a patchwork of legislation, conventions and legal decisions. While a comprehensive accounting would overwhelm this report,[40] four key statutes govern and inform the activities described below. They are the New Zealand Bill of Rights Act 1990 (BORA), Policing Act 2008, Search and Surveillance Act 2012, and Privacy Act 2020. These statutes have civil and human rights gaps that should be addressed through a combination of statutory updates and policy.

New Zealand Bill of Rights Act 1990

The New Zealand Bill of Rights Act 1990 (BORA) sets out protections for certain key democratic and civil rights, including:

- freedom of thought, conscience, religion and belief
- freedom of expression, including the freedom to seek, receive and impart information and opinions
- freedom of religion
- freedom of association and peaceful assembly
- freedom from discrimination.[41]

Section 21 of BORA also guarantees the right to be secure against unreasonable search or seizure, which has typically been taken as the linchpin of protections against overreaching state action.[42] Privacy "lies at the heart" of that right and underpins the protections for the freedoms of thought, conscience, religion and association.[43] These freedoms are implicated as well by the state's collection and analysis of information from social media, and the core values articulated in BORA therefore offer a foundation to bolster protections against overreaching social media monitoring.

At the same time, BORA has both structural and interpretive gaps. While BORA's protections "may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society", the statute explicitly denies courts the authority to overturn legislation that is in tension with the Act.[44] Even a finding by the Attorney-General that proposed legislation is inconsistent with BORA is

[40] The Search and Surveillance Act 2012 alone lists 78 other statutes governing the exercise of search, surveillance and inspection powers by non-police enforcement officers including Customs officers, Department of Internal Affairs and Inland Revenue investigators and fisheries inspectors: Law Commission and Ministry of Justice (June 2017), p. 9
[41] New Zealand Bill of Rights Act 1990, ss 13–17, 19
[42] Ibid. s 21; Law Commission and Ministry of Justice (2017), p. 39 (noting that the "principal expression of human rights values in the search and surveillance context is section 21" of BORA)
[43] Winkelmann, Hon. Justice Helen (Nov. 2018)
[44] New Zealand Bill of Rights Act 1990, ss 5, 4

merely advisory; Parliament need not amend a challenged Bill to bring it into alignment with the Act.[45]

In addition, there is some ambiguity as to whether BORA and its related constellation of statutes and case law permit the police (or other state actors) to do anything the public can do as long as not specifically proscribed, or if police action requires affirmative statutory authority.[46] Current consensus appears to put a thumb on the scale for the former approach, often called "third source authority," but a case currently before the New Zealand Supreme Court may result in some refinement of the theory.[47]

Finally, BORA was passed into law nearly a quarter of a century ago, before the world wide web was introduced to the public, let alone the creation of the mass of online data now easily available.[48] Not only does it not contemplate the impact of digital technologies but it famously does not include the word "privacy", which was considered at the time too contested to be enshrined in a bill of rights.[49] And while case law interpreting s 21 has reasoned that surveillance intruding on an individual's reasonable expectation of privacy rises to the level of a search, which would typically require a warrant, in the context of social media this is only the beginning of the discussion, not the end.[50] The notion of a "reasonable expectation of privacy", particularly when it comes to social media, may shift with societal norms and expectations, dependent in part on the platforms' changing policies and awareness of the hazards outlined below.[51] Moreover, social media monitoring is unlikely to require a warrant in all but the most intrusive circumstances. Thus, while BORA's foundational principles speak to the values implicated by overreaching social media monitoring, it cannot be relied upon as a certain bulwark.

Policing Act 2008

The Policing Act 2008 sets out the mechanisms for the police's governance and administration; given its vintage, it does not provide guidance regarding the collection or handling of information from social media or interaction with people online.[52] In keeping with a consent-based theory of policing, it leads with the proposition that "effective policing relies on a wide measure of public support and confidence", and sets out a related set of principles, including the importance of "principled, effective, and efficient policing services" to a "free and democratic society" and the provision of policing services that are independent and impartial and respect human rights.[53] It also enumerates police's functions, including public safety, community reassurance, law enforcement crime prevention, national security and emergency management, reflecting the general evolution of police responsibilities far beyond simply responding

[45] Ibid. ss 7, 7A, 7B
[46] Law Commission and Ministry of Justice (June 2017), p. 170
[47] Cardwell, Hamish, *RNZ*, 6 March 2024
[48] "A short history of the web" (n.d.)
[49] Palmer, Geoffrey (1985), pp. 103–104
[50] Law Commission and Ministry of Justice (June 2017), p. 10
[51] See Edwards, Lilian and Lachlan Urquhart (11 Dec. 2015), p. 27 ("To say that we implicitly give up all expectations of privacy when we join a platform used by millions because of terms and conditions we have not read, did not understand and could not alter seems surreal.")
[52] Policing Act 2008
[53] Ibid. s 8

to and solving crimes.[54, 55] This broad set of functions reappears in a police policy, covered below, for the proposition that any of them would provide a lawful purpose for data gathering.[56]

Search and Surveillance Act 2012

The Search and Surveillance Act 2012 is the primary law governing New Zealand Police's search and seizure powers; it pulled together what were previously multiple independent pieces of legislation governing police, and it enables by reference the enforcement activities of other agencies, including fisheries inspectors and immigration and tax officers.[57] Passed before law enforcement agencies began expending significant resources monitoring online activity, the Act "has not kept pace with developments in technology", in the words of the New Zealand Law Commission and Ministry of Justice in the 2017 report documenting their joint review of the Act.[58] It also has a major conceptual gap: while it sets out detailed procedures governing warrants and describes the circumstances in which a warrant is not required, it does not address the universe of activities that implicate privacy but for which a warrant regime would largely not be workable — such as social media collection.

The joint report highlighted the risks arising from this coverage gap, which have been supercharged in the intervening seven years. The authoring bodies noted that enforcement agencies' wide monitoring of online content, particularly to monitor protest activities, could chill people's willingness to engage in debate or voice unpopular opinions and could harm minority or marginalised groups.[59] Information posted online could be difficult to interpret or inaccurate, whether unintentionally or as a method of misdirection.[60] And the report emphasised that the mere fact that information is technically available without restriction does not necessarily reflect a desire for it to be available to all: users might reasonably contemplate "casual observation by peers but not intensive scrutiny by the State".[61]

Accordingly, the report urged that the Search and Surveillance Act 2012 be amended to require the Police Commissioner and the heads of other relevant enforcement agencies to issue policy statements specifically addressing social media monitoring.[62] The report recommended that the policy statements include guidance on (1) the purposes and circumstances in which social media monitoring could be carried out (limiting it, for example, to "certain law enforcement purposes to ensure it is not used to target legitimate activities such as peaceful protest"); (2) when a court order would be required; (3) how to minimise privacy intrusions (including by adequately limiting algorithmic social media monitoring); (4) oversight and accountability obligations; and

---

[54] Ibid. s 9
[55] See Coquilhat, Jenny (Sept. 2008)
[56] "Collection of personal information" (n.d.), p. 5
[57] See "Chapter 21: Creating powers of search, surveillance and seizure" (2021); "Review of the Search and Surveillance Act 2012" (n.d.)
[58] Law Commission and Ministry of Justice (June 2017), p. 9
[59] Ibid. pp. 180–181 (citing, inter alia, reports about US Department of Homeland Security's monitoring of Black Lives Matter protests via social media)
[60] Ibid. p. 181
[61] Ibid.
[62] Ibid. p. 175

(5) constraints on use, storage and destruction of information.[63] Oversight and accountability mechanisms are particularly important in light of the non-hypothetical risk that even strong policies are not followed in practice.[64] Despite the thoughtful and comprehensive analysis by the Law Commission and Ministry of Justice and the report's concrete recommendations, the push for reform appears to have gone dormant. Perhaps this report will help restart the conversation.

The joint report's recommendations are bolstered by a set of model standards released by the Public Service Commission in late 2018, sparked by revelations about the misuse of external contractors.[65] These standards, which were given additional teeth by the Public Service Act 2020, require agencies to put in place a policy framework and organisational safeguards for their collection of information "for regulatory compliance and law enforcement purposes."[66] The Commission appears to have been satisfied that the agencies complied with that obligation through their publication of general privacy and transparency statements.[67] While some of these statements provide the public with baseline information about the agency's use of social media, most are quite generic and some do not mention social media at all. The model standards would appear to require — or at least support — the development and publication of policies specifically addressing the collection and use of information from social media.

Privacy Act 2020

The final piece of the current legislative framework is the Privacy Act 2020. The Act, which builds on the original privacy statute, the Privacy Act 1993, protects individuals' privacy rights from intrusion or abuse by state entities, including law enforcement agencies, as well as private entities.[68] It provides a floor but not a ceiling for privacy protections — and it can be overridden with even less friction than BORA can, as it excuses an agency from being in breach of most of the Act's provisions if the agency's actions have been authorised by a contrary law, even if Parliament has not explicitly stated its intention to override the Act.[69]

The meat of the Act is its 13 Information Privacy Principles (IPPs). IPP 1 requires that agencies collecting personal information — defined as "information about an identifiable individual" — have a "lawful purpose" for doing so and that the collection be necessary for that purpose.[70] That requirement covers all personal information,

---

[63] Ibid. p. 183
[64] See, e.g., Pennington, Phil, *RNZ*, 28 Sept. 2022
[65] "Acting in the Spirit of Service: Information Gathering and Public Trust" (Dec. 2018-a); see also "Acting in the Spirit of Service: Information Gathering and Public Trust" (Dec. 2018-b); "Information gathering standards update" (23 April 2019)
[66] "Acting in the Spirit of Service: Information Gathering and Public Trust" (Dec. 2018-a), p. 1; Public Service Act 2020, ss 17 (authorising Public Service Commissioner to set minimum standards of integrity and conduct), 18 (directing agencies to comply with minimum standards)
[67] *Response to Official Information Act request* (17 July 2019). Note: in 2020, the State Services Commission changed its name to Public Service Commission. "New Public Service Act underlines spirit of service" (7 Aug. 2020)
[68] Privacy Act 2020; see also "Country reports on the functioning of the adequacy decisions adopted under Directive 95/46/EC" (15 Jan. 2024), p. 259 (specifying application of Privacy Act 2020 to law enforcement agencies)
[69] New Zealand Bill of Rights Act 1990, s 4
[70] Privacy Act 2020, s 22; ibid. s 7 (defining "personal information")

regardless of whether it is otherwise publicly available. Nevertheless, the Act does not appear to offer adequate protections to digital age data. The 2017 joint report from the Law Commission and Ministry of Justice was blunt on this point, declaring that "[w]e do not consider the principles in the Privacy Act provide sufficient protection against unjustified public surveillance", in light of their generality and lack of tailoring for law enforcement activity.[71]

The weaknesses are acute with respect to open source social media, as several of the privacy principles that give teeth to the Act exempt "publicly available information" from their protections.[72] IPP 2, for instance, requires that personal information be collected from the individual concerned, but exempts publicly available information, as well as situations where compliance with the obligation would "prejudice the purposes of the collection" or the "maintenance of the law".[73] This permits state entities to collect a significant amount of data about individuals from other sources, such as public social media posts or online contacts, without implicating the Privacy Act. To be sure, this is balanced to some extent by IPP 4, which requires that agencies collecting personal information must use a means that "in the circumstances of the case … is fair" and "does not intrude to an unreasonable extent upon the personal affairs of the individual concerned."[74] As detailed below, collection and monitoring of social media data can be quite intrusive for both the individual concerned and their associates, even when only "publicly available information" is at stake.

In addition, IPPs 7 and 8 require that agencies ensure to the extent possible that personal information they possess, use or disclose is accurate, up to date, complete and not misleading.[75] Social media data can pose obstacles to satisfying these obligations: interpretive challenges, including differences in language, tone or cultural context, can make it difficult to assess accuracy or even basic meaning. People commonly create online personas that do not reflect their real lives — seeking to portray, perhaps, a life of sun-filled vacations and perfect children. A user may have the views of friends or associates who post on their page or timeline incorrectly imputed to them. And enforcement agencies must be alert in an era of increasingly sophisticated deep fakes. This is not to undermine the importance of the principles set out in the Act. But public sector agencies will need to be thoughtful about how to satisfy those principles when it comes to social media data, and these hurdles offer an additional reason to tread cautiously and articulate robust policies.

There are some other carveouts for publicly available information that could invite misuse, whether intentional or inadvertent. For instance, IPP 10 limits agencies from using personal information for any purpose other than the one for which it was collected — but exempts data from the internet and other publicly available sources as long as the agency has reasonable grounds to believe that "in the circumstances of the case, it would not be unfair or unreasonable to use the information" for the additional

---

[71] Law Commission and Ministry of Justice (June 2017), p. 175

[72] Privacy Act 2020, s 7 (defining "publicly available information" as "personal information that is contained in a publicly available publication", which is defined to include an electronic publication "that is, or will be, generally available to members of the public free of charge or on payment of a fee". Publishing includes "disseminating by means of the Internet or any other electronic medium".)

[73] Ibid. s 22

[74] Ibid.

[75] Ibid.

purposes.[76] Similarly, while agencies are restricted under IPP 11 from disclosing personal information to any other agency or person, an agency may do so if the information was obtained from a publicly available source and it reasonably believes that it would not be unfair or unreasonable to disclose the information.[77] These are both broad carveouts for a wide swath of data, and it may be time to revisit them.

Finally, it is worth noting that the Act does not explicitly reference Te Tiriti o Waitangi / the Treaty of Waitangi, the foundational 1840 agreement between the British Crown and Māori chiefs.[78] In practice, this should not be an obstacle to recognising and incorporating the Treaty's principles. The Act directs the Privacy Commissioner to "take account of cultural perspectives on privacy". This is flexible language that can be — and has been — read to include Māori values, customs and culture.[79] In addition, New Zealand's courts have recognised that Te Tiriti principles form a part of the country's common law. The High Court has explicitly looked to tikanga (Māori customs) to help resolve at least one privacy case.[80]

At the same time, as scholars have explored, the Act's focus on individual privacy does not adequately protect Māori privacy values, with their collectivist lens.[81] Quince and Houghton have explained succinctly that the Privacy Act "champions individualistic Western conceptions of privacy with little regard for collective conceptions of privacy."[82] While an in-depth exploration of the intersection between the Privacy Act and Māori tikanga is beyond both the scope of this paper and the author's expertise, it necessarily underlies any discussion of the Act's application, and it is particularly relevant in the context of data that can be used to elicit information or draw conclusions about broader networks, as is true of social media data.

[76] Ibid.
[77] Ibid.
[78] Orange, Claudia (updated 28 March 2023)
[79] Privacy Act 2020, s 21; Quince, Khylee and Jayden Houghton (2023), pp. 123–124 (documenting the Office of the Privacy Commissioner's efforts to reinforce the office's obligations towards Māori)
[80] *Te Weehi v Regional Fisheries Officer* [1986] 1 NZLR 680 (HC); *Huakina Development Trust v Waikato Valley Authority* [1987] 2 NZLR 188 (HC); *New Zealand Maori Council v Attorney-General* [1987] 1 NZLR 641 (CA); *Te Pou Matakana Ltd v Attorney-General (No 2)* [2022] 2 NZLR 178 at [107] ("It is well accepted that tikanga Māori is part of New Zealand's common law.")
[81] See, e.g., Royal Society Te Apārangi (Dec. 2023), p. 20; Quince, Khylee and Jayden Houghton (2023); Kukutai, Tahu, et al (2023-a)
[82] Quince, Khylee and Jayden Houghton (2023), p. 45

2 Agency use of social media

In this section, this report offers the most comprehensive view available of how New Zealand public sector entities view, collect, monitor and analyse social media data.[83] Some of this information is revealed here for the first time. This material was obtained through review of publicly available policies and media reporting as well as interviews and correspondence with agency staff, civil society organisations, academics and advocates. It focuses largely on public entities with an investigative or enforcement role, while including some — like the Classification Office — that do not carry out either of those functions but whose work is closely tethered to offices that do. It does not purport to offer an exhaustive account, but it represents the most comprehensive picture currently available.

There are five main methods that enforcement and regulatory agents might use to obtain information from social media. Most agencies do not use all of these. First, agents may conduct online searches that do not require them to register for or log in to a social media site — for instance, a Google search whose results include a publicly available Facebook profile. Second, an agent may conduct more targeted social media searches or join a group using a social media profile, but interact minimally if at all with others on the platform. Depending on the circumstances, the profile may be identifiable as connected to the agency or may reflect an alias persona. Third, agents may use a false persona to engage more actively with a person of interest or their associates — for instance, commenting on posts or trading messages. This kind of activity may also involve an element of "backstopping" for the online persona: creating a believable online history to bolster its apparent legitimacy. Fourth, there are commercial tools that enable broadscale monitoring and data collection and analysis. Finally, in some limited circumstances, police may take over an individual's account either temporarily or permanently with their consent. The chart below summarises what is publicly known about which entities are authorised to use which methods, as well as whether they have a policy in place governing these activities and whether that policy has proactively been made available to the public.[84]

[83] The analysis begins with the New Zealand Police, which has the broadest usage of social media data; from there the analysis proceeds in alphabetical order, agency by agency. This report does not address in detail the national intelligence and security agencies.

[84] Several agencies have indicated that their policies are disclosable upon request under the Official Information Act 1982.

Overview

	General online searches that may yield publicly available social media information	Social media searches or engagement, including through use of persona accounts, but involving little to no direct interaction	Use of false persona to connect directly with individuals	Use of commercial tools	Account takeover with consent	Does the agency have a policy specifically covering use of social media?	Has the policy been proactively published?
Accident Compensation Corporation (ACC)	No	Yes, in limited circumstances with supervisory approval	No	No	No	Yes	No
Classification Office	No[85]	Yes, upon a referral or other information	No	No	No	No, though some information is available online	N/A
Department of Corrections	Yes	Yes	Not publicly known	Not publicly known	Not publicly known	Yes	No
Department of Internal Affairs –	Yes	Yes	Not publicly known	Yes, but does not use AI-driven tools or scrape data	Not publicly known	No, though some information is available online	N/A

[85] The Classification Office's business case does not encompass general online searches, though it may conduct some general searches as part of its due diligence to obtain context.

	General online searches that may yield publicly available social media information	Social media searches or engagement, including through use of persona accounts, but involving little to no direct interaction	Use of false persona to connect directly with individuals	Use of commercial tools	Account takeover with consent	Does the agency have a policy specifically covering use of social media?	Has the policy been proactively published?
Digital Safety Group							
Department of the Prime Minister and Cabinet	Not publicly known	Not publicly known	Highly unlikely	Yes, during the COVID-19 pandemic	No	Unknown	N/A
Firearms Safety Authority	Yes	Yes	Not publicly known	Not publicly known but unlikely	No	Yes	No
Inland Revenue	Yes	Yes	No	Yes	No	Yes	No
Ministry for Primary Industries	Yes	Yes	In limited circumstances with legal oversight	Yes, for searches of publicly available content	No	Yes	No
Ministry of Business, Innovation and	Yes	Yes	Yes	Yes	No	Yes	Yes

	General online searches that may yield publicly available social media information	Social media searches or engagement, including through use of persona accounts, but involving little to no direct interaction	Use of false persona to connect directly with individuals	Use of commercial tools	Account takeover with consent	Does the agency have a policy specifically covering use of social media?	Has the policy been proactively published?
Employment (MBIE) — Immigration NZ							
Ministry of Social Development	Likely yes	Yes	Unknown	Unknown	No	Pending	No
New Zealand Customs Service	Yes	Yes	No	No	No	Yes	No
New Zealand Police	Yes	Yes	Yes	Yes	Yes	Yes, multiple	Main policy on use of social media: no[86] Policy on account takeovers: no

[86] A redacted version of this policy was disclosed in response to a request under the Official Information Act, as detailed below.

	General online searches that may yield publicly available social media information	Social media searches or engagement, including through use of persona accounts, but involving little to no direct interaction	Use of false persona to connect directly with individuals	Use of commercial tools	Account takeover with consent	Does the agency have a policy specifically covering use of social media?	Has the policy been proactively published?
							Policy and framework on review of new technologies: yes

Police

New Zealand has a single centralised police service serving the whole country, with officers assigned to geographic districts. It can therefore issue policies that govern all policing staff in the country. The agency carries out a range of functions, including investigations, enforcement, counterterrorism, national security and intelligence collection, as well as coordination with other domestic agencies. In recent decades, it has increased its focus on intelligence while under pressures — familiar to other public sector entities in New Zealand and around the world — to reduce costs and boost efficiency, a state of affairs that often produces increased reliance on technological tools.[87] Police also ramped up their use of open source intelligence (OSINT) collection in the wake of the 2019 Christchurch terror attack; prior to that, according to public reporting, police used some OSINT tools but did not have capabilities focused specifically on open source collection.[88]

Police have both broad powers to use social media and access to a range of tools to facilitate these capabilities. Perhaps reflecting the benefit of having a single centralised service, the publicly available policies are stronger than most of the equivalent policies developed by local police departments in the United States, and the process for reviewing new technology, described herein, offers a robust approach to the promises and perils of new digital technology.[89] At the same time, police and the public would benefit from a holistic review of policies to ensure that they fit together coherently and are as privacy protective as possible, a commitment to public transparency to the fullest extent possible, and a collaborative exploration of the public licence for social media monitoring.

Policies

"Social Networking, Open Source Information and Online Practitioner" guidance

Chief among the policies guiding the police's use of social media data, both open source and otherwise, is the "Social Networking, Open Source Information and Online Practitioner" guidance.[90] The policy addresses various aspects of social media use, including: social media searches; the establishment, management and deconfliction of online personas; escalating levels of police online activity; administrative and data management matters; and overall organisational considerations. It builds in important guardrails, though it leaves some gaps, as described below.

The policy sets out five escalating levels of online activity, or "roles," with increasingly stringent levels of authorisation:[91]

---

[87] Lindsay, Angus, et al (2022), pp. 411–413
[88] Pennington, Phil, *RNZ*, 27 April 2021
[89] See Levinson-Waldman, Rachel (7 Feb. 2024-b), for a US comparison
[90] "Social Networking, Open Source Information and Online Practitioner" (2022). The New Zealand Police provided a less redacted version of the policy to the author. The majority of the discussion of this policy relies on the publicly available version, with references to several elements that appear in the version provided to the author, by permission of New Zealand Police.
[91] Ibid. pp. 7, 9–10

- Role 1: Overt Online. This stage entails conducting "general queries overtly online". It is authorised for police employees engaged in non-investigative activities such as public affairs, community policing or prevention. Assumed online identities are not used for this role.
- Role 2: Discreet Online Passive Operations. This is, according to the policy, "the most common role within Police." Employees playing this role "remain … passive" and do not engage directly with individuals online. While the policy permits employees to use an "overt identity" — one associated with their actual identity — if the risk of discovery is low, in practice overt identities are rarely if ever used for anything other than public-facing social media engagement, due to the risk that the employee will be identifiable. In almost all circumstances, therefore, Role 2 will entail the use of a false persona registered with the police. While the policy does not specifically indicate this, employees may also join Facebook groups using a persona account if there is a public safety interest in the members or in a discussion taking place in the group (for instance, regarding a crime surge or natural disaster) but will not interact directly with members.[92]
- Role 3: Discreet Online Active Operations. This role marks a shift from open source intelligence to "investigat[ing] crimes and gather[ing] intelligence using registered personas." Employees using personas at this stage will have backstopped their identities (that is, created a believable online history for their fake persona) and may "like" or make "passive comments" on posts but will not interact with individuals.
- Roles 4 and 5: Discreet Online Controlled Operations and Discreet Online Advanced Operations. Employees in these roles backstop their personas and may fully engage with individuals online.

Training is required for Roles 2–5.[93]

The policy contemplates the expanding use of false personas, noting that "[i]t is becoming increasingly necessary for trained staff to conduct targeted research of social media or other online forums, including … engagement with targets or POI's [persons of interest] using an assumed identity or persona."[94] The policy directs officers and supervisors to weigh the appropriateness of using an online persona by considering if it is "lawful, proportionate, and necessary in the circumstances," taking into account "legislative constraints and organisational risk."[95] Supervisors are directed to be aware of how online personas are used, including any groups they join.[96] If this is followed in practice, this is an important protection against overreach. The policy also nods to account takeovers, described in further detail below.[97]

---

[92] Correspondence with OSIG manager
[93] "Social Networking, Open Source Information and Online Practitioner" (2022), pp. 9–10
[94] Ibid. p. 6
[95] Ibid. Police also maintain a centralised database of online personas to ensure deconfliction, and the "owner" of the persona — the officer creating it — must both register the persona and obtain the appropriate level of approval: ibid. pp. 6–7. It is worth noting that Facebook's terms of service prohibit the use of false identities on the platform: see Letter from Facebook to Memphis Police Department (19 Sept. 2018)
[96] "Social Networking, Open Source Information and Online Practitioner" (2022), p. 7
[97] Ibid.

The policy also notes that the "*sharing* of information collected must abide by the principles of the Privacy Act 2020".[98] However, it does not address the Act's application to collection of information; instead, it acknowledges generally at the end that the Act "limit[s] what Police can lawfully do" with respect to using the internet "as a source of information and evidence."[99] To be sure, the Act provides broad licence to agencies to collect personal information for a lawful purpose that is necessary for an agency function.[100] But the statute does cover Police's collection activities, and this policy also addresses more than just publicly available information, calling into question whether its emphasis on sharing is adequate.

The New Zealand Police does have a separate policy on collection of information, but it is in broad terms, primarily tracking and reiterating the first four IPPs.[101] It generally advises police to be thoughtful about the information they are collecting — noting, for instance, that under IPP 1, information should be collected only if it genuinely needed, not if it is simply "nice to have".[102] This is a laudable value, though police have not always complied with it, as illustrated by the widely reported police practice of photographing of Māori rangatahi who were not suspected of engaging in criminal activity, which resulted in a joint inquiry by the Office of the Privacy Commissioner and the Independent Police Conduct Authority and the issuance of a compliance notice by the Office of the Privacy Commissioner.[103]

Consent to assume online identity

In 2021, reporting revealed that the New Zealand Police had a form allowing officers to fully take over an individual's online identity; according to a detective inspector with the service's Intercept and Technology Operations, the form had been used on a "regular basis" since 2012, largely in child exploitation investigations.[104] That form was quite broad; it permitted police to use the individual's online identity and accounts "for *any* purpose relating to an official investigation," including sending messages, accessing stored information, and using or disclosing any online information.[105] The form also required the signer to acknowledge that they were "relinquish[ing] all present and future claims" to the social media accounts listed and that the password would be changed to bar further access, raising concerns about potential misuse of this authority. In addition, defence counsel expressed apprehension that vulnerable people — including young people and those who felt under pressure or coerced by the police — might give consent under duress.[106]

The process was updated in 2022, and the new process is described here publicly for the first time. Police may now use one of two forms; one authorises police to assume an individual's online identity temporarily and the other authorises permanent account

---

[98] Ibid. p. 4 (emphasis added)
[99] Ibid. p. 13
[100] Privacy Act 2020, s 22
[101] "Collection of personal information" (n.d.)
[102] Ibid. p. 5
[103] *Joint inquiry by the Independent Police Conduct Authority and the Privacy Commissioner into Police conduct when photographing members of the public* (Sept. 2022)
[104] Espiner, Guyon, *RNZ*, 10 Nov. 2021; see also Crimes Act 1961, s 124A(2)
[105] *Consent to Assume Online Identity* (n.d.) (emphasis added)
[106] Espiner, Guyon, *RNZ*, 10 Nov. 2021

takeover. Both forms, which are attached as appendices to this report, lead with a section to document the specific identities, platforms/programs and passwords for the accounts that police are being authorised to use. The temporary consent form includes a section to specify the exclusive purposes for which police may use the individual's identity or accounts. It notes that police "may need" to change the account password and that they will make "every effort" to return the specified accounts once they are no longer required. By contrast, the permanent takeover form indicates that police will change the password and that the individual will entirely lose access to the account.

Both forms give police permission to use the accounts "to send and receive e-mails or carry out any other electronic communications and access any stored information," including photos and videos; for the temporary consent form, the activity must be relevant to the purposes specified. The temporary consent form also provides that while the authorisation may be revoked at any time, police may retain information that was obtained during their use of the accounts. Finally, both forms state that it is "not mandatory" to give consent for takeover and include a section requiring a parent or guardian to give authorisation for individuals under 16, neither of which appeared in the prior form.

These provisions address many of the concerns raised above, but it is impossible to judge the scope or appropriateness of their use in the absence of additional information, including how often they are used, what kinds of cases they may (and may not) be used for, data about any complaints filed, and measures in place to prevent explicit or implicit coercion outside the youth context. The New Zealand Police has indicated that the agency does not retain statistics about the use of the form. The agency also has a non-public policy governing account takeovers.

Account takeovers are not a per se inappropriate use of police power; it is not hard to imagine scenarios involving child sexual exploitation, cyberstalking or online scams in which it could be important for law enforcement to take on a victim's or other's persona, with consent. However, account takeovers are a deeply intrusive authority and they could be used to glean intimate information about the consenting individual or anyone they communicate with. Their use should be restricted to a small category of cases (as may be the case under the non-public policy); as the Law Commission and Ministry of Justice recommend in their joint report, robust oversight and auditing — necessitating records and statistics regarding the forms' use — and a public policy statement are critical as well.[107]

Review of new technologies

Between 2020 and 2022, the New Zealand Police introduced and refined a process to guide the trial and adoption of new technologies as well as the expansion of functionalities within an existing technology.[108] Decisions to launch a trial or adopt a new technology are guided by a set of ten technology-agnostic principles. They include

[107] Law Commission and Ministry of Justice (June 2017), pp. 296–298. The non-public policy, a largely redacted version of which was provided to the author, does have a section on "When to use" that may set out the types of cases for which takeovers are authorised.
[108] See *Trial or adoption of new technology — Police Manual chapter* (July 2022); "Trial or adoption of new policing technology" (n.d.), pp. 5, 7; *New Technology Framework* (2021)

a partnership principle, directing that if data will be collected or used, mechanisms must be in place "to ensure data is treated as taonga [treasure] and Māori sovereignty is maintained", and they require that Māori, Pacific peoples and other communities be consulted or involved in co-design.[109]

The policy directs police to pay particular attention to technologies that are "significantly based" on any of the following capabilities, which should encompass any new social media monitoring tool:

- AI or machine learning
- algorithmic risk assessments
- collection or analysis of data relating to individuals
- biometrics
- "the possibility of public place or online surveillance perceived or otherwise (irrespective of whether the provisions of the Search and Surveillance Act are considered to apply)."[110]

The policy directs that because these technologies "are likely to be inherently higher-risk … application of the policy to them should be considered the default position."[111] Tools that have an algorithm as a central aspect must be vetted against additional checklists, depending on whether the algorithm is internally developed or created by a third party.[112] The framework document puts a thumb on the scale in favour of review, advising that "where there is any room for doubt, the policy should be assumed to apply."[113]

The process is fairly robust; if it is followed in practice, it should contribute significantly towards ensuring that new and expanded technology deployments are grounded in principles of ethical and equitable decision-making. Notably, it does not apply to technologies that were in place at the time of the framework's adoption (and are not being expanded), including existing social media monitoring practices. If police roll out a new tool to assist with social media monitoring, however, particularly an algorithmically driven product, it should trigger review under the framework.

Open Source Intelligence Group

The Open Source Intelligence Group (OSIG), which sits within the New Zealand Police's National Intelligence Centre, plays a key role in the agency's use of social media.[114] OSIG serves "customers", or teams, within the New Zealand Police; it responds to requests for support and may initiate work on its own where an individual or team within the Police has expressed interest in the area. It might, for instance, identify a concerning trend online and then conduct further inquiries if a team indicates it wants more information. It may also support police response to major events or

[109] *New Technology Framework* (2021), p. 8
[110] "Trial or adoption of new policing technology" (n.d.), p. 7
[111] Ibid.
[112] *New Technology Framework* (2021), p. 19
[113] Ibid. p. 5
[114] This section is largely based on interviews and correspondence with the OSIG team manager.

significant investigations, depending on resource availability. District offices also have intelligence analysts that handle matters at that level, though OSIG at times assists with investigations that start at the district level. In general, OSIG does little "monitoring" of social media; most of its work is tailored to specific needs.

OSIG focuses a significant proportion of its work on supporting the department's national security mission through the National Intelligence Centre. OSIG might, for example, profile the online activities of a person who has come to the police's attention because of behaviour that appears to implicate national security; in this case OSIG's efforts would be one piece of a larger system that could include schools, family, mental health professionals, police engagements and others.

OSIG uses social media in a range of other ways as well, though they represent a minority of its efforts. Case studies shared by OSIG include:

- helping police identify a driver who had uploaded multiple videos to social media that showed high-risk driving behaviours: OSIG analysed the driver's social media handles and online interactions to assist in identification
- assisting with missing persons efforts during Cyclone Gabrielle in February 2023: while conducting research online, OSIG staff identified a social media community that was keeping a list of people marked safe. OSIG contacted the administrators to request access to the list, which they cross-checked against the police's list of missing persons to focus official search and rescue efforts more precisely
- identifying a suspect in a sexual assault case who was known only by a nickname and a social media handle that was connected to an account that had been deleted: OSIG's open source research uncovered a second social media account linked to the first and provided other corroborating information, enabling identification of the suspect and subsequent police action
- geolocating video footage from a rural location in support of an investigation into a serious crime; the geolocation data was used to confirm the location of the suspect and their associates at a point that was relevant to the commission of the crime
- identifying anonymous users who had purchased chemicals online that could be precursors to making explosives: this included one user whose social media posts indicated he was buying the chemicals for educational purposes, exempting him from possible investigative follow-up.

One other case study is illustrative. In March 2023, British anti-transgender activist Kellie-Jay Keen, who goes by the name Posie Parker, planned to travel to Australia and New Zealand for a series of public events under the banner "Let Women Speak". As a result of opposition by New Zealand rainbow communities, political leaders and others, border and immigration authorities conducted an inquiry into whether she posed a risk to the public order or public interest, which would have justified blocking her from the country.[115] To support the determination, police produced an intelligence notification that drew on social media to assess the dates and locations of the New

[115] See, e.g., *RNZ*, 22 March 2023

Zealand events and to identify the individuals and organisations that might attend in support as well as the details and organisers of a counter-protest.[116]

The police analysis, including the posts cited, appear focused primarily on assessing the likelihood of violence from the organisers or counter-protestors, as well as the likelihood that the events would still occur even if Parker were denied entrance to the country; this is largely in line with what I believe to be best practice for law enforcement use of social media to assist with planning in advance of potentially resource-intensive events.[117] It is worth noting, however, that an intelligence notification, fixed in time, can offer an incomplete narrative. While it singles out the nationwide transgender organisation Gender Minorities Aotearoa as a supporter of the counter-protest,[118] for example, many other allied organisations posted about the protest after the notification was compiled and thus were not included. This is not a critique of the notification itself; it does highlight that such notifications should not subsequently be used by police or others for alternate purposes.

More generally, these case studies highlight the importance of public visibility of both policy and practice. People may have different opinions, for instance, on what is "intrusive": would they prefer to have the police view their social media to determine whether they are within or outside of the scope of a criminal investigation, potentially sparing them an in-person visit but giving the analyst an intimate view of aspects of their personal life, or would they prefer to have police contact them directly, allowing them to address the specific concern but also producing the anxiety that comes from law enforcement interaction (and questions from nosy neighbours)?[119] There is not a singular answer, but it would benefit both police and the public to explore these questions, to articulate more clearly the boundaries of the police's social licence in this realm.

Third-party tools

Police have used a range of commercial tools in this area, though they may use a given tool for a narrower set of purposes than the range of capabilities for which it is advertised.

In a 2021 response to a request under the Official Information Act 1982, police disclosed that the New Zealand Police was using or trialling at least three tools to search publicly accessible social media pages during investigations.[120] The response provided scant information on what the tools were, however, based on the somewhat dubious assertion that providing almost any information about police methods would enable criminals to "hinder or defeat police investigations" and "harm the community and the public interest."[121] The response did briefly enumerate several uses of relevant data tools (though the New Zealand Police declined to provide significant additional

[116] "Intelligence notification: Let Women Speak tour" (17 March 2023)
[117] Levinson-Waldman, Rachel (7 Feb. 2024-a)
[118] "Intelligence notification: Let Women Speak tour" (17 March 2023), p. 4
[119] This also implicates IPP 2, directing agencies to collect information directly from the individual concerned (though exempting publicly available information): Privacy Act 2020, s 22
[120] Pennington, Phil, *RNZ*, 14 June 2021; *Response to Official Information Act request from Phil Pennington* (27 May 2021)
[121] *Response to Official Information Act request from Phil Pennington* (27 May 2021)

information, on the grounds that doing so was likely to prejudice the maintenance of law):

- From 2018 to 2020, the Cybercrime Unit "had access to a social media tool that searched accessible and open source internet pages" in order to assist with investigations.
- In 2019, police signed a contract with a "data analytics provider" to assist with responses to the 2019 Christchurch terrorist attack and to help respond to the Royal Commission of Inquiry.
- In November 2019, the National Intelligence Centre "introduced software that searches accessible and open source internet pages including social media"; according to the response, the OSINT team and Cybercrime Unit use this tool to help with investigations, support intelligence analysis and plan for major events. Although not specified, this appears to be the kind of tool that the police would have used during the 2022 Parliament protests, when police monitored publicly available information and communications on social media.[122]

Police also considered the use of a tool that would help them understand "attitudes, opinions, and general sentiment" through monitoring of various online channels.

The response noted that the police had previously disclosed the use of several tools, including:

- Signal AI, which was being used by the National Command & Coordination Centre, by some police districts and by teams in the National Intelligence Centre, including the OSINT team, to "surface social media posts as well as to identify trend information relating to public safety and criminal events". The use of Signal AI had been revealed as early as 2013, when it was described as being focused on "high-profile public events and emergencies."[123] Mark Evans, then New Zealand Police's director of intelligence, said at the time that it could be used to gather evidence or support investigations but was not typically used that way. He described its primary use as searching key words in specific geographical areas on publicly available social media posts in advance of significant public events or natural disasters.[124]
- Maltego, used by the Cybercrime Unit to "query open source data and visualise it in graph form," with a particular focus on "mapping internet infrastructure".
- Feedly, which "searches exclusively across publicly available information". This tool was in use by the OSINT team and could be used by the Cybercrime Unit to "collect information from online open source to assist with an investigation or support an intelligence report".

Another Official Information Act request from around the same time revealed that the Police OSINT team and the High Tech Crime Group were using a software system to

---

[122] *The Review: Policing of the Protest and Occupation at Parliament 2022* (April 2023), pp. 22, 36, 57, 61, 69

[123] Fisher, David, *New Zealand Herald*, 23 Feb. 2013; see also "NZ police case study: Social media opens up a new world of real-time intelligence" (6 Jan. 2014)

[124] Fisher, David, *New Zealand Herald*, 23 Feb. 2013

"draw on internet-based open sources to collect open-source information," but Police declined to provide any additional information, again on the grounds that doing so was "likely to prejudice the maintenance of law".[125]

Scraps of information can be gleaned from additional sources. Media reporting following the joint Office of the Privacy Commissioner / Independent Police Conduct Authority investigation of police officers taking pictures of predominantly Māori youth, for instance, suggested that officers were downloading pictures of youth from social media, though public reporting has revealed little additional information about the circumstances for doing so or any relevant guardrails or policies.[126] In addition, while there was widespread speculation that police had access to Cobwebs, a third-party social media monitoring tool used by Immigration New Zealand (described below), this has never been confirmed.[127]

In addition, in 2021, police considered trialling a tool called Zavy, which would have analysed the tone and content of social media posts to assess public sentiment about police.[128] The New Zealand Police's Expert Panel on Emergent Technology critiqued the proposal on the grounds that comments on a Facebook page would not be representative of the values or sentiments of New Zealanders as a whole; that the tool would collect individually identifiable information; and that the harms of intruding into individuals' privacy and undermining public trust in the Police outweighed any value from what was essentially brand research.[129] In response to concerns from the panel and the Office of the Privacy Commissioner, police ultimately decided not to move forward with a trial.[130]

Gang policing

One issue into which the public has little insight is whether and to what extent police use social media to identify, track or monitor gang members and their associates. In the United States, many local and state police departments turn to social media to help identify gang members and to build gang databases.[131] These efforts, which have been criticised for being inaccurate and biased, can include using social media to identify "associates" of gang members based on pictures depicting them together at a party.[132] Third-party social media monitoring tools have also been used in the US to designate individuals as gang members; employees of one company, Dataminr, reported that staff members there had scrutinised thousands of social media posts to determine who should

---

[125] *Response to Official Information Act request from Scott* (27 April 2021)
[126] Cardwell, Hamish, *New Zealand Herald*, 8 March 2023
[127] Pennington, Phil, *RNZ*, 9 Nov. 2023-a
[128] "Zavy proposal — we asked, they said, we did" (n.d.)
[129] Ibid.
[130] Ibid.
[131] See, e.g., Andino, Carlos (17 Feb. 2022) ("MPD admitted that over the last 13 years it built its Gang Tracking and Analysis System … by secretly surveilling D.C. residents, in-person and over social media."); Judd, Alan, *GovTech*, 9 March 2020 (noting that Georgia includes posting "gang material" on social media as a factor in designating someone as a gang member); Rivlin-Nadler, Max, *The Appeal*, 19 Jan. 2018 (documenting a police officer's identification of a young man as a gang member based on photos and tweets on his social media feed, as well as the officer's testimony that statements on the youth's behalf were irrelevant to character determinations because "We look at what they put on social media.")
[132] Popper, Ben, *The Verge*, 10 Dec. 2014; Robinson, Sara (6 July 2018)

be listed as a gang member, guided by little more than extremely loose guidance, their own instincts and input from predominantly white former law enforcement officers.[133]

It is unclear how widespread these methods are in New Zealand. While an in-depth comparison of the gang landscape in the United States and New Zealand is outside the scope of this report, some surface-level differences may be salient. In the United States, ostensible indicia of gang membership range from hand gestures to tattoos to clothing colours or styles, inviting police to exercise outsized discretion in identifying someone as a gang member. In New Zealand, by contrast, almost all gang members are "patched", meaning they wear patches on their jackets, making identification of active gang members a more straightforward process.

At the same time, while the research does not show a clear trend, reporting suggests that New Zealand gangs may be expanding their use of social media, which could make social media a tempting source for intelligence gathering.[134] A 2022 parliamentary report on gang membership articulated the factors that could be used to add individuals to the Police National Gang List, which included "intelligence from operations"; the report does not clarify whether that includes social media intelligence.[135]

One recent parliamentary gang-policing proposal seeking to limit the public display of patches would have banned gangs from posting insignia on social media.[136] The social media prohibition was eventually removed, but the Bill still includes a provision that allows district courts to issue orders banning gang offenders from "consorting" with each other under certain circumstances.[137, 138] While the Bill does not specify how a breach of a non-consorting order would be discovered, social media would be one way to search for gang offenders spending time together.

Moreover, as the New Zealand Council for Civil Liberties pointed out, while the Bill carves out certain activities from the coverage of non-consorting orders, including spending time with immediate family members, it does not exempt attending a protest, activity that is protected by BORA and for which social media would be a rich lode of information.[139] Using social media to mine data about who is in violation of a non-consorting order will also invite police to dig further into people's lives to determine, for instance, who is an "immediate" family member and who is perceived as more distant, and will have an outsized impact on Māori, in light of the disproportionate

---

[133] Biddle, Sam, *The Intercept*, 21 Oct. 2020

[134] See, e.g., Gee, Samantha, *Stuff*, 28 May 2021; Yalden, Phillipa, *Stuff*, 16 Aug. 2018; Leask, Anna, *New Zealand Herald*, 29 June 2023; McCann, Mitch, *Newshub*, 23 Aug. 2020; but see *Toward an understanding of Aotearoa New Zealand's adult gang environment* (June 2023), p. 52 ("While international research suggests that some gangs have used the internet to commit or promote criminal behaviour, to coordinate street-level illegal activities, or to effectively keep a digital score of which gang is 'winning' in any given turf war, the extent to which this is true for NZAGs [New Zealand Adult Gangs] is not clear.")

[135] *New Zealand Gang Membership: A snapshot of recent trends* (July 2022)

[136] See *Checkpoint*, 25 Oct. 2023 (noting that the proposal was inspired by a western Australia law that included a specific ban on posting gang insignia online). The New Zealand Police Commissioner also recently announced the planned creation of a new National Gang Unit: "Police to establish new National Gang Unit and frontline teams to increase pressure on gangs" (14 May 2024)

[137] Maher, Rachel, *New Zealand Herald*, 12 June 2022; see also Desmarais, Felix, *1News*, 7 March 2024

[138] Gangs Legislation Amendment Bill, cl 19(1). Breaches of non-consorting orders can incur a prison term of up to five years or a fine of up to $15,000. Ibid. cl 23

[139] "Submission: Gangs Legislation Amendment Bill" (6 April 2024)

representation of Māori in New Zealand gangs.[140] And while the ban on posting gang paraphernalia online died, the offence of posting offending behaviour online was made an aggravating factor in sentencing in mid-2023, giving criminal justice agencies an extra incentive to pay attention to social media.[141]

Accident Compensation Corporation

The Accident Compensation Corporation (ACC) provides support to help anyone in New Zealand who is injured in an accident. Conversations with ACC staff indicate that ACC takes a very cautious approach to use of social media to detect possible fraud by claimants — driven, in part, by the aftermath of a well-publicised privacy breach in 2021.[142] ACC does not use pseudonymous accounts or commercially available social media monitoring tools and does not proactively monitor or search social media.

If ACC receives an allegation that a client is engaged in an activity that could affect their receipt of ACC benefits, and the complaint cites to or references a social media post, ACC staff will begin by verifying the legitimacy of the post, without looking further on social media or googling the client, so as to avoid introducing bias into their assessment of the complaint or the client. Staff will then directly contact the client to notify them about the allegation and learn more. If the client directs ACC to additional social media posts to contextualise or refute the allegation, ACC will look to those posts but will not explore further without the client's permission. All social media searches, even with a client's consent, require manager approval. ACC has a policy to guide use of social media, but it is not publicly available.[143]

Staff indicated in correspondence that ACC also has some limited discretion, with suitable governance approvals and oversight, to conduct open-source information gathering without the knowledge of the person concerned where there are clear indications of organised crime or serious offending or other extenuating circumstances.

Classification Office

The Classification Office is responsible under the Films, Videos, and Publications Classification Act 1993 for restricting or banning content appearing in films, videos, or publications that is "objectionable" or harmful to the public good; that content may include social media posts.[144] The Office has, for instance, banned the livestream of the 2019 Christchurch terror attack and the manifesto published by the perpetrator, as well as the same materials from the 2022 Buffalo, New York copycat supermarket massacre

---

[140] *New Zealand Gang Membership: A snapshot of recent trends* (July 2022)
[141] "System shake-up to tackle youth and gang crime" (17 July 2023); Ensor, Jamie, *Newshub*, 17 July 2023
[142] See *RNZ*, 15 June 2022
[143] ACC's transparency statement, issued pursuant to the Public Service Commission's Model Standards, does not address use of social media except by oblique reference, stating that ACC's Integrity Services "may also collect and use publicly available information [including "publicly available internet information"] … where this is relevant to carrying out our compliance functions." *Transparency Statement — Integrity Services (Information gathering and public trust)* (n.d.)
[144] "Our role" (n.d.); see also Films, Videos, and Publications Classification Act 1993; "The classification process" (n.d.)

that cited the Christchurch manifesto.[145] In classifying content appearing on social media, the Office is guided by factors including whether the content has a nexus to New Zealand or will pose a significant harm to New Zealanders, as well as the impact of classification on freedom of expression. It also classifies child sexual abuse material and collaborates on removals of such material.[146]

Once material is classified as objectionable, individuals who distribute it can be penalised, including via monetary fines and incarceration; the Department of Internal Affairs, New Zealand Police and the New Zealand Customs Service prosecute non-compliance.[147] The Classification Office can also recommend to platforms that material be taken down and may issue takedown orders as a last resort. It does not impose any filtering; some child sexual abuse material is voluntarily filtered at the internet service provider level, and other materials may be added to voluntary user-level filters, such as parental or school filters.

Because the Office does not have an investigative or enforcement function, it typically does not affirmatively undertake social media monitoring. It may receive information from the public or a referring agency about relevant content on social media (as it did in the context of the Buffalo shooting) and may turn to social media to aid in the classification process, including to determine whether material is likely to have a significant impact on a New Zealand audience. In short, as one staffer described it, while the Office cannot look for things proactively, it can look for something it has heard about. The Office does not have a standalone policy covering its use of social media.

Department of Corrections

The intelligence team at the Department of Corrections is guided in its use of social media by a set of operational guidelines that are not publicly available, as well as by the Department's intelligence priorities.[148, 149] The guidelines outline several tiers of social media use for risk assessment; the department does not use social media for investigations. The team can collect intelligence, including through social media, where it is related to individuals under the Department's management or in circumstances in which there is a threat to the safety, security and good order of a prison. Corrections staff may also request assistance from other agencies, such as the New Zealand Police,

---

[145] "Classification Office response to the March 2019 Christchurch terrorist attack" (9 Dec. 2020); "Buffalo mass shooting livestream and 'manifesto' permanently banned" (15 June 2022)

[146] "About the Classification Office" (n.d.)

[147] "Plain English guide to offence provisions in the Films, Videos, and Publications Classification Act 1993 and its Regulations" (2015); "Enforcement, offences and penalties" (n.d.)

[148] The information in this section is largely based on communications with Corrections staff. As of February 2023, there were three primary areas in which the Intelligence team contributed to national security: organised crime; violent extremism, including trend identification; and "response to nationally significant events", including natural disasters like earthquakes and the COVID-19 pandemic. "National Security & Intelligence: The Role of Government Agencies" (Feb. 2023), p. 4

[149] The Department of Corrections' transparency statement, issued pursuant to the Public Service Commission's Model Standards, also includes some information about the Department's use of social media: "Corrections does employ social media platforms to gain intelligence about individual offenders in a lawful manner, and may monitor groups, such as criminal gangs, to protect our people, information and places." "Our privacy and transparency commitment" (n.d.)

and may obtain assistance from the Department of Internal Affairs on online trend identification.

A Bill introduced in June 2023 would expand the Department's statutory functions, enabling it to monitor, collect and use "open source information", which would include social media, when a two-part test is met. First, the Department must believe such action to be "reasonably necessary for an intelligence purpose," which covers the identification of risk, the deterrence and prevention of harm and support for the "good order, safety, and security of prisons."[150] Second, it must be targeted only at "individuals who present a serious risk of harm to the good order, safety, and security of prisons or to public safety."[151] The Minister's justification memo to the Cabinet committee suggests that this would be focused on posts or other activities from prisoners themselves and that it would represent an expansion of the Department's current authority.[152]

Department of Internal Affairs

The Department of Internal Affairs does not have a standalone policy on use of social media, though its transparency statement provides some generic information.[153] The Department's Digital Safety Group enforces classification and censorship decisions regarding "objectionable" material under the Films, Videos, and Publications Classification Act 1993, including with respect to online violent extremism.[154, 155] The group's Digital Violent Extremism Team learns about potentially objectionable online content through one or more of several mechanisms: an online reporting form, domestic and international governmental and non-governmental entities, and scanning of online

---

[150] Corrections Amendment Bill (see Explanatory Note and proposed ss 127A and 127B)

[151] Ibid. (see Explanatory Note and Subpart proposed s 127H)

[152] See "Proposed amendments to the Corrections legislative framework regarding improved safety, rehabilitation and reintegration outcomes" (9 Dec. 2022), p. 3 ("It is likely that in time prisoners will gain access to regular use of digital technologies, yet Corrections currently has no power to monitor them").

[153] The statement indicates that the Department "collect[s] information from a wide variety of sources in both physical and digital environments. These sources include … information from online sources (including websites, social media, and public registers)". More generally, the Department may "collect publicly available information — for example from social media, news reporting, and press releases — where this would assist us in carrying out any DIA functions, including to verify information that is collected by other means." It is not clear how, if at all, these two methods of collection differ from each other. "Transparency statement" (n.d.-b)

[154] The Digital Safety Group plays four main regulatory roles: prevention and harm reduction (for instance, public education), intelligence and insights (including trend analysis and assessing connections between online and real-world events), investigations (based on overall trends and referrals) and prosecutions. The Department of Internal Affairs also has a significant role in fighting the trading and spread of child sexual abuse material online, which is not addressed here; see, e.g., "Operation H Case Study" (n.d.).

[155] A publication is "objectionable" if it "describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good": "Objectionable and restricted material" (n.d.). Material that "promotes criminal acts or acts of terrorism" is likely to be categorised as objectionable. Factors including "the character of the publication, including any merit, value, or importance that the publication has in relation to literary, artistic, social, cultural, educational, scientific, or other matters" are also taken into consideration in some circumstances: Films, Videos, and Publications Classification Act 1993, s 3

platforms using "specialist tools and techniques."[156] After receiving a referral, Department of Internal Affairs staff will look online to determine the legitimacy of the complaint and the severity of the flagged material; the Department can also ask the Classification Office to classify the content and determine whether it is objectionable.[157] To be objectionable, material must have a New Zealand nexus or adversely affect New Zealanders.

When the Department identifies material that violates the Act, it can use collaborative mechanisms like trusted flagger programmes and in-platform reporting systems, formal takedown notices, and criminal warnings and prosecutions.[158] It also coordinates with international partners in responding to online aspects of violent events that are tied to or inspired by events in New Zealand.[159] It does not use AI-driven tools and does not scrape data.[160] The Department of Internal Affairs also assists other agencies with online trend identification.

In addition, the Digital Safety Group coordinates New Zealand's Online Crisis Response Process, which was developed primarily to respond to content arising from acts of terrorism or violent extremism and aims to keep such content from going viral.[161] The Process is activated "when a piece of significantly harmful online content (which is highly likely to be objectionable) is spread rapidly and widely (both geographically local and/or across multiple platforms) and is likely to create significant harm to New Zealanders who are exposed to it."[162] This material can be identified through a variety of mechanisms, including ordinary online scanning by other agencies.[163] Once a major crisis is declared, the Department of Internal Affairs can undertake increased online monitoring to "understand the type of content that is trending and that may present a risk of harm to the New Zealand public."[164] The Department may also prosecute illegal content that violates the Films, Videos, and Publications Classification Act or serve takedown notices to international websites.[165]

---

[156] "About the Digital Safety Group" (n.d.); "How NZ responds to violent extremism online" (n.d.). In 2023, the most referrals were for URLs on Twitter, and the vast majority of all referrals of identity-motivated violent extremism related to white identity: *Digital Violent Extremism Transparency Report* (2023), pp. 17–18

[157] See "How NZ responds to violent extremism online" (n.d.)

[158] *Digital Violent Extremism Transparency Report* (2022); *Digital Violent Extremism Transparency Report* (2023), p. 23

[159] *Digital Violent Extremism Transparency Report* (2023), p. 9

[160] Data scraping is the practice of using a computer program to extract large amounts of data from a website. See "What is Data Scraping?" (n.d.)

[161] *New Zealand Online Crisis Response Process* (n.d.), pp. 3–4. The Online Crisis Response Process was not activated in 2023: *Digital Violent Extremism Transparency Report* (2023), p. 8

[162] *Digital Violent Extremism Transparency Report* (2023), p. 8

[163] *New Zealand Online Crisis Response Process* (n.d.), p. 4 (referring to agencies' "business as usual activity in the online space")

[164] *Digital Violent Extremism Transparency Report* (2022), p. 8; see also *New Zealand Online Crisis Response Process* (n.d.), p. 5 (describing the factors considered in the process of assessing risk to the public)

[165] *New Zealand Online Crisis Response Process* (n.d.), pp. 10–12

Department of the Prime Minister and Cabinet

The Department of the Prime Minister and Cabinet provides advice and support to the Prime Minister, Cabinet and Governor-General. Early in the COVID-19 pandemic, the Department commissioned a company called Annalect to monitor comments posted publicly on Facebook, Twitter, Reddit and other social media sites and produce "Social Listening Reports".[166] The contract was not revealed until 2022. The reports, which were produced twice a week between April 2020 and April 2022, included screenshots of individual comments on "Unite Against COVID-19" social media channels and direct messages to the Department. The Department of the Prime Minister and Cabinet described the comments as being anonymised, but some reports included direct quotes from public comments, which would not have been difficult to re-identify, as well as thumbnail-sized photos of commenters.[167] While these comments evidently helped to gauge public sentiment about topics such as vaccinations and the "traffic light system" used to inform the level of restrictions in place during the pandemic, one expert warned that revelations about surreptitious monitoring would fuel distrust in government and that public social media comments were highly unlikely to be statistically representative of New Zealanders.[168]

Firearms Safety Authority

The Firearms Safety Authority, which was established in late 2022 in response to the Christchurch attacks, oversees the process for determining whether to grant an application for a licence to carry a firearm, including an assessment that the applicant is a "fit and proper person" of "good conduct and character."[169, 170] The Authority is authorised to consider an applicant's "overall character and conduct" through reference to information held or received "from any source", without limitation.[171] Prior to the establishment of the Authority, the New Zealand Police indicated that its fitness evaluations could include reviewing online activity, and the Royal Commission of Inquiry into the masjidain attacks suggested that the perpetrator's firearm license could have been revoked by police on the basis of his social media comments.[172, 173]

Inland Revenue

Inland Revenue is New Zealand's tax-collection agency. Inland Revenue disseminates internal staff guidance on use of social media, but does not have a publicly available

---

[166] Todd, Katie, *RNZ*, 30 April 2022
[167] McNamara, Kate, *New Zealand Herald*, 8 June 2022
[168] McNamara, Kate, *New Zealand Herald*, 12 May 2022 (quoting Lara Greaves, senior lecturer in New Zealand politics at Auckland University)
[169] "Launch of Te Tari Pureke — Firearms Safety Authority" (30 Nov. 2022)
[170] "Before you apply for a firearms licence" (n.d.)
[171] Ibid.
[172] Pennington, Phil, *RNZ*, 16 March 2019
[173] See "Chapter 2: The three ways the individual may have been detected" (8 Dec. 2020) (noting that if the attacker's Facebook comments had been attributed to him, and it was learned that he held a New Zealand licence, those factors could have "justified further investigation, perhaps initially as to his suitability to hold a firearms licence.")

policy on social media.[174] It also does not specifically train staff on the use of open-source social media. While there are few publicly available details about Inland Revenue's use of social media for information collection, Inland Revenue staff were able to provide some insights. Broadly speaking, Inland Revenue uses social media for two purposes: targeted inquiries and intelligence-related scanning.

In the first category, Inland Revenue staff may look for information about a specific individual or organisation as part of an investigation or audit, including to corroborate a tip received from the public. Staff may look at both the content of an individual's posts and their online connections to determine, for instance, whether they are posting about work for which they are not paying taxes or selling items to a person who appears to be violating tax laws. Staff may not conduct "fishing expeditions", use covert accounts or lie about their identity, and they are required to verify the accuracy of online information.

In the second category, Inland Revenue's intelligence team scans social media to assist with tasks like sentiment analysis and future planning, both conducting its own collection and analysis and using third-party tools. It may also obtain data sets from other agencies (subject to written agreements) and companies to assist with network analysis. The intelligence team does not use covert accounts but can share information with the New Zealand Police or Department of Internal Affairs under an information-sharing agreement if one of those agencies needs to undertake covert activity for an investigation.

Ministry for Primary Industries

The Ministry for Primary Industries focuses on protecting New Zealand's fisheries, forests, agriculture, food safety and biosecurity. It has authority to enforce its laws through criminal investigations and prosecution, including in coordination with the New Zealand Police, MBIE, Maritime NZ, and other central and local government agencies, and it uses engagement and outreach to educate members of the public and address lower-level violations. Its use of social media is primarily focused on risk identification rather than individual targeting. It has internal policies and procedures governing its staff's use of social media, but they are not published.[175] The Ministry's privacy and transparency statement, published in response to the Public Service Commission's Model Standards, also provides useful information about its use of social media; it is one of the more fulsome of the various agency transparency statements.[176] According to the statement, Ministry for Primary Industries staff may undertake "open … searching of information" where no password or account registration or login is required — for instance, through a Google query — without formal approval as long as it is for work purposes. It also addresses undercover use of social media, noting that covert use:

---

[174] Inland Revenue's online privacy policy briefly mentions that the agency "collect[s] information that is publicly available, for instance on open source websites", and that the information may be used for intelligence purposes. "Our privacy policy" (n.d.)
[175] The information in this section is largely based on communications and correspondence with staff.
[176] *MPI Privacy and Transparency Commitment* (n.d.)

> to support regulatory, compliance and enforcement work, such as use for active engagement with individuals online without identifying the staff member or the Ministry, is restricted to staff with specialist knowledge, experience and competence, and requires case-by-case approval by relevant senior staff.

Ministry staff may also draw information from social media if there is reasonable cause to suspect a threat to staff or the public.

The Ministry's fishery officers may use social media in several different ways, including conducting keyword searches on open social media and joining Facebook groups under clearly identified Ministry for Primary Industries profiles to conduct engagement, outreach and education through public posts and direct messages. Officers may spot issues on Facebook groups, including low-level and even inadvertent infractions, such as a Facebook post advertising for sale a few fish that were caught within the legal limits, as well as higher-level violations, such as repeat offenders or large-scale black market fishing operations. Surveillance and incursion investigators working under the Biosecurity Act 2015 may also use social media for public education and to support engagement — for example, in cases of an invasive or regulated plant species inadvertently put up for sale.

The Ministry for Primary Industries does not currently use automated tools, though its Emerging Risk Team uses an external provider to support searches of publicly available content from publicly available internet sources (e.g., news media publications, science literature, op-eds and reviews) to improve the Ministry's intelligence function, particularly in the area of food safety.[177]

Ministry of Business, Innovation and Employment — Immigration New Zealand

MBIE has been the subject of significant reporting about the use of social media by Immigration New Zealand, which sits within the Ministry. The reporting raised two high-profile issues: use of third-party social media monitoring tools and use of fake social media personas.

In 2022, reporting revealed that Immigration New Zealand had signed a contract two years earlier with Cobwebs, a software tool that scans open social media sites, including Twitter, Facebook, Instagram, Reddit, Tumblr, LinkedIn, Snapchat and WhatsApp.[178] The capabilities of Cobwebs — which later reporting revealed the Ministry had not used in a live setting for the first two years of the contract[179] — would have represented a significant force multiplier for the agency, which had previously relied for its research and analysis on standard online search engines that offered far less sensitive and sophisticated search capabilities.[180] While the contract itself was not disclosed, it evidently required Cobwebs to leave no trace of its monitoring and data collection.[181]

---

[177] According to the Ministry, the provider is classified as compliant with the General Data Protection Regulation, the EU's information privacy regulation.

[178] Pennington, Phil, *RNZ*, 12 Oct. 2022

[179] Pennington, Phil, *RNZ*, 9 Nov. 2023-a

[180] Pennington, Phil, *RNZ*, 14 Oct. 2022

[181] Pennington, Phil, *RNZ*, 12 Oct. 2022. Meta — which owns Facebook and Instagram — had previously ejected accounts operated by Cobwebs and some of its clients on the grounds that they "engaged in

MBIE ultimately released information about Cobwebs under the Official Information Act in response to an intervention from the Office of the Ombudsman, but redacted the vast majority of the documents.[182] One document indicated that Cobwebs stores the data it collects and sends it to analysts in Immigration New Zealand's Intelligence Unit, a team that historically contributed to national security and law enforcement and was expanded in 2023 to focus broadly on national security and intelligence.[183, 184] Under some circumstances, the data could also be shared with "border partners" and other New Zealand government agencies, though as of late 2022 no data had been shared with the US, Canada, the UK or Australia, the rest of the so-called "Five Eyes" nations.[185, 186]

The unredacted portions of the documents did not clarify who would be targeted or the specific purposes for which Cobwebs would be used, though New Zealand's Immigration Minister told the press that a small number of immigration officers were using it to screen visa applicants for risks like involvement in international crime, child sexual exploitation or violent extremism, and that it was not used to facilitate fake accounts.[187] The Ministry did not publicly disclose any steps it was taking to ensure that this screening function did not incorporate bias or to test, for instance, whether the screening was disproportionately targeted at Muslim or Pacific applicants for immigration. In 2023, MBIE belatedly revealed that its sole purpose for acquiring Cobwebs was to help detect and prevent a "mass arrival" on the shores of New Zealand.[188]

Cobwebs had previously told RNZ that it was inspired by the 2019 Christchurch mosque attacks to put together a "dashboard" mapping the potential local impact of major global incidents, though the public reporting does not reveal whether any New Zealand agency commissioned or used this product or what practical value it added.[189] Notably, while the Ministry did conduct a privacy impact assessment early in its deployment of the technology, it did not consult with the Privacy Commissioner prior to signing with Cobwebs or notify the immigration minister.[190] In addition, although the Ministry has said publicly that its use of Cobwebs was subject to internal monitoring and audit, as well as external oversight by the Office of the Privacy Commissioner, there are scant publicly available details, and the Ministry is not subject to inspector general oversight.[191, 192] While the tool was used several times before immigration staff were trained to use it, a monitoring group set up in February 2023 concluded that the previous uses were justified.[193] As of November 2023, the tool had

---

social engineering to join closed communities and forums and trick people into revealing personal information" and were used to target activists, opposition politicians and government officials in several countries. Dvilyanski, Mike, et al (Dec. 2021). There is no evidence that MBIE used the tool this way.

[182] Pennington, Phil, *RNZ*, 12 Oct. 2022

[183] Pennington, Phil, *RNZ*, 12 Oct. 2022

[184] Pennington, Phil, *RNZ*, 4 Oct. 2023

[185] Pennington, Phil, *RNZ*, 12 Oct. 2022

[186] Pennington, Phil, *RNZ*, 4 Dec. 2022

[187] Pennington, Phil, *RNZ*, 14 Oct. 2022

[188] Pennington, Phil, RNZ, 4 Oct. 2023

[189] Pennington, Phil, *RNZ*, 14 Oct. 2022

[190] *RNZ*, 20 Oct. 2022; Pennington, Phil, RNZ, 4 Dec. 2022

[191] *RNZ*, 23 Oct. 2022

[192] Pennington, Phil, *RNZ*, 9 June 2024

[193] Pennington, Phil, *RNZ*, 9 Nov. 2023-a

been used sparingly: a total of six times in the prior 18 months, "to investigate leads at … scale".[194, 195] The contract was not renewed in April 2024, though it has been reported that MBIE is looking for a new provider to take its place.[196] The Ministry has also refused to reveal any details about the cost of its contract, citing security needs, its negotiating position and Cobwebs' commercial interests.[197]

In addition, MBIE revealed in September 2017 that Immigration New Zealand was using fake social media personas for purposes including assessments of "reputational and national security risks", investigations of potential migrant exploitation and verification of visa application information, as well as deployment by teams investigating the sale of illegal products.[198] MBIE subsequently contracted with a private provider to train its staff on how to use false personas "for verification and investigations purpose."[199] The contract, which was publicly revealed about a year after its signing, provided for an "Advanced SOCMINT [Social Media Intelligence] Course" that included a number of topics:

- training on how to search Facebook, Twitter, LinkedIn and Instagram
- an introduction to natural language processing, including how it could be used to identify people by their usage of language
- methods for "automated harvesting" of content and "trending and pattern analysis"
- guidance on managing covert identities, including "backstopping," or creating a believable history for a fake persona
- creating a "detailed dossier on a group or individual".[200]

As of early 2019, the Ministry reported that staff had received training on a number of these skills but had not done the modules on automated harvesting or creation of dossiers.[201] An MBIE spokesperson further explained in response to a 2021 Official Information Act request that social media might offer insight in a circumstance in which information posted on a site "contradict[s] information provided to the ministry by a person of interest in an investigation into migrant exploitation."[202]

In 2019, in response to revelations about its contract as well as the Public Service Commission inquiry into government use of outside consultants, MBIE developed guidelines to govern its staff's use of social media for verification and investigations.[203] At a high level, the guidelines, which are similar in concept to the

---

[194] Ibid.
[195] Pennington, Phil, *RNZ*, 9 June 2024
[196] Ibid.
[197] Pennington, Phil, *RNZ*, 9 Nov. 2023-a; Pennington, Phil, *RNZ*, 9 June 2024
[198] Edens, John, *RNZ*, 27 Sept. 2017
[199] *RNZ*, 9 Jan. 2019
[200] "Master agreement for advanced social media search training" (12 Dec. 2017)
[201] *RNZ*, 9 Jan. 2019
[202] Daalder, Marc, *Newsroom*, 8 June 2021
[203] "Procedures for MBIE staff using social media for verification and investigation purposes to support regulatory compliance and law enforcement work" (July 2019); Daalder, Marc, *Newsroom*, 8 June 2021. The Ministry also published a transparency statement in response to the Public Service Commission's

New Zealand Police's social networking policy, set out four tiers of social media access, from the use that is most preferred and least risky to the use that is least preferred and riskiest:

- Level 1 (open unregistered searching): At this level, staff may use a generic search engine such as Google, or a search platform such as Social Search, to look for information that does not require either account registration or a login.[204] This is the only level of use that does not require approval, and it is used to "confirm or validate concerns" using publicly available, open source information.
- Level 2 (overt passive membership): This level requires use of an MBIE email account, and it is used to "access and confirm or validate information that may be considered publicly available but is subject to personalised privacy settings that require an account login to view", such as on Facebook, LinkedIn or Google Groups.[205] This level only authorises passive viewing of information. Approval may be given on a one-off or ongoing basis, but ongoing approvals must be reviewed and updated annually.[206] If the staff member carrying out the searches finds information that may lead to a formal investigation, they must switch to Level 3 or Level 4 searching and obtain the appropriate approvals.[207]
- Level 3 (discreet searching (false persona)): This level is used when some additional ground for information gathering has been identified in order to "investigate and/or verify a specific individual in relation to a specific task or case". It requires the use of a false persona but still contemplates only passive viewing of information, not engagement with the target or any other individuals.[208] As with Level 2, approval may be given on a one-off or ongoing basis, with annual review of ongoing approvals.[209]
- Level 4 (discreet active engagement (false persona)): This is the highest and most intrusive level, involving the use of a false persona that is set up specifically for an individual investigation and is logged in to a social media account.[210] It is used to "directly engage a specific individual in relation to a specific case," including by joining closed groups. The policy notes that this type of use is not encouraged in MBIE due to the potential risks.[211]

In 2021, MBIE disclosed that it had used false personas under its Level 3 authority 426 times since the beginning of 2020; because MBIE did not provide a breakdown across the Ministry, it is not known how many of these were used by Immigration New Zealand.[212] MBIE disclosed that Level 2 usage had been authorised 100 times during

---

Model Standards, which is in relevant part essentially identical to the Department of Internal Affairs' statement. "Transparency statement" (n.d.-a)

[204] See "Procedures for MBIE staff using social media for verification and investigation purposes to support regulatory compliance and law enforcement work" (July 2019), pp. 5, 7

[205] Ibid. p. 5

[206] Ibid. p. 8

[207] Ibid. p. 7

[208] Ibid. p. 6

[209] Ibid. p. 9

[210] Ibid. pp. 6, 9

[211] Ibid. pp. 6, 9

[212] Daalder, Marc, *Newsroom*, 8 June 2021

the same time period. There were no approvals for Level 4 usage, and no records of unapproved usage at Levels 2–4.

Immigration New Zealand also produced an informational summary to assist in the risk assessment of Posie Parker's planned March 2023 visit to New Zealand.[213] The summary draws on a variety of online sources, including newspaper articles, YouTube videos and tweets — many posted by, shared by or featuring Parker herself — to assemble a picture of Parker's ideology and language and provide context on previous events. While the summary does not state so explicitly, the research depicted in the report likely would have been obtained under Level 1 or 2 searching. The public record does not suggest overreach or misuse by Immigration New Zealand; the social media posts it examined were relevant to the assessment of the risk Parker might pose upon her visit to New Zealand. She was ultimately authorised for entry to the country but left before her planned Wellington rally after a chaotic rally in Auckland.[214]

Ministry of Social Development

In 2016, reporting revealed that Ministry of Social Development staff obtain information from social media to assist in benefits investigations, though the Ministry has stated that it does not trawl social media more broadly.[215] Reporting did not reveal the specific purposes for which Ministry investigators would scrutinise social media, though Ministry documents show that "relationship cases" make up the majority of investigations, and ample stories have been reported demonstrating the arbitrary nature of its relationship determinations.[216] Kay Brereton, an advocate for welfare beneficiaries, observed that recipients may be confronted with out-of-context pictures or other materials as proof of a change in relationship status and expressed concern that a post on social media could be taken as definitive evidence. As Brereton put it, social media is an unreliable medium: people use Facebook and other social media to "create a new person — they don't have to be themselves."[217] Māori are disproportionately likely to interact with the Ministry of Social Development and thus particularly likely to experience the impact of these policies.[218]

The Ministry disclosed in a subsequent Official Information Act response that it did not have a policy for social media monitoring and refused to divulge any other information about the fraud investigation team's methods for use of social media on the grounds that doing so would prejudice the maintenance of the law.[219] While the stated reason for not having a policy on social media monitoring was that it used social media in a targeted way, it was not clear whether the Ministry had any policy at all governing its use of social media. A 2019 report from the Office of the Privacy Commissioner on fraud investigations conducted by the Ministry of Social Development also revealed that the Ministry had collected Facebook information about a couple accused of having

---

[213] "Information Summary — Kellie-Jay KEEN-MINSHULL" (20 March 2023)
[214] McClure, Tess and Charlotte Graham-McLay, *The Guardian*, 26 March 2023
[215] Pereyra Garcia, Kate, *RNZ*, 10 Feb. 2016; see also "MSD investigations and social media" (10 Feb. 2016); *Response to Official Information Act request* (25 Aug. 2017) (stating that "social media … is not monitored as a means of detecting potential new cases.")
[216] *Response to Official Information Act request* (Nov. 2020), p. 1; Edmunds, Susan, *Stuff*, 30 Sept. 2019
[217] Interview with the author, 27 May 2024
[218] Quince, Khylee and Jayden Houghton (2023), p. 76
[219] *Response to Official Information Act request from Alex Harris* (16 March 2016)

misrepresented their relationship; the report did not address whether that information collection was inappropriate.[220]

According to a staff member at the Ministry, the ministry is in the process of finalising a policy addressing the use of social media for intelligence collection and investigation of fraud, but the policy had not been released at the time this report went to print. The Ministry's online information collection disclosure also does not mention social media.[221]

New Zealand Customs Service

The New Zealand Customs Service (Customs) does not currently have a publicly available policy in place, though it is reviewing its social media collection practices and a Social Media Use Policy that covers investigations and research. It is also in the process of obtaining guidance on the use of covert accounts in light of some platform prohibitions on false personas to ensure its procedures align with legal requirements and best practices. As a general matter, Customs collects information from social media to assist with two main functions: intelligence and investigations, which includes fraud detection. Staff do not communicate directly with targets for intelligence collection purposes. Where there is an investigation into an offence under the Customs and Excise Act 2018, a customs officer may undertake "discreet engagement" but will not interact with an individual under the guise of a false online persona.[222]

New Zealand Security Intelligence Service / Government Communications Security Bureau

The activities of New Zealand's security agencies are largely outside the scope of this report, as they raise additional complex issues and equities and deal with information that is often outside the public view. Nevertheless, a discussion of state use of social media is incomplete without briefly addressing the role of these agencies, particularly in the wake of the Christchurch mosque attacks.

The Government Communications Security Bureau collects intelligence derived from electronic communications, referred to as signals intelligence, and it is primarily focused on foreign intelligence; it has limited ability to collect information about New Zealanders.[223] The New Zealand Security Intelligence Service has a broad remit, covering domestic security, and uses a variety of methods to collect information and intelligence relevant to national security, including social media collection.[224] Prior to the Christchurch attacks, neither agency had any significant resources dedicated to social media scanning.[225]

---

[220] *Inquiry into the Ministry of Social Development's Exercise of Section 11 (Social Security Act 1964) and Compliance with the Code of Conduct* (May 2019)
[221] "Collecting your information" (n.d.)
[222] The information in this section is based on correspondence with Customs staff
[223] "Intelligence collection" (n.d.)
[224] "About us" (n.d.); "Our methods" (n.d.); Kitteridge, Rebecca (18 Sept. 2019)
[225] The Government Communications Security Bureau had limited capabilities, and New Zealand Security Intelligence Service had one fulltime officer doing open-source monitoring. Pennington, Phil, *RNZ*, 27 April 2021

In September 2019, the head of the Security Intelligence Service noted that the agency hosted and managed the Combined Threat Assessment Group, a multi-agency group that scans open source and other data from domestic and international sources to "produce assessments about the threats of terrorism around the world."[226] There is some ambiguity about the scope of the agency's social media review and collection; while the agency's director-general has publicly stated that no intelligence agency "monitor[s] internet usage across the board", the Security Intelligence Service does "regularly become aware of concerning activity on the internet" as a result of "leads".[227] Leads can come from "discovery" work, which entails "look[ing] for indicators of violent extremist views or activities"[228] — presumably on social media as well as other sources. Leads that are outside the realm of national security or intelligence are referred to New Zealand Police or other relevant agencies.

In 2022, the Minister in charge of the Government Communications Security Bureau and the New Zealand Security Intelligence Service issued the most recent ministerial policy statement on publicly available information.[229] In the main, the statement sets out seven principles to guide decisions around obtaining, collecting and using publicly available information: respect for privacy, necessity, proportionality, preference in favour of the least intrusive means, respect for freedom of expression, compliance with legal obligations and oversight. The policy also requires that there be protections in place for sensitive categories of individuals, including youth, journalists, refugees and asylum seekers.[230] New Zealand Police considers the statement to be strongly persuasive guidance, though it is not formally binding, and these principles are reflected in the New Zealand Police's policies as well.

Cross-agency data sharing

Agencies are not siloed from each other, and they may share information in appropriate circumstances. The case of Ahamed Samsudeen, who perpetrated a stabbing attack in a New Zealand supermarket in September 2021, is instructive. Samsudeen, a Sri Lankan national, entered New Zealand in 2011 on a student visa and obtained refugee status in 2013.[231] In 2015 and 2016, he began posting images and videos of graphic violence on Facebook.[232] These postings brought him to the attention of the New Zealand Security Intelligence Service and the New Zealand Police, who visited him in person to warn him against posting this kind of material and continued to monitor his social media footprint in the years following.[233] Samsudeen was ultimately arrested for knowingly possessing objectionable material — his 2016 Facebook posts — in violation of the Films, Videos, and Publications Classification Act 1993 and arrested a second time for purchasing a knife.[234] After his releases from confinement and prior to the attack, he

[226] Kitteridge, Rebecca (18 Sept. 2019).
[227] Ibid.
[228] Ibid.
[229] *Ministerial Policy Statement: Publicly available information* (1 March 2022) (defining "publicly available information" as information that is "published in printed or electronic form or broadcast" or is "generally available to members of the public free of charge or on payment of a fee")
[230] Ibid. p. 6
[231] *Coordinated Review of the Management of the LynnMall Supermarket Attacker* (14 Dec. 2022), p. 8
[232] Ibid. p. 29
[233] Ibid. pp. 36–42
[234] Ibid. p. 47

was under intensive monitoring and supervision by the Security Intelligence Service and police, who closely coordinated with each other as well as with Immigration New Zealand and the Government Communications Security Bureau.[235] Notably, the subsequent review of his case critiqued the nearly exclusive focus on surveillance in response to warning signs that Samsudeen was radicalising, to the exclusion of other kinds of intervention or support.[236]

3 Potential harms of social media monitoring

This section turns to the harms that can arise from state access to and use of social media. They do not stand in isolation. The use of automated tools, for instance, holds the potential to magnify many of the risks set out below, and they will have different — and often more acute — consequences for members of vulnerable groups. These risks are heightened when these tools are used by agencies with coercive powers: authority to criminally investigate, enforce and imprison. On the flip side, not every use of social media will implicate every concern described here or implicate them to the same degree; the assessment will depend on factors including the agency involved, the methods used, who is targeted and the purpose. A consistent theme, however, is the need for transparency, clear standards and oversight of policies, processes and impact.

While not the focus of this paper, social media platforms themselves also have a role. In the aftermath of the 2019 Christchurch attacks, a global collective of governments, tech companies and non-governmental and civil society organisations came together under the leadership of then-New Zealand Prime Minister Jacinda Ardern and French president Emmanuel Macron to create the Christchurch Call, intended to combat terrorist and violent extremist content online.[237] Compliance by some of the biggest social media platforms in the world has been spotty, however.[238] The major platforms have their own policies against use of their customer data for surveillance purposes, but detection and enforcement are inconsistent.[239]

Ease of creating comprehensive picture

A substantial amount of the data that public sector agencies view and collect is open source; it is available generally to the public and requires at most a social media account to view it. But data that is technically public might still be perceived as private — indeed, it is covered by many provisions of the Privacy Act. Social media platforms are a repository for an almost incalculably vast and rich store of data: photos of family, friends and travels; information about events attended; links to articles read and shared; a map of personal associations, both close and remote; work history; and more. As the

---

[235] Heron, Michael QC (14 March 2022)
[236] *Coordinated Review of the Management of the LynnMall Supermarket Attacker* (14 Dec. 2022), p. 38
[237] Christchurch Call to Eliminate Terrorist & Violent Extremist Content Online (n.d.). The Global Internet Forum to Counter Terrorism, which was founded in 2017 as an industry effort and was spun off in the wake of the Christchurch Call into an independent non-profit organisation, does parallel work. See "About" (n.d.)
[238] Clark, Emily, *RNZ*, 28 April 2024; Risius, Marten and Stan Karanasios, *The Conversation*, 20 March 2024; Witton, Bridie, *RNZ*, 12 Nov. 2023
[239] See Letter from ACLU Foundation of Northern California, Brennan Center for Justice, and ACLU to US Federal Trade Commission (12 Dec. 2023); "Comments submitted to the Federal Trade Commission on social media monitoring" (21 Nov. 2022)

US Supreme Court has said with respect to cell phones, this "immense storage capacity" has several ramifications for privacy.[240]

First, as with cell phones, social media enables the "collect[ion] in one place [of] many distinct types of information … that reveal much more in combination than any isolated record."[241] A piece of information that may not be noteworthy standing alone could prove revealing when a larger body of data facilitates inferences about sensitive matters.[242] Even a single category of information — for instance, some of the hundreds of millions of photos that users have uploaded to a platform — may convey a finely detailed picture to whomever chooses to look: "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions".[243] Indeed, photos and other desiderata of human life can reveal much about the private lives of other people reflected in them, not just the original poster. And such data can predate a search by months or years, creating a virtual time machine.

To be sure, individual users can increasingly control, through platform settings, who gets to see their social media self.[244] But that serves only to mitigate, not eliminate, this risk. The preservation of core democratic values cannot be dependent on the vagaries of a social media platform's terms and conditions. And the sense of safety arising from the understanding that postings are viewable only by "friends" heightens the intrusiveness of covert accounts that connect directly with people under false pretences and gain an intimate view of their entire online persona.

The cheapness and ease of accessing and assembling this information also differentiates it from analogue-era data collection. Monitoring that requires the time and energy of individual officers invites prioritisation and thoughtful consideration of the trade-offs. Because the state cannot have its agents everywhere all the time, there are natural constraints on how they are used.[245] The overt surveillance that would otherwise be necessary to gather the wealth of information that is now easily available through social media would invite "community hostility" that would serve as a natural constraint as well.[246]

By contrast, the ability to surreptitiously access and compile this information at the click of a button — as well as the means to do so at a large scale with the use of

---

[240] *Riley v California* 573 US 373 (2014), p. 393
[241] Ibid.
[242] See, e.g., "Country reports on the functioning of the adequacy decisions adopted under Directive 95/46/EC" (15 Jan. 2024), p. 251 (noting that "the New Zealand privacy framework considers information sensitive … when the inferences that can be drawn about the individual from information are potentially sensitive," including with respect to "information about race, ethnicity, gender, sexual orientation, sex life, health, disability, age, membership of advocacy group, trade union or political party and religious, cultural or political beliefs") (citing "Sensitive personal information and the Privacy Act 2020" (n.d.)); see also *Glukhin v Russia* (ECHR 11519/20), p. 22 ("The Court has previously found that the collection and storing of data by the authorities on particular individuals constituted an interference with those persons' private lives, even if that data concerned exclusively the person's public activities [citations omitted], such as participation in anti-government demonstrations")
[243] *Riley v California* 573 US 373 (2014), p. 394
[244] See "Public information on Facebook" (n.d.)
[245] See Law Commission and Ministry of Justice (2017), p. 173 (citing *US v Jones* 132 SCt 945 (2012), p. 963 (Alito J concurring)
[246] *US v Jones* 565 US 400 (2012), p. 416 (Sotomayor J concurring) (citing *Illinois v Lidster* 540 US 419 (2004), p. 426)

inexpensive specialised tools — eliminates these natural checks.[247] Indeed, the treatment of publicly available social media data has implications far beyond the online context, as the "Internet of Things" and related technologies vastly expand the scope, quantity and sensitivity of data that can be collected as we move in public spaces, and a reluctance to extend privacy protections to publicly available social media information may vitiate the privacy afforded to data collected by these tools as well.[248]

Social media can also be used to glean information about entire networks, far beyond the person targeted. This contradicts the notion that all information on social media has been voluntarily shared by the person to whom it relates — since that person may be far attenuated from the original target — and has significant implications for Māori values of collective privacy as well. As Māori law experts Quince and Houghton have explained: "from a Māori viewpoint, the well-being of the individual and the group are inextricably linked, such that recognising and enforcing individual rights without reference to the broader context actually undermines the individual."[249]

The views of both close associates and remote contacts may also be imputed to each other. A Palestinian student coming to the US to matriculate at Harvard was turned back at the airport in Boston, Massachusetts, after a border agent looked at the social media accounts on his phone and blamed him for the "anti-American" sentiments she saw in his friends' posts on his timeline.[250] At a larger scale, one social media monitoring and analysis company trying to get a contract with a major US municipal police department put together a case study purporting to show the power of its network analysis. For the case study, the company collected over 3,500 Facebook posts by a Muslim Brotherhood member living in New York City, including videos, pictures and public geotags, and information about nearly 4,000 of his Facebook "friends".[251] The case study, which was focused on assessing whether any of his contacts had extremist ideologies, insinuated that he might share the "violent, radical ideologies" of people who were two degrees out — contacts of contacts, at best.[252]

In short, whether publicly available or not, social media is not just pieces of atomised data — it can be used to create a mosaic of a person, a group or even a whole community.

Difficulty of interpretation

The ability of social media to facilitate the creation of a layered, detailed profile of an individual or group creates one set of risks. The other side of the coin is another, potentially equally weighty concern: that the picture created through analysis of social media, which is highly contextual and easy to misinterpret, reveals not the person themselves but a distorted, misleading simulacrum. Examples abound: a teenager in Kansas whose Snapchat post denounced violence that he feared might reach his town

[247] See also Edwards, Lilian and Lachlan Urquhart (2015), p. 25 ("Historically, then, what has separated police-state-like ubiquitous surveillance from legitimate police observation has been the compiling and keeping of systematic dossiers")
[248] See Edwards, Lilian and Lachlan Urquhart (2015), p. 28
[249] Quince, Khylee and Jayden Houghton (2023), p. 47
[250] See, e.g., Hartocollis, Anemona, *New York Times*, 3 Sept. 2019
[251] "Covid-19 Outbreak: Investigating a Threat Actor" (March 2020)
[252] Levinson-Waldman, Rachel and Mary Pat Dwyer (17 Nov. 2021)

was arrested after police wrongly concluded it was attempting to incite a riot.[253] A British traveller's slangy tweet about partying was disastrously misconstrued by US border agents, who thought his declaration that he planned to "destroy America" was a violent threat, leading them to interrogate and ultimately deport him.[254] The head of a civil rights department was tagged as a threat for posting graphics from a well-known rap album and ultimately stripped of his job.[255] A teenager was deported from the US in large part due to Facebook pictures depicting him in Chicago Bulls gear, Nikes and a blue shirt that was part of his school uniform — clothes that were erroneously taken to be evidence of his involvement in a Central American gang.[256]

Communication is always open to interpretation and misunderstanding, of course — even between two people ostensibly speaking the same language, as I have learned during my time here. But social media is particularly dependent on cultural references, ingroup speak and memes whose meaning may be highly fluid, dependent upon both their own evolution and the identities of the speaker and viewer. As one scholar noted, in an observation that has salience beyond the LGBTQ+ communities she was studying, "group humour" can be used to "distinguish … between the group and outsiders who do not understand the jokes."[257] This can be in the context of language that means one thing to the in-group and another (or nothing) to the outsider, or memes that "draw upon shared experience, knowledge, and understanding of insiders to draw boundaries between themselves and outsiders."[258]

Of course, so-called "insiders" are not a monolithic group; despite terminology in common use (including in this paper), there is no single "Muslim community", "immigrant community" or "rainbow community." Indeed, the term "community" can obscure significant internal differences, which may play out in social media spaces as well. Thus, it may not just be the outside observer who has a different understanding of a comment or reference or meme from the one who is using it, but also her neighbour who shares some aspects of the same identity but is cis rather than transgender, or comes from a comfortable upper-class religious background rather than an impoverished one, or immigrated to New Zealand from a country whose residents have historically been welcomed rather than shunned or discriminated against. Granular distinctions among social media platforms can mean that even people who are aligned in the core parts of their identities but use different platforms may remain ignorant of the meaning of a particular cultural reference until it migrates to their preferred platform.[259]

Language on social media can also be used to intentionally mislead, as the 2017 joint report from the Law Commission and Ministry of Justice noted.[260] White nationalist groups such as Action Zealandia, for instance, are skilled in using misdirection and ostensible jokes as a way to defang their hateful content while drawing in new

---

[253] See Levinson-Waldman, Rachel and Ángel Díaz, *Brookings*, 9 July 2020
[254] Wagenseil, Paul, *NBC News*, 31 Jan. 2012
[255] Sepulvado, John, *Oregon Public Broadcasting*, 12 April 2016
[256] Hlass, Laila L. and Rachel Prandini (21 May 2018), p. 3; see also Marcelo, Philip, *Boston.com*, 12 Jan. 2022 (describing a federal appeals court's decision to overturn an immigration board's deportation determination based on failures in the Boston Police Department's gang database)
[257] Black, Claire (2018), p. 70
[258] Ibid. pp. 74–75
[259] See ibid. p. 86
[260] Law Commission and Ministry of Justice (2017), p. 181

adherents.[261] A style guide for the neo-Nazi website The Daily Stormer, quoted in the report of the Royal Commission's inquiry into the Christchurch attacks, advised: "The unindoctrinated should not be able to tell if we are joking or not."[262] Symbols play much the same role, and can get significant traction online, "fly[ing] under the radar of the mainstream, while giving a wink and a nod to those in the know."[263] These are highly fluid as well: "what matters is that they are innocent enough that everyday people use them, and they change frequently enough so by the time mainstream audiences catch on, they've moved on to a different one."[264] While knowledgeable analysts will be schooled in understanding the subtext, the phenomenon speaks more generally to the pitfalls in relying uncritically on social media.

On a somewhat more innocuous (but still serious) front, pranksters have circulated false information on social media during natural disasters to mislead first responders or simply prank the public. During 2012's Superstorm Sandy, which devastated parts of New York City, someone created false images of the New York Stock Exchange underwater and the subway system infested by sharks. CNN aired the photos of the Stock Exchange as breaking news, "contribut[ing] to the public's general confusion."[265] AI bots could magnify the problem as well; if bots were directed to post about an upcoming protest to make it appear as though a large number of counter-protesters were planning to turn out, they could bait the police into turning out in larger numbers as well, escalating the potential for confrontation — a social media analogue to "swatting".[266]

Chilling of freedoms fundamental to personal and political expression

Social media monitoring can also undermine core individual and democratic freedoms. In her 2018 Sir Bruce Slane Memorial Lecture, Chief Justice Helen Winkelmann (then a judge on the Court of Appeal) succinctly defined the right to privacy as "the right to control certain types of personal information, personal space and one's own physical integrity, and the ability to develop intimate relationships and associations away from the gaze of others."[267] Privacy lies at the "heart of freedom of thought" — and constant surveillance is inimical to the development of self, to creativity, and to the flourishing of thoughts and ideas that are outside the mainstream.[268]

---

[261] See, e.g., Chen, Serena (2020), p. 157 ("Online fascist groups expertly manipulate their own labelling to appeal to mainstream or less in-the-know audiences"); Halpin, James and Chris Wilson (2022)

[262] "Chapter 5: Harmful behaviours, right-wing extremism and radicalisation" (8 Dec. 2020). The style guide went on to say: *"*There should also be a conscious awareness of mocking stereotypes of hateful racists. I usually think of this as self-deprecating humor — I am a racist making fun of stereotypes of racists, because I don't take myself super-seriously. *This is obviously a ploy and I do want to gas kikes. But that's neither here nor there.*" (emphasis added)

[263] Chen, Serena (2020), p. 158

[264] Ibid.; see also Romano, Aja, *Vox*, 16 March 2019 (analysing the Christchurch attacker's manifesto)

[265] Wukich, Clayton and Alan Steinberg (2016)

[266] See Campbell, Josh and Kat Jaeger, *CNN*, 15 Jan. 2024

[267] Winkelmann, Hon. Justice Helen (Nov. 2018)

[268] Ibid.; see also *R v Alsford* [2017] 1 NZLR 710 (SCNZ) at [63] (recognising that it is reasonable for individuals to expect that "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination by the state" will be protected from unreasonable state intrusion, including information "which tends to reveal intimate details of the lifestyle and personal choices of the individual"); Kaye, David (29 Aug. 2018), p. 13 ("The right to privacy often acts as a gateway to the enjoyment of freedom of opinion and expression."); Law

Her words underscore that privacy, and the rights to freedom of thought, expression and association, are fundamental aspects of human dignity, which is "central to both human rights and Māori custom."[269] They also form the core of political organising, protest and dissent, activities that are fundamental to a democratic society.[270] Unchecked scrutiny of the vast scope of human experience that is expressed and shared on social media would pose grave risks to these rights. As privacy scholar Daniel Solove has put it, "Espousing radical beliefs and doing unconventional things takes tremendous courage; the attentive gaze, especially the government's, can make these acts seem all the more daring and their potential risks all the more inhibitory."[271] Even the threat of surveillance — "real or imagined" — can have a significant impact on social media users' behaviour; one research study concluded that the mere possibility of social media surveillance led users to "censor their opinions or opt out of social media altogether."[272]

This effect is not limited to those who are directly targeted; surveillance may have a chilling impact as well on members of the public who see the power of the state and the consequences for those targeted.[273] This effect is likely to be particularly profound for marginalised communities, particularly those who are more dependent upon — and thus exposed to — state power; as the UN special rapporteur on freedom of opinion and expression has noted, "[s]urveillance exerts a disproportionate impact on the freedom of expression of a wide range of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities".[274] And as always, the use of automated tools will magnify these risks considerably. In the words of the New Zealand Law Commission, the broad use of powerful tools by enforcement agencies to "monitor the population at large could have a chilling effect on freedom of expression."[275]

The risk that dissenting views will be explicitly targeted is not hypothetical. The case of Rob Gilchrist is well known — the informant who was paid by New Zealand Police to infiltrate and report on the activities of environmental and other activists, eventually forming long-term romantic relationships with fellow activists.[276] The New Zealand

---

Commission and Ministry of Justice (June 2017), p. 40 (suggesting that "privacy involves a number of separate but related interests," including an "interest in freedom from surveillance and from monitoring or interception of one's communications" and "an interest in freedom from monitoring of one's associations") (citing Penk, Stephen and Rosemary Tobin (2018) at 1.1.3)

[269] Law Commission and Ministry of Justice (June 2017), p. 43

[270] See *Glukhin v Russia* (ECHR 11519/20), p. 25 (noting that "[p]ersonal data revealing political opinions, such as information about participation in peaceful protests, fall in the special categories of sensitive data attracting a heightened level of protection") (citations omitted)

[271] Solove, Daniel (2006), p. 499; see also Cohen, Julie (2000), pp. 1425–1426

[272] Green, Jordan (July 2020), p. 22

[273] Morse, Valerie (2019a), p. 36; see also Solove, Daniel (2006), p. 493 ("Because of its inhibitory effects, surveillance is a tool of social control, enhancing the power of social norms, which work more effectively when people are being observed by others in the community"); *US v Jones* 565 US 400 (2012) at 416 (Sotomayor J concurring) ("Awareness that the government may be watching chills associational and expressive freedoms")

[274] Kaye, David (11 May 2016), p. 15

[275] Law Commission and Ministry of Justice (Nov. 2016), p. 87

[276] Rees, Rochelle, *Sydney Morning Herald*, 27 March 2018. Gilchrist was managed by the New Zealand Police's Special Investigations Group, now known as the National Security Team, which was formed to respond to "terrorism threats to national security" — a category that seems an ill fit for environmental and other activists, though it is not unusual for a range of activism to be categorised as national security threats. *Sunday Star Times*, *Stuff*, 25 April 2009; Tan, Lincoln, *New Zealand Herald*, 15 Dec. 2008

Council for Civil Liberties has documented the history of New Zealand policing and security agencies in surveilling and creating dossiers on people who are associated with activists — even if they themselves have no political involvement.[277] And the practice is likely to have a disproportionate impact on Māori.[278]

A 2018 inquiry by the Public Service Commission into the use of outside consultants by multiple government agencies and independent Crown entities revealed that a private firm had used false profiles to monitor social media.[279] While the record is not entirely clear, it appears the firm may have accessed both open and closed sources to monitor activist groups including Greenpeace. More generally, the report identified the firm's longstanding practice of casting activist groups as "issue motivated groups", with the knowledge and consent of several agencies, as well as the use of social media monitoring with inadequate oversight.[280] These revelations led to the Public Service Commission's development of model standards on information gathering and the public trust.[281]

The international landscape is instructive as well. In the United States, multiple law enforcement agencies have used social media to police, monitor and even infiltrate movements for racial and social justice.[282] Evidence of this kind of online targeting is scarcer in New Zealand. This could have several possible explanations.

First, unlike the United States, which has some 18,000 law enforcement agencies at the local, county, state and federal level to police over 300 million people, New Zealand has a single, centralised police service that serves a tiny fraction of that population. This allows for uniformity and national prioritisation, with a single set of policies that governs every police officer in the country. The New Zealand Police is accountable to the entire country's population and to a suite of oversight and regulatory functions, as opposed to the patchwork system in the US.

Second, as a matter of national psyche, both the New Zealand Police and New Zealand public sector agencies as a whole seem to seek to align their behaviour — or at least the perception of their behaviour — with the notion of "social licence": essentially a grant of societal trust and legitimacy.[283] Based on experience, US agencies tend to be guided

---

[277] "Founding and Early History of New Zealand Council for Civil Liberties" (13 Aug. 2023)

[278] Quince, Khylee and Jayden Houghton (2023), p. 74 (noting that a range of security agencies "are charged with collating information on persons and group of interest in the name of national security. While such a practice may not be deliberately targeting Māori, the political situation in New Zealand is such that Māori have a high profile in the struggle for recognition of our rights as tangata whenua. Debates over the Treaty relationship mean that Māori will always be at the forefront of political activism in this country")

[279] Martin, Doug and Simon Mount, QC (18 Dec. 2018), pp. 9, 51

[280] Martin, Doug and Simon Mount, QC (18 Dec. 2018)

[281] "Acting in the Spirit of Service: Information Gathering and Public Trust" (Dec. 2018-a)

[282] See, e.g., Levin, Sam, *The Guardian*, 8 Sept. 2021; Farivar, Cyrus and Olivia Solon, *NBC News*, 20 June 2020; Farzan, Antonia Noori, *Washington Post*, 23 Aug. 2018; Perez, Chris, *New York Post*, 7 Feb. 2018

[283] See "Overcoming preconceptions: How big data can gain a social licence in New Zealand" (5 April 2023) (offering a definition of social licence); "An informed use of facial recognition technology by NZ police" (n.d.) ("For Police, who have a role at the heart of the community, social licence to operate is vital"); "Chapter 2: The three ways the individual may have been detected" (8 Dec. 2020) (noting that informed public debate would assist public sector agencies in gauging the social licence for a variety of work)

more by what is legally permitted than the somewhat nebulous question of what *should* be done. If there is a perception of broad social licence for social media monitoring, that could open the floodgates — but on the whole, attention to social licence seems likely to exert a constraining influence.

Finally, as a practical matter, this kind of political social media targeting is rarely revealed by the state itself. The revelations in the United States have typically emerged from a combination of journalistic investigations, litigation and open records requests, often by civil society organisations. In New Zealand, the smaller (and shrinking) media landscape, near absence of civil society ecosystem and weaker constitutional protections may combine to make it less likely that any abuses that do occur become public.

Implications for vulnerable groups

When it comes to the implications of social media monitoring for vulnerable or marginalised communities, there is not a single, neat narrative. Māori, immigrant and LGBTQ+ communities are disproportionately targeted online by hateful and violent speech, which can spark violence and, even without leading to violence, lead to a deterioration in feelings of safety and community belonging.[284] At the same time, there is a historic lack of trust between law enforcement and security agencies on the one hand and Māori, Muslim and rainbow communities on the other, due to overcriminalisation of members of these communities combined with, in some cases, inadequate attention to the threats against them. This dynamic heightens the stakes of surveillance that is, or is perceived to be, directed at those communities — stakes that are even higher for New Zealanders with intersectional identities, such as takatāpui (a Māori person identifying as LGBTQ+). At a minimum, the state must be sure it is taking a "do no harm" approach, which can only happen in close consultation and partnership with marginalised communities, following their lead as they articulate what they need.

In the wake of the 2019 Christchurch terror attack, for instance, Muslim community members spoke out in outrage that New Zealand security agencies had been searching for online threats from Islamic extremists rather than attending to the growing white supremacist threat.[285] It appears that many in the community saw an important role for the state to play, as long as it was appropriately tailored to the nature of the online threat. While there is reason to be highly sceptical, as the Royal Commission of Inquiry observed, about whether broadscale social media monitoring could have both identified the individual in advance and correctly assessed that, unlike the vast majority of online denizens, he would move from violent speech to violent action, this dynamic speaks to the high stakes for groups who are targeted with vile speech online.[286] It also highlights

[284] "Hui Summary and Compendium" (15–16 June 2021), pp. 28–29 (citing Kate Hannah); "Hui Summary and Compendium" (30 Oct.–1 Nov. 2022), p. 13 (quoting Chris Kumeroa); ibid., p. 37 (noting online hate directed at LGBTQI+ people)

[285] "Chapter 4: What communities told us about the broader context in which the terrorist attack occurred" (8 Dec. 2020), Pennington, Phil, *RNZ*, 25 March 2019; Foon, Eleisha, *RNZ*, 8 Dec. 2020

[286] "Executive summary" (8 Dec. 2020); see also Wilson, Chris (2022) ("Only a tiny minority of those who express hateful and extremist rhetoric online put their words into action")

the risk that surveillance for counterterrorism and intelligence purposes will degrade relationships with the very communities the state needs to protect.[287]

For rainbow communities, scholars have documented the importance of digital spaces, particularly social media, observing that "[s]ocial media and other internet technologies allow young LGBTQ+ people to express themselves, feel less alone, learn new things, and simply go about everyday life."[288] But the centrality of social media heightens the risks on multiple fronts. Queer-themed online content has a history of being interpreted as sexual, even criminal, by both individuals and automated commercial tools.[289] At the same time, the online targeting of LGBTQ+ communities in Aotearoa New Zealand has exploded, particularly in the wake of the 2023 visit by anti-transgender activist Posie Parker, whose earlier events in Australia were attended by people wearing Nazi regalia.[290]

In light of these threats, some advocates for rainbow communities' safety and equality have emphasised that their most urgent concerns lie with the volume of abusive and threatening speech online and what the platforms themselves are doing to police that speech. In conversations, some have suggested that law enforcement may be underestimating the risk to LGTBQ+ communities and that attention to these threats could help bolster their safety while stressing that LGBTQ+ communities often experience enforcement agencies as a coercive, not protective, force.[291] As a result, several advocates have proposed that the preferred approach would be for non-governmental organisations to handle identification of online threats, potentially with government funding, and for the persons targeted to decide whether or how to report the threats to law enforcement. This approach is worth serious attention.

Māori, too, "bear the brunt of brunt of online threats, harassment and threats of violence — likely by those extremists who feel most threatened by these groups and the challenge they pose to the status quo."[292] As for LGBTQ+ communities, however, the combination of online targeting and "hypersurveillance of Māori" is likely to make the right balance a complex one.[293] Some critics have argued that the state should not play a threat-monitoring role for security purposes, because the state itself has "normalised harm against Māori through its own history."[294]

Studies have also shown both that Māori respondents have different reactions to scenarios involving potential privacy invasions than non-Māori — sometimes ranking them more invasive and sometimes less — and that Māori have a heightened sense of concern about public space surveillance and tracking, as well as about protection of

---

[287] See *Coordinated Review of the Management of the LynnMall Supermarket Attacker* (14 Dec. 2022), p. 122

[288] Black, Claire (2018), pp. 4–5; see also ibid., p. 16 ("[W]hen interviewees explained what they did on the internet, time and time again they offered a roll-call of social media sites and apps")

[289] See, e.g., Black, Claire, *Craccum*, May 2017; Fox, Chris, *BBC.com*, 10 Sept. 2020; Natanson, Hannah, *Washington Post*, 9 June 2023

[290] See Hattotuwa, Sanjana, et al (April 2023), p. 14

[291] See, e.g., Rapira, Laura O'Connell and Kassie Hartendorp, *RNZ*, 13 Nov. 2018; Murphy, *RNZ*, 27 Nov. 2018

[292] "Hui Summary and Compendium" (30 Oct.–1 Nov. 2022), p. 13 (quoting Chris Kumeroa)

[293] Quince, Khylee and Jayden Houghton (2023), p. 73 n. 140

[294] "Hui Summary and Compendium" (30 Oct.–1 Nov. 2022), p. 8 (quoting Tina Ngata)

personal information overall.[295] The Office of the Privacy Commissioner's most recent biennial privacy survey, for instance, revealed that Māori are far more likely than other New Zealanders to say that they have avoided visiting a particular place due to concerns about surveillance; they are also more likely to report that privacy concerns have dissuaded them from contacting a government department, suggesting a potential lack of trust that would be important for agencies to take into account.[296]

Collection of data from, about or relating to Māori individuals, whānau (family), hapu (subtribe), or iwi (tribe) also raises heightened considerations, as "Māori data is a living taonga, treasure, and is significant emotionally, spiritually, economically, and intergenerationally."[297] Under the principles of the Treaty of Waitangi, state agencies should abide by these values in handling Māori information.[298]

Finally, tamariki and rangatahi (children and youth) may be particularly vulnerable when it comes to the state's use of social media data. Youth are unlikely to be able to fully account for the consequences of their online activity (which may be true for most adults as well).[299] The Privacy Act's IPP 4, which requires that information collection be fair and not unreasonably intrusive, contemplates higher protections for youth.[300] And privacy is "vital for child development," heightening the stakes of using social media to monitor youth or collect information about them.[301]

In addition, while public reporting does not indicate these tools are in use in Aotearoa New Zealand, a number of school districts in the United States have invested in tools to monitor students online.[302] If such tools were brought across the Pacific, officials would need to confront the lack of empirical evidence of their effectiveness, indications that they may be counterproductive, the risk that they might result in "outing" kids and significant concerns about their impact on children's social and civic development as well as on LGBTQ+ youth and Māori youth, who experience far greater rates of punishment in school than Pākehā youth.[303]

Risks from use of AI-driven and third-party tools

As agencies face budget cuts and resource constraints, tools offering AI capabilities and touting time- and cost-saving results with the click of a button may become ever more

---

[295] Quince, Khylee and Jayden Houghton (2023), pp. 107–111; "Research on Privacy Concerns and Data Sharing" (April 2024), p. 6
[296] "Research on Privacy Concerns and Data Sharing" (April 2024), p. 16
[297] Royal Society Te Apārangi (Dec. 2023), p. 29
[298] de Silva, Tommy, *The Spinoff*, 3 Feb. 2024
[299] See Edwards, Lilian and Lachlan Urquhart (2015), p. 25 (citing danah boyd for the proposition that "teens … do not imagine" the audiences other than their peers, including parents, teachers and the police, "who are also invisibly able to watch" them online)
[300] Privacy Act 2020, s 22
[301] Livingstone, Sonia, et al (2019)
[302] See, e.g., Burke, Colin and Cinnamon Bloss (Nov. 2020); Prothero, Arianna, *EducationWeek*, 20 Sept. 2023
[303] See, e.g., Herold, Benjamin, *EducationWeek*, 30 May 2019; *Social Media Monitoring in K-12 Schools: Civil and Human Rights Concerns* (17 Oct. 2019); McCaull, Ashleigh, *RNZ*, 19 Dec. 2022

appealing. But automated social media monitoring tools are not a panacea. Instead, they both magnify the risks described above and pose additional ones.[304]

As an initial matter, these promises may be part puffery. It is becoming almost axiomatic that if a company hypes cutting-edge AI technologies that replace human involvement, you don't have to go far to find the people behind the curtain.[305] In the Dataminr example described above, while the company promised high-tech AI functions, in practice it relied on (likely poorly paid) employees to do the work. Another social media monitoring company's claims that it used "cutting-edge AI-based technologies" such as "machine learning", "cognitive computing" and "combinatorial and statistical algorithms" were critiqued by an expert data scientist as meaningless "word salad".[306] AI systems are simultaneously opaque, essentially by design, making it difficult to achieve oversight or transparency or even to define what those qualities would look like.[307] They can nevertheless tempt human users who believe them to be objective into relying on them.[308]

In addition, these tools' functional weaknesses are manifold. Most AI-driven tools are still trained primarily on English language and Western sources, a notable shortcoming in Aotearoa New Zealand, which has te reo Māori as an official language and an increasing saturation of Pacific and Asian languages; as a result of their circumscribed training, AI tools frequently struggle with navigating context and language.[309] Training data may have underlying bias as well; in one recent example, an AI grading tool gave poorer grades to identical essays based solely on the perceived gender, race or ethnicity of the student.[310]

When language ineptitude and bias come together, the results can be particularly toxic: last year, Instagram's AI-driven auto-translate feature inserted the word "terrorist" into the bios of users whose posts contained a combination of the word "Palestinian", a picture of the Palestinian flag and the Arabic phrase for "thank God."[311] The UN's Special Rapporteur on freedom of opinion and expression has, in the context of public sector bodies' use of AI, called for "[p]articular attention [to] be given to the disparate

---

[304] For further guidance on the intersection of AI and the information privacy principles, see "Artificial Intelligence and the Information Privacy Principles" (2023)
[305] See Bridle, James, *The Guardian*, 10 April 2024
[306] Bhuiyan, Johana and Sam Levin, *The Guardian*, 17 Nov. 2021
[307] See Kaye, David (29 Aug. 2018), p. 6 ("[A]s humans are progressively excluded from defining the objectives and outputs of an AI system, ensuring transparency, accountability and access to effective remedy becomes more challenging, as does foreseeing and mitigating adverse human rights impacts"); Shenkman, Carey, et al (May 2021), p. 8 ("State-of-the-art machine learning tools, by default, cannot be 'opened up' to get a plain-spoken explanation of why they reached a decision they did. These tools utilize large neural networks which may have up to millions or billions of interrelated parameters involved in learning and producing outputs")
[308] See Kaye, David (29 Aug. 2018), p. 9 (noting the "tendency to defer to machine-made decisions (on the assumption of objectivity …)")
[309] See, e.g., North, Madeleine, *World Economic Forum*, 17 May 2024; Shwartz, Vered, *The Conversation*, 14 Feb. 2024; cf. Bhatia, Ripu, *Stuff*, 8 June 2022
[310] Furze, Leon (May 2024)
[311] Martin, Cathy, *Multilingual.com*, 26 Oct. 2023; see also Thompson, Nicholas, *Wired*, 14 Aug. 2017 (describing a sentiment analysis algorithm that concluded, based on its ingestion of the internet, that the word "Mexican" was a slur and accordingly downgraded reviews of Mexican restaurants)

impact of such technologies on racial and religious minorities, political opposition and activists."[312]

In this vein, it is laudable that the New Zealand Police's new technology review framework requires that any AI-driven technology have been used or tested in a New Zealand context, and that Māori and Pacific communities be consulted; these measures should be the baseline for any other agency considering automated tools.[313] The Office of the Privacy Commissioner has also emphasised concerns that AI systems developed overseas may further entrench bias against Māori.[314] The recent misidentification of a Māori woman as a suspected shoplifter by an automated facial recognition system in a New Zealand supermarket — and her ejection from the store despite providing multiple documents to prove her identity — offers a case study of the pitfalls of systems not trained on New Zealand-specific data as well as the inclination to rely on automated systems even in the face of contrary evidence.[315]

As noted above, social media is highly contextual and can be difficult for even the keenest observers to accurately interpret. Automated tools will always be clumsier than humans at identifying nuance, determining when something is a joke or understanding sarcasm.[316] Humour plays multiple roles: far-right groups manipulate it as a recruitment strategy, while many social media users use sarcasm, irony and coded in-group words because their followers appreciate it or because it's the best way to convey their message, not because they aim to mask anything nefarious. An automated tool is likely to struggle with identifying the particular brand of humour that masks white extremist messaging while not sweeping in the vast majority of innocuous content online. This contextuality also raises questions about AI tools that are themselves trained in part on open-source social media data.[317] What are they learning as they ingest it?

Some platforms have features that may be particularly ill-suited to automated analysis. Telegram's "stickers", for instance, "enable visual and animated expression which cannot be studied computationally"; animated GIFs can carry multiple meanings.[318] More generally, machine learning-driven AI tools may struggle to accurately understand posts that include images, videos, symbols or any other non-text content.[319]

The Classification Office's review of Ahamed Samsudeen's case offers an illuminating case study. After the videos and other materials Samsudeen posted were deemed to be objectionable, the Classification Office undertook a detailed evaluation that assessed the context of the videos and his reasons for posting them.[320] It ruled that while his postings depicted violence and its aftermath, the posts themselves did not convey "promotion or support" of the violent events, nor was there anything that "promoted or encouraged others to carry out acts of violence, crime or terrorism", which was required

---

[312] Kaye, David (29 Aug. 2018), p. 20.
[313] *New Technology Framework* (2021), p. 8
[314] "Artificial Intelligence and the Information Privacy Principles" (2023)
[315] Paewai, Pokere, *RNZ*, 17 April 2024
[316] See Shenkman, Carey, et al (May 2021), p. 8 ("Machines are ill-suited to make contextual assessments or apply the nuanced ethical standards that may be necessary for any given decision")
[317] See Leffer, Lauren, *Scientific American*, 19 Oct. 2023
[318] Hattotuwa, Sanjana, et al (April 2023), pp. 15–16
[319] Cf. ibid. p. 11
[320] See *Coordinated Review of the Management of the LynnMall Supermarket Attacker* (14 Dec. 2022), pp. 69–70 (analysing factors such as whether they contained ISIS branding)

for an objectionable publication.[321] As the Office observed, records of violent events, particularly those occurring in war zones, in conflict regions or in the context of recording a criminal act, "can have value in multiple ways, ranging from evidential value in pursuing justice to social value in raising awareness of heinous acts."[322] Instead, Samsudeen's stated reason for posting the images and videos was to "highlight the unjust treatment of Muslims around the world", undermining the claim that they were meant to promote or support violence or criminal or terrorist acts.[323] This kind of nuanced evaluation would be close to impossible with an automated tool.

The technical and data protection aspects of many automated tools are likely to pose substantial concerns as well. Few AI companies are based in New Zealand, store their data in New Zealand or train their tools on New Zealand data, undermining both New Zealand and Māori data sovereignty. And many automated tools are likely to use data scraped from social media platforms, implicating privacy concerns.[324]

Finally, automated tools supercharge the capacity to stitch together a comprehensive picture of a person's life and that of their associates:

> In these modern times it [network analysis] has become a high art form … through the automated harvesting of email, landline, mobile phone, Skype, Facebook, Twitter, LinkedIn and other communications and social media metadata and content. Sophisticated algorithms are then used to digitally analyse that metadata (i.e. who is talking to who), combined with time and frequency analysis, to build pictures of inner and outer networks and to predict likely conspirators or terrorist and criminal networks. A lot of that data can be obtained from open sources without warrant just by harvesting what is freely available on the Internet, and sophisticated software is commercially available to do just that.[325]

While this observation was penned a decade ago, these capabilities have become only more powerful since, posing risks to both personal privacy and collective privacy.[326] Privacy Commissioner Michael Webster highlighted these threats in a 2022 speech, noting that "[t]he explosion of new data sources and platforms, together with potent new data scraping, mining, linking and analysis tools, creates new risks of privacy intrusion. There are new risks that in the analogue world we would simply not accept without complementary security protections — including against unreasonable

---

[321] Ibid. p. 52

[322] Ibid. Documentary evidence of acts of violence could "be misappropriated by extremists seeking to promote their own illegitimate agenda", which might be signalled through "recognisable markers, branding or promotional text", but the Office did not see evidence of that here.

[323] Ibid. p. 54

[324] See, e.g., Vanian, Jonathan, *CNBC*, 12 Jan. 2023; *Joint statement on data scraping and the protection of privacy* (Aug. 2023)

[325] "Operation 8: The evidence and police spying methods" (Nov. 2013). The purchase of data from data brokers — an endemic problem in the United States — is an important issue that is beyond the scope of this report.

[326] See, e.g., *Investigation of the RCMP's collection of open-source information under Project Wide Awake* (15 Feb. 2024) (the result of an inquiry into the Royal Canadian Mounted Police's use of social media monitoring tool Babel X, albeit under a privacy regime that offers more protection for publicly available information)

surveillance."[327] The European Union Court of Human Rights, too, has recognised the need to safeguard personal data that could affect the right to privacy and enjoyment of family life, particularly "where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes, and especially where the technology available is continually becoming more sophisticated."[328]

Risks of undercover accounts

Finally, the use of undercover accounts to connect directly with targets online deserves special attention. This practice may be critical in some circumstances — for instance, in combatting online child sexual exploitation. At the same time, the use of such accounts poses unique risks. In the "real world", an agent seeking to infiltrate a group or connect with someone under false pretences must adopt a persona that matches at least the outward indicia of their true identity; they cannot pretend to have a different racial or ethnic identity from their own, be a height or age they are not or impersonate an actual person known to their target. Online, however, the options are limitless. A 25-year-old male Pākeha officer could pretend to be a 50-year-old wahine Māori — or to be five different people, if he has the time and technical capability to build up five different facially legitimate accounts.[329] The absence of built-in structural limitations on the use of undercover accounts makes them particularly susceptible to misuse and abuse and in need of guardrails and robust oversight.

The 2017 joint report from the Law Commission and Ministry of Justice addressed covert operations, which would encompass the use of online aliases to form relationships and build trust with targets, though not the use of alias accounts simply to conduct research or find information online.[330] The joint report expressed unease at having covert operations constrained only by internal agency review, "without the benefit of Parliamentary guidance, independent external approval or review, or any consistent policy across government."[331] Recognising that not all covert operations would be appropriate for a warrant regime, the report recommended that agencies conducting covert operations be required to develop and publish a policy statement.[332] The report also emphasised the importance of external oversight "in light of [the] unique aspects of covert operations" through a structure tailored to the different levels of invasiveness of different covert methods.[333] Such a scheme would go a long way towards mitigating the risks of these practices.

---

[327] Webster, Michael (21 Oct. 2022); see also Law Commission and Ministry of Justice (June 2017), p. 181 ("Tools that collate and analyse significant amounts of information about individuals — for example, by combining their social media posts, location check-ins and the people and groups they associate with to assign "risk profiles" or predict offending — have the potential to intrude on reasonable expectations of privacy")

[328] *Glukhin v Russia* (ECHR 11519/20), p. 25 (citations omitted)

[329] Fake accounts are also produced in bulk by third-party companies and used to scrape data, often in a way that is nearly invisible to the social media platforms themselves: see Vanian, Jonathan, *CNBC*, 12 Jan. 2023

[330] Law Commission and Ministry of Justice (June 2017), p. 289

[331] Ibid. p. 286

[332] Ibid. p. 296

[333] Ibid. pp. 297–298

Recommendations

In light of the historical and cultural landscape in New Zealand; the statutory gaps; the outstanding recommendations from the Law Commission and Ministry of Justice; the obligations embedded in the Public Service Commission's model standards; and the risks to privacy, civil rights and democratic values outlined above, this report makes several concrete recommendations.

First, the gaps in the Search and Surveillance Act 2012 and the Privacy Act 2020 should be addressed and filled to ensure that both enforcement authorities and privacy protections are fit for purpose in the digital age. All agencies deploying social media for information collection should develop a clear policy and make it public to the maximum extent possible. The Government Chief Privacy Officer would be a natural partner in this effort.[334]

Second, all public sector entities using social media for other than public-facing purposes should publish policies that inform the public about their governance structures and practices, including clear information about the accountability mechanisms in place.

Finally, as public sector agencies develop or update their policies, and as they consider developing use cases or opportunities that may not yet be covered by a policy, a set of questions for consideration may help guide and refine their efforts. Some of these may already be embedded in an agency's policies or practices, and not every consideration will be relevant to every agency. Taken together, however, they represent key touchpoints to help guide agencies' thinking. The joint report from the Law Commission and Ministry of Justice articulates some of these considerations as well, emphasising minimisation of intrusion into individual privacy, prioritisation of Māori values and "any other relevant cultural, spiritual or religious considerations", and minimisation of impact on youth and other vulnerable individuals.[335]

A suggested sample set of questions for consideration follows.

Proof of concept

- Has the particular use been evaluated for efficacy, or have measures been put into place to do so?
- Is it the least intrusive method of gathering the relevant information?

Impact on privacy and civil liberties

- Is the practice directed at publicly available or private/protected information?
- Could it affect the exercise of rights protected by BORA? If so, how will that impact be mitigated?

---

[334] See "Privacy organisations" (n.d.) (describing the Government Chief Privacy Officer's role in working with agencies to support and improve their privacy practices)
[335] Ibid. p. 12

- Is the retention of data limited to the maximum extent possible, consistent with enforcement and investigative needs?
- Could the information be collected directly from the individual — for instance, through a survey or other means?

Scope of use

- Is the use of social media lawful, proportionate and necessary in the circumstances?
- Is the specific use well tailored to the seriousness of the offence or the significance of the regulatory need, with less serious or significant agency purposes entailing less intrusive methods?

Bias and disproportionate impact

- Has potential bias been assessed, and steps taken to mitigate or eliminate it?
- Could the use nevertheless have a disproportionate impact on marginalised or vulnerable groups? If so, what steps have been taken to mitigate or minimise the impact?
- Have the groups (and/or their advocates, in the case of youth) who could experience bias or disproportionate impact been consulted directly, and are there plans are in place for ongoing consultation and coordination?
- Have Māori privacy values been specifically considered and provided for in close coordination with Māori experts?
- Have other relevant obligations and commitments under Te Tiriti been considered and satisfied?

Third-party tools and use of AI

- Have the tool's capabilities been evaluated by an external reviewer?
- Does the company have a publicly available privacy policy?
- Does the company disclose its algorithm and/or make it available for outside assessment?
- Does the company scrape data?
- How is the data protected?
- Is the data hosted in New Zealand or offshore/in the cloud?
- How does the company mitigate the risks of the use of AI?
- Has an expert on data ethics been consulted?

Oversight and transparency

- Is there a policy in place?
- Has the policy been developed in consultation with outside experts and affected groups as needed?

- Is the policy publicly available to the maximum extent possible?
- Has other relevant information been shared with the public to the maximum extent possible?
- Are there mechanisms to assess compliance with policy, law and values, including individual remedies or periodic audits?
- Does the agency track the use of specific methods, such as the use of undercover accounts or account takeovers, including how often they are used and for which purposes?
- Are there mechanisms to verify the accuracy, legitimacy and/or reliability of social media data?

Appropriate government role

- Particularly in the context of monitoring online activity for violent extremism or other threats, can civil society play a role to mitigate some of the risks arising from government monitoring — for instance, by identifying threats and sharing them with relevant agencies and/or targeted individuals or groups? Can funding or other support be made available to enable civil society organisations to carry out that function?

Conclusion

Aotearoa New Zealand is at an inflection point when it comes to public sector use of social media. As detailed in this report, a variety of New Zealand agencies access social media for purposes connected to their missions, and many are doing the hard work of trying to develop policies and processes that reflect best practices and vindicate the public trust. Indeed, the impression I came away with is of a country stepping cautiously into these practices more often than it is rushing headlong into them.

At the same time, there continues to be a lack of public visibility into agency practices, close to a decade after the independent New Zealand Law Commission and the Ministry of Justice definitively recommended that policies on use of social media be developed and published. While New Zealand's Official Information Act appears to be a more functional and timely method of obtaining information from federal agencies than the US's equivalent Freedom of Information Act, providing policies to individuals who make an Official Information Act request is not an adequate substitute for making this information easily available to all. And when there is no policy at all, the public is even more in the dark.

This report also argues that the stakes of social media monitoring are high and growing higher. Public sector entities looking to social media must be cognisant of the hazards articulated here, including the risks that their efforts will result in bias, intrude into privacy or human dignity, interfere with exercise of core democratic rights or simply not further their goals effectively because the information is messy or misleading. These risks are present even when it comes to publicly available social media data. But they can be mitigated, including by considering the questions posed in this report.

There is a tremendous opportunity to build guardrails and mechanisms for transparency and accountability into public sector processes, aided by statutory frameworks; Treaty of Waitangi principles and obligations; and the work of entities including the Office of the Privacy Commissioner, the Public Services Commission and the Government Chief Privacy Officer. By offering a window into agencies' existing practices and articulating reasons to move with caution, this report endeavours to provide both an impetus and a guide for this next stage of evolution, led by Aotearoa New Zealand's values and expertise.

Bibliography

"A short history of the web" (n.d.), CERN. Retrieved 5 June 2024 from: https://home.cern/science/computing/birth-web/short-history-web

"About" (n.d.), Global Internet Forum to Counter Terrorism. Retrieved 5 June 2024 from: https://gifct.org/about/

"About the Classification Office" (n.d.), Te Mana Whakaatu | Classification Office. Retrieved 2 May 2024 from: https://www.classificationoffice.govt.nz/media/documents/J000981_CO_-_About_Us_A4_FF.pdf

"About the Digital Safety Group" (n.d.), Te Tari Taiwhenua | Internal Affairs. Retrieved 5 June 2024 from: https://www.dia.govt.nz/About-the-Digital-Safety-Group

"About us" (n.d.), New Zealand Security Intelligence Service. Retrieved 2 May 2024 from: https://www.nzsis.govt.nz/about-us/

"Acting in the Spirit of Service: Information Gathering and Public Trust" (Dec. 2018-a), Te Kawa Mataaho | Public Service Commission. Retrieved 5 June 2024 from: https://www.publicservice.govt.nz/assets/Information-gathering-and-public-trust-2023.pdf

"Acting in the Spirit of Service: Information Gathering and Public Trust" (Dec. 2018-b), State Services Commission | Te Kawa Mataaho. Retrieved 5 June 2024 from: https://www.publicservice.govt.nz/assets/DirectoryFile/Model-Standards-Information-Gathering-and-Public-Trust.pdf

"An informed use of facial recognition technology by NZ police" (n.d.), Data.govt.nz. Retrieved 5 June 2024 from: https://data.govt.nz/blog/police-frt/

Andino, Carlos (17 Feb. 2022), Testimony Before the Council of the District of Columbia, Committee on the Judiciary and Public Safety Concerning the Year 2021 to 2022 Performance Oversight of the District of Columbia Metropolitan Police Department. Retrieved 6 May 2024 from: https://www.washlaw.org/wp-content/uploads/2022/02/WLC-Gang-Database-Testimony-by-Carlos-Andino-Final-Version-2_17_22-Accessible.pdf

Arnold, Hon Sir Terence KNZM KC and Matanuku Mahuika (2023), *Taumaru: Protecting Aotearoa New Zealand as a free, open and democratic society*. Wellington: Ministry of Justice. Retrieved 27 May 2024 from: https://www.dpmc.govt.nz/sites/default/files/2023-05/Taumaru%20-%20Protecting%20Aotearoa%20New%20Zealand.PDF

"Artificial Intelligence and the Information Privacy Principles" (2023), Office of the Privacy Commissioner. Retrieved 7 May 2024 from: https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/AI-Guidance-Resources-/AI-and-the-Information-Privacy-Principles.pdf

BBC News, “Caution on twitter urged as tourists barred from US”, *BBC.com*, 8 March 2012. Retrieved 3 May 2024 from: https://www.bbc.com/news/technology-16810312

Baker, James, “Spate of ram-raids driven by social media — police”, *1News*, 27 April 2022. Retrieved 28 May from: https://www.1news.co.nz/2022/04/27/spate-of-ram-raids-driven-by-social-media-police/

“Before you apply for a firearms licence” (n.d.), Te Tari Pūreke | Firearms Safety Authority. Retrieved 12 April 2024 from: https://www.firearmssafetyauthority.govt.nz/manage-and-apply/firearms-licence/you-apply-firearms-licence

Bennett, Lucy, “MBIE hired security firm to increase staff skills in gathering information from social media”, *New Zealand Herald*, 9 Jan. 2019. Retrieved 5 April 2024 from: https://www.nzherald.co.nz/nz/mbie-hired-security-firm-to-increase-staff-skills-in-gathering-information-from-social-media/FE6SBBHEDHQPDEGTTZWYBOSLMU/

Bhatia, Ripu, “Tech firm builds artificial intelligence that speaks te reo Māori”, *Stuff*, 8 June 2022. Retrieved 11 June 2024 from: https://www.stuff.co.nz/pou-tiaki/128837945/tech-firm-builds-artificial-intelligence-that-speaks-te-reo-mori

Bhuiyan, Johana and Sam Levin, “Revealed: the software that studies your Facebook friends to predict who may commit a crime”, *The Guardian*, 17 Nov. 2021. Retrieved 5 May 2024 from: https://www.theguardian.com/us-news/2021/nov/17/police-surveillance-technology-voyager

Biddle, Sam, “Twitter surveillance startup targets communities of color for police”, *The Intercept*, 21 Oct. 2020. Retrieved 1 May 2024 from: https://theintercept.com/2020/10/21/dataminr-twitter-surveillance-racial-profiling/

Black, Claire, “Restricting the Rainbow”, *Craccum*, May 2017, pp. 24–25. Retrieved 5 May 2024 from: http://www.craccum.co.nz/wp-content/uploads/2018/07/Craccum-08-2017.pdf

Black, Claire (2018), *Rainbow Connections: LGBTQ Young People’s use of Digital Technologies in New Zealand*, http://hdl.handle.net/2292/45224

Bridle, James, “So, Amazon’s ‘AI-powered’ cashier-free shops use a lot of … humans. Here’s why that shouldn’t surprise you”, *The Guardian*, 10 April 2024. Retrieved 30 May 2024 from: https://www.theguardian.com/commentisfree/2024/apr/10/amazon-ai-cashier-less-shops-humans-technology

“Buffalo mass shooting livestream and ‘manifesto’ permanently banned” (15 June 2022), Classification Office. Retrieved 2 May 2024 from: https://www.classificationoffice.govt.nz/news/news-items/buffalo-mass-shooting-livestream-and-manifesto-permanently-banned/

Burke, Colin and Cinnamon Bloss (Nov. 2020), "Social Media Surveillance in Schools: Rethinking Public Health Interventions in the Digital Age", *J Med Internet Res* 22(11), DOI: 10.2196/22612.

Campbell, Josh and Kat Jaeger, "High-profile political figures are the targets in the latest wave of 'swatting' incidents. Why the trend is so alarming", *CNN*, updated 15 Jan. 2024. Retrieved 30 May 2024 from: https://edition.cnn.com/2024/01/14/us/swatting-incidents-trend-explained/index.html

Cardwell, Hamish, "Police lawyers advised photographing youth likely breached UN protections for children", *New Zealand Herald*, 8 March 2023. Retrieved 30 April 2024 from: https://www.nzherald.co.nz/nz/police-lawyers-advised-photographing-youth-likely-breached-un-protections-for-children/GOHFWTSSA5EUXGBCURRXHB7J4I/

Cardwell, Hamish, "Supreme Court case raises questions of police powers, lawyer says", *RNZ*, 6 March 2024. Retrieved 5 June 2024 from: https://www.rnz.co.nz/news/national/511028/supreme-court-case-raises-questions-of-police-powers-lawyer-says

"Chapter 2: The three ways the individual may have been detected" (8 Dec. 2020), in *Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques on 15 March 2019*, Part 7. Retrieved 5 June 2024 from: https://christchurchattack.royalcommission.nz/the-report/part-7-detecting-a-potential-terrorist/the-three-ways-the-individual-may-have-been-detected/

"Chapter 4: What communities told us about the broader context in which the terrorist attack occurred" (8 Dec. 2020), in *Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques on 15 March 2019*, Part 3. Retrieved 5 June 2024 from: https://christchurchattack.royalcommission.nz/the-report/voices-of-the-community/what-communities-told-us-about-the-broader-context-in-which-the-terrorist-attack-occurred/

"Chapter 5: What people told us about the national security system and counter-terrorism effort" (26 Nov. 2020), in *Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques on 15 March 2019*, Summary of Submissions. Retrieved 28 May 2024 from: https://christchurchattack.royalcommission.nz/assets/Publications/Summary-of-submissions.pdf

"Chapter 5: Harmful behaviours, right-wing extremism and radicalisation" (8 Dec. 2020), in *Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques on 15 March 2019*, Part 2. Retrieved 5 June 2024 from: https://christchurchattack.royalcommission.nz/the-report/part-2-context/harmful-behaviours-right-wing-extremism-and-radicalisation/

"Chapter 6: Planning the terrorist attack" (8 Dec. 2020), in *Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques on 15 March 2019*, Part 4. Retrieved 11 June 2024 from https://www.christchurchattack.royalcommission.nz/the-report/firearms-licensing/planning-the-terrorist-attack/

"Chapter 21: Creating powers of search, surveillance and seizure" (2021), Legislation Design and Advisory Committee. Retrieved 5 June 2024 from: https://www.ldac.org.nz/guidelines/legislation-guidelines-2021-edition/new-powers-and-entities-2/chapter-21/

Checkpoint, "What will National's crackdown on gangs look like?", *RNZ*, 25 Oct. 2023. Retrieved 24 April 2024 from: https://www.rnz.co.nz/national/programmes/checkpoint/audio/2018912603/what-will-national-s-crackdown-on-gangs-look-like

Chen, Serena (2020), "The Spread of Online Fascism | Te Horapa o te Mana Whakamatua Kotahi i te Ao Tuihono", in *Shouting Zeros and Ones: Digital Technology, Ethics and Policy in New Zealand*, Andrew Chen, ed., Wellington: Bridget Williams Books Ltd

Christchurch Call to Eliminate Terrorist & Violent Extremist Content Online (n.d.). Retrieved 6 May 2024 from: https://www.christchurchcall.com/

Clark, Emily, "After the Christchurch attacks, Twitter made a deal with Jacinda Ardern over violent content. Elon Musk changed everything", *RNZ*, 28 April 2024. Retrieved 5 June 2024 from: https://www.rnz.co.nz/news/world/515401/after-the-christchurch-attacks-twitter-made-a-deal-with-jacinda-ardern-over-violent-content-elon-musk-changed-everything

"Classification Office response to the March 2019 Christchurch terrorist attack" (9 Dec. 2020), Classification Office. Retrieved 2 May 2024 from: https://www.classificationoffice.govt.nz/news/news-items/response-to-the-march-2019-christchurch-terrorist-attack/

"Co-designing Māori data governance" (2 Feb. 2021), Data.govt.nz. Retrieved 29 April 2024 from: https://www.data.govt.nz/toolkit/data-governance/maori/

Cohen, Julie (2000), "Examined Lives: Informational Privacy and the Subject as Object", *52 Stan L Rev* 1373. Retrieved 23 May 2024 from: https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1819&context=facpub

"Collecting your information" (n.d.), Work and Income | Te Hiranga Tangata. Retrieved 10 June 2024 from: https://www.workandincome.govt.nz/about-work-and-income/privacy-notice/collecting-your-information.html

"Collection of personal information" (n.d.), New Zealand Police. Retrieved 26 April 2024 from: https://www.police.govt.nz/sites/default/files/publications/privacy-collection-of-personal-information-090622.pdf

Comerford, Milo, Jakob Guhl and Carl Miller (2021), *Understanding the New Zealand Online Extremist Ecosystem*. Retrieved 5 May 2024 from: https://www.isdglobal.org/wp-content/uploads/2021/06/NZ-Online-Extremism-Findings-Report.pdf

Comerford, Milo, Jacob Davey, Jakob Guhl, Hannah Rose and Michel Seibriger (15 March 2024), "Five years on from Christchurch: Assessing the evolution of the threat

landscape and policy response", Institute for Strategic Dialogue. Retrieved 5 June 2024 from: https://www.isdglobal.org/digital_dispatches/five-years-on-from-christchurch-assessing-the-evolution-of-the-threat-landscape-and-policy-response/

"Comments submitted to the Federal Trade Commission on social media monitoring" (21 Nov. 2022), Brennan Center for Justice. Retrieved 5 June 2024 from: https://www.brennancenter.org/our-work/research-reports/comments-submitted-federal-trade-commission-social-media-monitoring

Cooke, Henry, "Bridges v Coster: Top cop in fiery spat with National MP over gang numbers and 'policing by consent'", *Stuff*, 25 Feb. 2021. Retrieved 5 June 2024 from: https://www.stuff.co.nz/national/300239000/bridges-v-coster-top-cop-in-fiery-spat-with-national-mp-over-gang-numbers-and-policing-by-consent

Cooke, Henry and Bernadette Basagre, "Government to formally apologise for race-based dawn raids", *Stuff*, 14 June 2021. Retrieved 26 May 2024 from: https://www.stuff.co.nz/national/politics/300332534/government-to-formally-apologise-for-racebased-dawn-raids

Coordinated Review of the Management of the LynnMall Supermarket Attacker (14 Dec. 2022), Inspector-General of Intelligence and Security, Independent Police Conduct Authority, and Office of the Inspectorate. Retrieved 30 April 2024 from: https://inspectorate.corrections.govt.nz/__data/assets/pdf_file/0003/49179/14_DECEMBER_2022_-_Coordinated_Review_of_the_Management_of_the_LynnMall_Supermarket_Attacker.pdf

Consent to Assume Online Identity (n.d.), New Zealand Police. Retrieved 5 April 2024 from: https://fyi.org.nz/request/17510/response/68403/attach/3/Harris%20Alex%20IR%2001%2021%2036948%20signed%20response.pdf

Coquilhat, Jenny (Sept. 2008), *Community Policing: An International Literature Review*. Wellington: New Zealand Police. Retrieved 26 May 2024 from: https://www.police.govt.nz/resources/2008/community-policing-lit-review/elements-of-com-policing.pdf

Cormack, Donna, Tahu Kukutai and Chris Cormack (2020), "Not One Byte More | Kia Kaua Tētahi Paita Anō", in *Shouting Zeros and Ones: Digital Technology, Ethics and Policy in New Zealand*, Andrew Chen, ed., Wellington: Bridget Williams Books Ltd

"Country reports on the functioning of the adequacy decisions adopted under Directive 95/46/EC" (15 Jan. 2024), European Commission Staff Working Document. Retrieved 3 May 2024 from: https://commission.europa.eu/system/files/2024-01/JUST_template_comingsoon_Commission%20Staff%20Working%20Document%20-%20Report%20on%20the%20first%20review%20of%20the%20functioning.pdf

"Covid-19 Outbreak: Investigating a Threat Actor" (March 2020), Voyager Labs. Retrieved 5 June 2024 from: https://www.brennancenter.org/sites/default/files/2021-11/J945-954-%20Investigating%20a%20Threat%20Actor.pdf

Daalder, Marc, “Fake accounts used hundreds of times in immigration investigations”, *Newsroom*, 8 June 2021. Retrieved 1 May 2024 from: https://newsroom.co.nz/2021/06/08/fake-accounts-used-hundreds-of-times-in-immigration-investigations/

de Silva, Tommy, “The principles of the Treaty of Waitangi, explained”, *The Spinoff*, 3 Feb. 2024. Retrieved 5 May 2024 from: https://thespinoff.co.nz/atea/03-02-2024/the-principles-of-the-treaty-of-waitangi-explained.

Desmarais, Felix, “Gang patch ban inconsistent with rights — Attorney General”, *1News*, 7 March 2024. Retrieved 24 April 2024 from: https://www.1news.co.nz/2024/03/07/gang-patch-ban-inconsistent-with-rights-attorney-general/

Digital Violent Extremism Transparency Report (2022), Te Tari Taiwhenua | Internal Affairs. Retrieved 1 May 2024 from: https://www.dia.govt.nz/diawebsite.nsf/Files/Countering-violent-extremism-online/$file/DVE-Transparency-Report-2022.pdf

Digital Violent Extremism Transparency Report (2023), Te Tari Taiwhenua | Internal Affairs. Retrieved 9 May 2024 from: https://www.dia.govt.nz/diawebsite.nsf/Files/Countering-violent-extremism-online/$file/DVE-Transparency-Report-2023.pdf

Dvilyanski, Mike, David Agranovich and Nathaniel Gleicher (Dec. 2021), *Threat Report on the Surveillance-for-Hire Industry*. Retrieved 8 April 2024 from: https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

Edens, John, “Immigration NZ, MBIE use fake social media profiles”, *RNZ*, 27 Sept. 2017. Retrieved 5 April 2024 from: https://www.rnz.co.nz/news/national/340384/immigration-nz-mbie-use-fake-social-media-profiles

Edmunds, Susan, “Benefit relationship test ‘is putting our lives on hold’”, *Stuff*, 30 Sept. 2019. Retrieved 28 May 2024 from: https://www.stuff.co.nz/business/116188360/benefit-relationship-test-is-putting-our-lives-on-hold

Edwards, Lilian and Lachlan Urquhart (11 Dec. 2015), “Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?”, *Int’l Journal of Law and Information Tech* (Autumn 2016) 24(3), 279-310. Retrieved 28 May 2024 from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2702426

“Enforcement, offences and penalties” (n.d.), Te Mana Whakaatu | Classification Office. Retrieved 2 May 2024 from: https://www.classificationoffice.govt.nz/classification-info/enforcement-offences-penalties/

Ensor, Jamie, “Government announces new aggravating factor for people using children to commit crime, crackdown on posting offending to social media”,

Newshub, 17 July 2023. Retrieved 1 May 2024 from: https://www.newshub.co.nz/home/politics/2023/07/government-announces-new-offence-for-people-using-children-to-commit-crime-crackdown-on-posting-offending-to-social-media.html

Espiner, Guyon, "Police try to assume people's online identities to gather information", *RNZ*, 10 Nov. 2021. Retrieved 5 April 2024 from: https://www.rnz.co.nz/news/top/455331/police-try-to-assume-people-s-online-identities

"Executive summary" (8 Dec. 2020), in *Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques on 15 March 2019*. Retrieved 5 June 2024 from: https://christchurchattack.royalcommission.nz/the-report/executive-summary-2/executive-summary/

Farivar, Cyrus and Olivia Solon, "FBI trawled Facebook to arrest protestors for inciting riots, court records show", *NBC News*, 20 June 2020. Retrieved 5 June 2024 from: https://www.nbcnews.com/tech/social-media/federal-agents-monitored-facebook-arrest-protesters-inciting-riots-court-records-n1231531

Farzan, Antonia Noori, "Memphis police used fake Facebook account to monitor Black Lives Matter, trial reveals", *Washington Post*, 23 Aug. 2018. Retrieved 5 June 2024 from: https://www.washingtonpost.com/news/morning-mix/wp/2018/08/23/memphis-police-used-fake-facebook-account-to-monitor-black-lives-matter-trial-reveals/

Fisher, David, "Police software mines social media," *New Zealand Herald*, 23 Feb. 2013. Retrieved 9 April 2024 from: https://www.nzherald.co.nz/nz/police-software-mines-social-media/WQM7OYWWXJEKL2EMZOAGVUKXBE/

Foon, Eleisha, "Christchurch terror attack report: 'We should have been safe here' – mosque leaders", *RNZ*, 8 Dec. 2020. Retrieved 5 June 2024 from: https://www.rnz.co.nz/news/national/432394/christchurch-terror-attack-report-we-should-have-been-safe-here-mosque-leaders

"Founding and Early History of New Zealand Council for Civil Liberties" (13 Aug. 2023), New Zealand Council for Civil Liberties. Retrieved 6 May 2024 from: https://nzccl.org.nz/the-founding-and-early-history-of-the-new-zealand-council-for-civil-liberties/

Fox, Chris, "TikTok admits restricting some LGBTQ hashtags", *BBC.com*, 10 Sept. 2020. Retrieved 5 April 2024 from: https://www.bbc.com/news/technology-54102575

Furze, Leon (May 2024), "Don't use Generative AI to grade student work. It's that simple", LinkedIn. Retrieved 5 June 2024 from: https://www.linkedin.com/posts/leonfurze_ai-aieducation-aiassessment-activity-7200342216626589696-NQXN/

Gee, Samantha, "Drugs, social media and new territory factors in rising gang numbers, police say", *Stuff*, 28 May 2021. Retrieved 30 April 2024 from:

https://www.stuff.co.nz/national/crime/125237016/drugs-social-media-and-new-territory-factors-in-rising-gang-numbers-police-say

Green, Jordan (July 2020), *Māori Instagram: The social media lifeworlds and decolonising practices of Rangatahi Māori*. Retrieved 27 May 2024 from: https://ourarchive.otago.ac.nz/esploro/outputs/graduate/M%C4%81ori-Instagram-The-Social-Media-Lifeworlds/9926480246601891?institution=64OTAGO_INST#file-0

Greener, Bethan, "Policing by consent is not 'woke' — it is fundamental to a democratic society", *The Conversation*, 24 Feb. 2021. Retrieved 29 April 2024 from: https://theconversation.com/policing-by-consent-is-not-woke-it-is-fundamental-to-a-democratic-society-155866

Halpin, James and Chris Wilson (2022), "How online interaction radicalises while group involvement restrains: a case study of Action Zealandia from 2019 to 2021", *Political Science*. DOI: 10.1080/00323187.2022.2101493

Hartocollis, Anemona, "Palestinian Harvard student blocked from coming to U.S. is allowed to enter", *New York Times*, 3 Sept. 2019. Retrieved 5 May 2024 from: https://www.nytimes.com/2019/09/03/us/palestinian-harvard-student.html

Hattotuwa, Sanjana, Kate Hannah and Kayli Taylor (April 2023), *Transgressive Transitions: Transphobia, community building, bridging, and bonding within Aotearoa New Zealand's disinformation ecologies March–April 2023*, The Disinformation Project. Retrieved 5 May 2024 from: https://static1.squarespace.com/static/65c9ceb1a6a5b72d6f280d67/t/65cc227b8c94e134021c9141/1707877007526/Transgressive-Transitions.pdf

Herold, Benjamin, "Schools are deploying massive digital surveillance systems. The results are alarming", *EducationWeek*, 30 May 2019. Retrieved 5 May 2024 from: https://www.edweek.org/technology/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05

Heron, Michael QC (14 March 2022), *ACRE–INZ Review, Final Report*. Retrieved 5 June 2024 from: https://www.mbie.govt.nz/dmsdocument/25830-operational-review-into-immigration-new-zealands-handling-of-acre

Hill, Richard (2008), "Māori, Police and Coercion in New Zealand History", in *Terror In Our Midst? Searching for Terror in Aotearoa New Zealand*, Danny Keenan, ed., Wellington: Huia Publishers

Hill, Ruth, "Privacy fears over New Zealand government departments' use of Google Analytics", *New Zealand Herald*, 11 April 2023. Retrieved 7 June 2024 from: https://www.nzherald.co.nz/nz/privacy-fears-over-new-zealand-government-departments-use-of-google-analytics/LAOGHBZ3YNDRZOCSOVM6MKRP3E/

Hlass, Laila L. and Rachel Prandini (21 May 2018), *Deportation by Any Means Necessary: How Immigration Officials Are Labeling Immigrant Youth as Gang Members*, Immigrant Legal Resource Center. Retrieved 3 May 2024

from: https://www.ilrc.org/sites/default/files/resources/deport_by_any_means_nec-20180521.pdf

"How NZ responds to violent extremism online" (n.d.), Te Tari Taiwhenua | Internal Affairs. Retrieved 5 June 2024 from: https://www.dia.govt.nz/Countering-Violent-Extremism-How-NZ-responds-to-violent-extremism-online

"Hui Summary and Compendium" (15–16 June 2021), *He Whenua Tauikura Hui: New Zealand's Hui on Countering Terrorism and Violent Extremism*, Department of the Prime Minister and Cabinet. Retrieved 27 May 2024 from: https://www.dpmc.govt.nz/sites/default/files/2021-09/He%20Whenua%20Taurikura%202021%20-%20hui%20compendium_1.pdf

"Hui Summary and Compendium" (30 Oct.–1 Nov. 2022), *He Whenua Taurikura, New Zealand's Hui on Countering Terrorism and Violent Extremism*, Department of the Prime Minister and Cabinet. Retrieved 27 May 2024 from: https://www.dpmc.govt.nz/sites/default/files/2022-12/hui-summary-report-2022-compendium.pdf

Hurihanganui, Te Aniwa, "Police using app to photograph innocent youth: 'It's so wrong'", *RNZ*, 26 March 2021. Retrieved 29 April 2024 from: https://www.rnz.co.nz/news/in-depth/437944/police-using-app-to-photograph-innocent-youth-it-s-so-wrong

"Information gathering standards update" (23 April 2019), Te Kawa Mataaho | Public Service Commission. Retrieved 5 June 2024 from: https://www.publicservice.govt.nz/news/information-gathering-standards-update

"Information Summary — Kellie-Jay KEEN-MINSHULL" (20 March 2023), Ministry of Business, Innovation & Employment, Immigration New Zealand Verification Network, disclosed in Official Information Act response, pp. 11–20. Retrieved 5 June 2024 from: https://fyi.org.nz/request/22297/response/85027/attach/4/Appendix%20One%20Part%202.pdf

Inquiry into the Ministry of Social Development's Exercise of Section 11 (Social Security Act 1964) and Compliance with the Code of Conduct (May 2019), Office of the Privacy Commissioner. Retrieved 6 May 2024 from: https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Commissioner-inquiries/Privacy-Commissioners-Inquiry-in-MSDs-Exercise-of-s.11-SSA-1964-and-Compliance-of-the-Code-of-Conduct-Final-Report.pdf

"Intelligence collection" (n.d.), Government Security Communications Bureau. Retrieved 2 May 2024 from: https://www.gcsb.govt.nz/our-work/intelligence-collection/

"Intelligence notification: Let Women Speak tour" (17 March 2023), New Zealand Police, disclosed in response to Official Information Act request, pp. 24–31. Retrieved 5 June 2024 from: https://fyi.org.nz/request/22297/response/85027/attach/4/Appendix%20One%20Part%202.pdf

Investigation of the RCMP's collection of open-source information under Project Wide Awake (15 Feb. 2024), Office of the Privacy Commissioner of Canada. Retrieved 29 May 2024 from: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/sr_pa_20240215_rcmp-pwa/#toc0

Joint inquiry by the Independent Police Conduct Authority and the Privacy Commissioner into Police conduct when photographing members of the public (Sept. 2022), Privacy Commissioner and Independent Police Conduct Authority. Retrieved 30 April 2024 from: https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Commissioner-inquiries/8-SEPTEMBER-2022-IPCA-AND-OPC-Joint-Inquiry-into-Police-photographing-of-members-of-the-public.pdf

Joint statement on data scraping and the protection of privacy (Aug. 2023), Office of the Australian Information Commissioner et al. Retrieved 5 May 2024 from: https://www.oaic.gov.au/newsroom/global-expectations-of-social-media-platforms-and-other-sites-to-safeguard-against-unlawful-data-scraping

Judd, Alan, "L.A.'s Gang-Tracking Database Offers Lessons to Others", *GovTech*, 9 March 2020. Retrieved 6 May 2024 from: https://www.govtech.com/public-safety/las-gang-tracking-database-offers-lessons-to-others.html

Kaye, David (11 May 2016), *Report on freedom of expression, states and the private sector in the digital age*. Retrieved 15 May 2024 from: https://www.ohchr.org/en/calls-for-input/report-freedom-expression-states-and-private-sector-digital-age

Kaye, David (29 Aug. 2018), *Report on Artificial Intelligence technologies and implications for freedom of expression and the information environment*. Retrieved 23 May 2024 from: https://www.ohchr.org/en/calls-for-input/report-artificial-intelligence-technologies-and-implications-freedom-expression-and

Kitteridge, Rebecca (18 Sept. 2019), "Speech: Understanding Intelligence", Address to the Institute of Public Administration New Zealand. Retrieved 11 April 2024 from: https://www.nzsis.govt.nz/news/speech-understanding-intelligence/

Kukutai, Tahu, Kyla Campbell-Kamariera, Aroha Mead, Kirikowhai Mikaere, Caleb Moses, Jesse Whitehead and Donna Cormack (2023-a), *Māori data governance model*, Te Kāhui Raraunga. Retrieved 4 June 2024 from: https://www.kahuiraraunga.io/_files/ugd/b8e45c_803c03ffe532414183afcd8b9ced10dc.pdf

Kukutai, Tahu, Shemana Cassim, Vanessa Clark, Nicholas Jones, Jason Mika, Rhianna Morar, Marama Muru-Lanning, Robert Pouwhare, Vanessa Teague, Lynell Tuffery Huria, David Watts and Rogena Sterling (2023-b), *Māori data sovereignty and privacy*. Tikanga in Technology discussion paper. Hamilton: Te Ngira Institute for Population Research. Retrieved 4 June 2024 from: https://www.waikato.ac.nz/assets/Uploads/Research/Research-institutes-centres-and-groups/Institutes/Te-Ngira-Institute-for-Population-Research/MDSov-and-Privacy_20March2023_v2.pdf

Lal, Shaneel (2023), *One Of Them*, Auckland: Allen & Unwin NZ

"Launch of Te Tari Pureke — Firearms Safety Authority" (30 Nov. 2022), New Zealand Police. Retrieved 6 June 2024 from: https://www.police.govt.nz/news/release/launch-te-tari-p%C5%ABreke-firearms-safety-authority

Law Commission and Ministry of Justice (June 2017), *Review of the Search and Surveillance Act 2012 — Report 141* (Wellington). Retrieved 5 May 2024 from: https://www.lawcom.govt.nz/assets/Publications/Reports/NZLC-R141.pdf

Law Commission and Ministry of Justice (Nov. 2016), *Review of the Search and Surveillance Act 2012 — Issues Paper* (Wellington). Retrieved 5 May 2024 from: https://www.lawcom.govt.nz/assets/Publications/IssuesPapers/NZLC-IP40.pdf

Leask, Anna, "Social media giant TikTok deletes, bans thousands of NZ gang-linked accounts, videos — promises more to come", *New Zealand Herald*, 29 June 2023. Retrieved 30 May 2024 from: https://www.nzherald.co.nz/nz/cancelled-social-media-giant-tiktok-deletes-bans-thousands-of-nz-gang-linked-accounts-videos-promises-more-to-come/KMZDEB77MNCOBJQLZOGXWIO4EI/

Leffer, Lauren, "Your personal information is probably being used to train generative AI models", *Scientific American*, 19 Oct. 2023. Retrieved 28 May 2024 from: https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/

Letter from ACLU Foundation of Northern California, Brennan Center for Justice, and ACLU to US Federal Trade Commission (12 Dec. 2023). Retrieved 5 June 2024 from: https://www.aclunc.org/sites/default/files/2023.12.12_ACLU%20NorCal_Brennan%20Center_ACLU_Letter_Social_Media_Surveillance.pdf

Letter from Facebook to Memphis Police Department (19 Sept. 2018). Retrieved 5 June 2024 from: https://www.eff.org/document/facebook-letter-memphis-police-department-fake-accounts

Levin, Sam, "Revealed: LAPD officers told to collect social media data on every civilian they stop", *The Guardian*, 8 Sept. 2021. Retrieved 5 June 2024 from: https://www.theguardian.com/us-news/2021/sep/08/revealed-los-angeles-police-officers-gathering-social-media

Levinson-Waldman, Rachel and Ángel Díaz, "How to reform police monitoring of social media", *Brookings*, 9 July 2020. Retrieved 3 May 2024 from: https://www.brookings.edu/articles/how-to-reform-police-monitoring-of-social-media/

Levinson-Waldman, Rachel and Mary Pat Dwyer (17 Nov. 2021), "LAPD documents show what one social media surveillance firm promises police", Brennan Center for Justice. Retrieved 5 June 2024 from: https://www.brennancenter.org/our-work/analysis-opinion/lapd-documents-show-what-one-social-media-surveillance-firm-promises

Levinson-Waldman, Rachel, Harsha Panduranga and Faiza Patel (7 Jan. 2022), "Social media surveillance by the U.S. government", Brennan Center for Justice. Retrieved 5 June 2024 from: https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government

Levinson-Waldman, Rachel (7 Feb. 2024-a), "Principles for Social Media Use by Law Enforcement", Brennan Center for Justice. Retrieved 5 May 2024 from: https://www.brennancenter.org/our-work/research-reports/principles-social-media-use-law-enforcement

Levinson-Waldman, Rachel (7 Feb. 2024-b), "Directory of Police Department Social Media Policies", Brennan Center for Justice. Retrieved 28 May 2024 from: https://www.brennancenter.org/our-work/research-reports/directory-police-department-social-media-policies

Lindgren, Simon and Coppélie Cocq (2017), "Turning the inside out: Social media and the broadcasting of indigenous discourse", *European Journal of Communication* 32(2), 131–150. https://doi.org/10.1177/0267323116674112

Lindsay, Angus, Trevor Bradley, and Simon MacKenzie (2022), "Organisational barriers to institutional change: The case of intelligence in New Zealand policing", *Howard J Crim Justice* 61, 407–426. Retrieved 23 May 2024 from: https://onlinelibrary.wiley.com/doi/epdf/10.1111/hojo.12486

Livingstone, Sonia, Mariya Stoilova and Rishita Nandagiri (2019), *Children's data and privacy online: Growing up in a digital age. An evidence review*. London: London School of Economics and Political Science. Retrieved 5 May 2024 from: https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf

MPI Privacy and Transparency Commitment (n.d.), Ministry for Primary Industries. Retrieved 10 June 2024 from: https://www.mpi.govt.nz/dmsdocument/35520/direct

"MSD investigations and social media" (10 Feb. 2016), Ministry of Social Development media release. Retrieved 5 June 2024 from: https://www.msd.govt.nz/about-msd-and-our-work/newsroom/media-releases/2016/msd-investigations-and-social-media.html

Maher, Rachel, "Expert says National's gang-busting social media policy nearly impossible to police, while proposals may infringe on Bill on Rights", *New Zealand Herald*, 12 June 2022. Retrieved 24 April 2024 from: https://www.nzherald.co.nz/nz/expert-says-nationals-gang-busting-social-media-policy-nearly-impossible-to-police-while-proposals-may-infringe-on-bill-on-rights/MG3GYKSCBWA2WXCP72VWYBAFPQ/

Marcelo, Philip, "Court Decision Deals Blow to Boston Police Gang Database", *Boston.com*, 12 Jan. 2022. Retrieved 3 May 2024 from: https://www.boston.com/news/local-news/2022/01/12/court-decision-deals-blow-to-boston-police-gang-database

Martin, Cathy, "Instagram egregiously mistranslates Palestinian user bios, inserting word 'terrorist'", *Multilingual.com*, 26 Oct. 2023. Retrieved 5 May 2024 from: https://multilingual.com/instagram-egregiously-mistranslates-palestinian-user-bios-inserting-word-terrorist/

Martin, Doug and Simon Mount, QC (18 Dec. 2018), *Inquiry into the use of external security consultants by government agencies*. Retrieved 5 May 2024 from: https://www.publicservice.govt.nz/publications/inquiry-into-the-use-of-external-security-consultants-by-government-agencies.

"Master agreement for advanced social media search training" (12 Dec. 2017), between Ministry of Business, Innovation & Employment and ZX Security Limited. Retrieved 1 May 2024 from: https://www.documentcloud.org/documents/5677593-Section-6-Contracts-and-Policies-Relating-to

Matika, Correna (Dec. 2023), *New Zealand's Internet Insights 2023*. Retrieved 11 April 2024 from: https://internetnz.nz/assets/Uploads/New-Zealands-Internet-Insights-2023-v2.pdf

McCann, Mitch, "Police warn gangs using Instagram, TikTok to recruit younger members", *Newshub*, 23 Aug. 2020. Retrieved 30 May 2024 from: https://www.newshub.co.nz/home/new-zealand/2020/08/police-warn-gangs-using-instagram-tiktok-to-recruit-younger-members.html

McCaull, Ashleigh, "Rates of Māori stood down from school twice that of Pākeha students", *RNZ*, 19 Dec. 2022. Retrieved 5 May 2024 from: https://www.rnz.co.nz/news/te-manu-korihi/481012/rates-of-maori-stood-down-from-school-twice-that-of-pakeha-students

McClure, Tess and Charlotte Graham-McLay, "Anti-trans activist Posie Parker leaves New Zealand after chaotic protests", *The Guardian*, 26 March 2023. Retrieved 30 May 2024 from: https://www.theguardian.com/world/2023/mar/25/anti-trans-activist-posie-parker-ends-new-zealand-tour-after-violent-protests-erupt

McKenzie, Peter, "How art and technology mobilised an army of support for Ihumātao," *The Spinoff*, 1 Aug. 2019. Retrieved 5 May 2024 from: https://thespinoff.co.nz/atea/01-08-2019/how-art-and-technology-mobilised-an-army-of-support-for-ihumatao

McNamara, Kate, "Govt warned quarter-million-dollar spend of social listening 'ethically questionable'", *New Zealand Herald*, 12 May 2022. Retrieved 1 May 2024 from: https://www.nzherald.co.nz/business/govt-warned-quarter-million-dollar-spend-of-social-listening-ethically-questionable/LZJAM4HCP4RTVJKKJKV45P4NNY/

McNamara, Kate, "Social media surveillance included Kiwis' private messages sent to Government", *New Zealand Herald*, 8 June 2022. Retrieved 1 May 2024 from: https://www.nzherald.co.nz/business/social-media-surveillance-included-kiwis-private-messages-sent-to-government/6YG3KCJJYPMOQF5HHHPEY6R5TI/.

Ministerial Policy Statement: Publicly available information (1 March 2022). Wellington: Government Communications Security Bureau and New Zealand

Security Intelligence Service. Retrieved 30 April 2024 from: https://www.nzsis.govt.nz/assets/Ministerial-Policy-Statements-2022/MPS-Publicly-available-information.pdf

Morse, Valerie (2019a), "Peace, Action, and Anarchist Organising for Aotearoa" (interview with Murdoch Stephens), in *Counterfutures: Left Thought and Practice Aotearoa* (Vol. 7). Retrieved 5 May 2024 from: https://ojs.victoria.ac.nz/counterfutures/article/view/6373/5526

Morse, Valerie (2019b), "Spies wide shut: Responses and resistance to the national security state in Aotearoa New Zealand", in *Activists and the surveillance state: Learning from repression*, Aziz Choudry, ed., London: Pluto Press

Murphy, "Pride and police: The history, issues and decisions behind the debate", *RNZ*, 27 Nov. 2018. Retrieved 5 June 2024 from: https://www.rnz.co.nz/news/national/376950/pride-and-police-the-history-issues-and-decisions-behind-the-debate

Natanson, Hannah, "Objection to sexual, LGBTQ content propels spike in book challenges", *Washington Post*, updated 9 June 2023. Retrieved 5 May 2024 from: https://www.washingtonpost.com/education/2023/05/23/lgbtq-book-ban-challengers/.

"National Security & Intelligence: The Role of Government Agencies" (Feb. 2023), National Security Workforce. Retrieved 1 May 2024 from: https://www.dpmc.govt.nz/sites/default/files/2023-04/National-Security-and-Intelligence-Role-of-Government-Agencies-updated-February-2023.pdf

"New Public Service Act underlines spirit of service" (7 Aug. 2020), Te Kawa Mataaho | Public Service Commission. Retrieved 5 June 2024 from: https://www.publicservice.govt.nz/news/new-public-service-act-underlines-spirit-of-service

New Technology Framework (2021), New Zealand Police. Retrieved 30 April 2024 from: https://www.police.govt.nz/sites/default/files/publications/new-technology-framework.pdf

New Zealand Gang Membership: A snapshot of recent trends (July 2022), Parliamentary Service. Retrieved 7 April 2024 from: https://www.parliament.nz/en/pb/library-research-papers/research-papers/new-zealand-gang-membership-a-snapshot-of-recent-trends/

New Zealand Online Crisis Response Process (n.d.), Te Tari Taiwhenua | Internal Affairs. Retrieved 12 April 2024 from: https://www.dia.govt.nz/diawebsite.nsf/Files/New%20Zealand%20Online%20Process/$file/New%20Zealand%20Online%20Crisis%20Response%20Process.pdf

New Zealand's Security Threat Environment 2023 (Aug. 2023), Te Pā Whakamarumaru | New Zealand Security Intelligence Service. Retrieved 29 May 2024 from: https://www.nzsis.govt.nz/assets/NZSIS-Documents/New-Zealands-Security-Threat-Environment-2023.pdf.

Nine to Noon, NZ's "Disinformation Dozen," *RNZ*, 18 May 2022. Retrieved 24 April 2024 from: https://www.rnz.co.nz/national/programmes/ninetonoon/audio/2018842409/nz-s-disinformation-dozen

North, Madeleine, "Generative AI is trained on just a few of the world's 7,000 languages. Here's why that's a problem — and what's being done about it", *World Economic Forum*, 17 May 2024. Retrieved 11 June 2024 from: https://www.weforum.org/agenda/2024/05/generative-ai-languages-llm/

"NZ police case study: Social media opens up a new world of real-time intelligence" (6 Jan. 2014), Informa Insights. Retrieved 30 May 2024 from: https://www.informa.com.au/insight/nz-police-case-study-social-media-opens-up-a-new-world-of-real-time-intelligence/

"OECD: High level of trust in the Public Service" (n.d.), Te Kawa Mataaho | Public Service Commission. Retrieved 5 June 2024 from: https://www.publicservice.govt.nz/news/oecd-high-level-of-trust-in-the-public-service

"Objectionable and restricted material" (n.d.), Te Tari Taiwhenua | Internal Affairs. Retrieved 5 June 2024 from: https://www.dia.govt.nz/Digital-Child-Exploitation-Objectionable-and-Restricted-Material

"Operation H Case Study" (n.d.), Te Tari Taiwhenua | Internal Affairs. Retrieved 1 May 2024 from: https://www.dia.govt.nz/Preventing-Online-Child-Sexual-Exploitation-Operation-H-case-study

"Operation 8: The evidence and police spying methods" (Nov. 2013), *Te Putatara*. Retrieved 4 April 2024 from: https://putatara.net/2013/11/25/operation-8-the-evidence/

Orange, Claudia (updated 28 March 2023), "Te Tiriti o Waitangi — the Treaty of Waitangi", *Te Ara — the Encyclopedia of New Zealand*. Retrieved 6 June 2024 from: https://teara.govt.nz/en/te-tiriti-o-waitangi-the-treaty-of-waitangi/print

"Our methods" (n.d.), New Zealand Security Intelligence Service. Retrieved 2 May 2024 from: https://www.nzsis.govt.nz/about-us/our-methods/

"Our privacy and transparency commitment" (n.d.), Ara Poutama Aotearoa | Department of Corrections. Retrieved 11 June 2024 from: https://www.corrections.govt.nz/about_us/who_we_are/our_privacy_commitment

"Our privacy policy" (n.d.), Inland Revenue | Te Tari Taake. Retrieved 10 June 2024 from: https://www.ird.govt.nz/about-this-site/your-privacy/privacy-policy

"Our role" (n.d.), Te Mana Whakaatu | Classification Office. Retrieved 2 May 2024 from: https://www.classificationoffice.govt.nz/about/our-role/

"Overcoming preconceptions: How big data can gain a social licence in New Zealand" (5 April 2023), Australia and New Zealand School of Government. Retrieved 5 June 2024 from: https://anzsog.edu.au/news/overcoming-preconceptions/

Paewai, Pokere, “Foodstuffs facial recognition trial: AI mistaking Māori woman as thief not surprising, experts say”, *RNZ*, 17 April 2024. Retrieved 4 June 2024 from: https://www.nzherald.co.nz/kahu/foodstuffs-facial-recognition-trial-maori-woman-mistaken-as-thief-not-surprising-experts-say/3DH6KYDHZ5GNVDUBHW5PARFGDM/

Palmer, Geoffrey (1985), “A Bill of Rights for New Zealand: A White Paper”. Wellington: Department of Justice. Retrieved 27 May 2024 from: https://www.ojp.gov/pdffiles1/Digitization/108981NCJRS.pdf

Penk, Stephen and Rosemary Tobin (eds) (2018), *Privacy Law in New Zealand*, 2nd ed, Wellington: Thomson Reuters

Pennington, Phil, “Police don’t necessarily check online activity of firearms licence applicants — lawyer”, *RNZ*, 16 March 2019. Retrieved 12 April 2024 from: https://www.rnz.co.nz/news/national/384870/police-don-t-necessarily-check-online-activity-of-firearms-licence-applicants-lawyer

Pennington, Phil, “SIS accused of breaching NZ Muslims’ rights: It’s ‘unethical, misleading’, says critic”, *RNZ*, 25 March 2019. Retrieved 5 June 2024 from: https://www.rnz.co.nz/news/national/385487/sis-accused-of-breaching-nz-muslims-rights-it-s-unethical-misleading-says-critic

Pennington, Phil, “Police had no dedicated team to scan internet before mosque attacks”, *RNZ*, 27 April 2021. Retrieved 5 April 2024 from: https://www.rnz.co.nz/news/national/441270/police-had-no-dedicated-team-to-scan-internet-before-mosque-attacks

Pennington, Phil, “Police tight-lipped on tools used to scan social media activity”, *RNZ*, 14 June 2021. Retrieved 30 April 2024 from: https://www.rnz.co.nz/news/national/444670/police-tight-lipped-on-tools-used-to-scan-social-media-activity

Pennington, Phil, “Police made false report to use ANPR cameras to track women who triggered Northland lockdown”, *RNZ*, 28 Sept. 2022. Retrieved 4 June 2024 from: https://www.rnz.co.nz/news/national/475662/police-made-false-report-to-use-anpr-cameras-to-track-women-who-triggered-northland-lockdown

Pennington, Phil, “Immigration NZ enlists ‘cyber mercenaries’ banned from Facebook to covertly collect data,” *RNZ*, 12 Oct. 2022. Retrieved 1 May 2024 from: https://www.rnz.co.nz/news/national/476506/immigration-nz-enlists-cyber-mercenaries-banned-from-facebook-to-covertly-collect-data

Pennington, Phil, “Government’s use of surveillance firm Cobwebs embroiled in controversy”, *RNZ*, 14 Oct. 2022. Retrieved 1 May 2024 from: https://www.rnz.co.nz/news/national/476659/government-s-use-of-surveillance-firm-cobwebs-technologies-embroiled-in-controversy

Pennington, Phil, Immigration minister questioned over knowledge of Cobwebs use, RNZ, 4 Dec. 2022. Retrieved 1 May 2024 from:

https://www.rnz.co.nz/news/political/480072/immigration-minister-questioned-over-knowledge-of-cobwebs-use

Pennington, Phil, MBIE expands intelligence spy unit MI beyond immigration, RNZ, 4 Oct. 2023. Retrieved 1 May 2024 from https://www.rnz.co.nz/news/national/499349/mbie-expands-intelligence-spy-unit-mi-beyond-immigration

Pennington, Phil, "Immigration New Zealand paid for spyware for 2 years without using it", *RNZ*, 9 Nov. 2023-a. Retrieved 30 April 2024 from: https://www.rnz.co.nz/news/national/502040/immigration-nz-paid-for-spyware-for-two-years-without-using-it

Pennington, Phil, "Threat reporting system to counter terrorism, extremist violence in limbo", *RNZ*, 9 Nov. 2023-b. Retrieved 5 May 2024 from: https://www.rnz.co.nz/news/national/502003/threat-reporting-system-to-counter-terrorism-extremist-violence-in-limbo

Pennington, Phil, "MBIE ends contract with spyware company — but is looking for a replacement", *RNZ*, 9 June 2024. Retrieved 10 June 2024 from: https://www.rnz.co.nz/news/national/519051/mbie-ends-contract-with-spyware-company-but-is-looking-for-a-replacement

Pereyra Garcia, Kate, "Beneficiaries being monitored online", *RNZ*, 10 Feb. 2016. Retrieved 30 May 2024 from: https://www.rnz.co.nz/news/national/296151/beneficiaries-being-monitored-online

Perez, Chris, "Boston cops used social media to spy on black, Muslim protesters: ACLU", *New York Post*, 7 Feb. 2018. Retrieved 5 June 2024 from: https://nypost.com/2018/02/07/boston-cops-used-social-media-to-spy-on-black-muslim-protesters-aclu/

"Plain English guide to offence provisions in the Films, Videos, and Publications Classification Act 1993 and its Regulations" (2015), Classification Office. Retrieved 2 May 2024 from: https://classification-office-stage.octave.nz/media/documents/Plain_English_Guide_to_the_Offence_Provisions.pdf

"Police to establish new National Gang Unit and frontline teams to increase pressure on gangs" (14 May 2024), New Zealand Police press release. Retrieved 5 June 2024 from: https://www.police.govt.nz/news/release/police-establish-new-national-gang-unit-and-frontline-teams-increase-pressure-gangs

Popper, Ben, "How the NYPD is using social media to put Harlem teens behind bars", *The Verge*, 10 Dec. 2014. Retrieved 24 April 2024 from: https://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison

"Privacy organisations" (n.d.), Digital.govt.nz. Retrieved 12 June 2024 from: https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/privacy-organisations/

"Procedures for MBIE staff using social media for verification and investigation purposes to support regulatory compliance and law enforcement work" (July 2019), Ministry of Business, Innovation, and Employment. Retrieved 30 April 2024 from: https://www.mbie.govt.nz/dmsdocument/14003-procedures-for-mbie-staff-using-social-media-for-verification-and-investigation-purposes-to-support-regulatory-compliance-and-law-enforcement-work-july-2019

"Proposed amendments to the Corrections legislative framework regarding improved safety, rehabilitation and reintegration outcomes" (9 Dec. 2022), Office of the Minister of Corrections. Retrieved 5 June 2024 from: https://www.corrections.govt.nz/__data/assets/pdf_file/0007/49399/Proposed_amendments_to_the_Corrections_legislative_framework_improved_safety,_rehabilitation_and_reintegration_outcomes_Redacted.pdf

Prothero, Arianna, "Monitoring or blocking what students do online poses all kinds of problems", *EducationWeek*, 20 Sept. 2023. Retrieved 5 June 2024 from: https://www.edweek.org/technology/monitoring-or-blocking-what-students-do-online-poses-all-kinds-of-problems/2023/09

"Public information on Facebook" (n.d.), Facebook.com. Retrieved 5 June 2024 from: https://www.facebook.com/help/203805466323736

Quince, Khylee, "Policing by consent is not 'woke' — it's the only way it can work", *Stuff*, 6 March 2021. Retrieved 27 May 2024 from: https://www.stuff.co.nz/national/politics/opinion/124445966/policing-by-consent-is-not-woke--its-the-only-way-it-can-work

Quince, Khylee and Jayden Houghton (2023), "Privacy and Māori Concepts", in *Privacy Law in New Zealand*, 3rd ed, Nikki Chamberlain and Stephen Penk, eds., Wellington: Thomas Reuters

Rapira, Laura O'Connell and Kassie Hartendorp, "Police and Pride: We need to heal our relationships first", *RNZ*, 13 Nov. 2018. Retrieved 5 June 2024 from: https://www.rnz.co.nz/news/on-the-inside/375801/police-and-pride-we-need-to-heal-our-relationships-first

Rees, Rochelle, "My partner was spying on me for the police", *Sydney Morning Herald*, 27 March 2018. Retrieved 24 May 2024 from: https://www.smh.com.au/lifestyle/life-and-relationships/my-partner-was-spying-on-me-for-the-police-20180327-p4z6h2.html

"Research on Privacy Concerns and Data Sharing" (April 2024), New Zealand Office of the Privacy Commissioner. Retrieved 5 June 2024 from: https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Surveys/2024-04-30-Privacy-Commission-Report-Mar-24-FINAL-A969809.pdf

Response to Official Information Act request (25 Aug. 2017), Ministry of Social Development. Retrieved 5 June 2024 from: https://www.msd.govt.nz/documents/about-msd-and-our-work/publications-resources/official-information-responses/2017/august/r-20170825-social-media-monitoring-for-benefit-fraud.pdf

Response to Official Information Act request (17 July 2019), State Services Commission | Te Kawa Mataaho. Retrieved 5 June 2024 from: https://www.publicservice.govt.nz/assets/DirectoryFile/OIA-response-Compliance-with-Information-Gathering-and-Public-Trust-model-standards.pdf

Response to Official Information Act request (Nov. 2020), Ministry of Social Development. Retrieved 5 June 2024 from: https://www.msd.govt.nz/documents/about-msd-and-our-work/publications-resources/official-information-responses/2020/november/13112020-request-to-details-about-benefit-fraud-investigation-processes-and-domestic-violence-p7.pdf

Response to Official Information Act request from Alex Harris (16 March 2016), Ministry of Social Development. Retrieved 5 June 2024 from: https://fyi.org.nz/request/3626/response/11823/attach/html/2/20160316%20Harris%20Alex%20Response.pdf.html

Response to Official Information Act request from Phil Pennington (27 May 2021), New Zealand Police, Reference No. 01-21-14416. Retrieved 29 May 2024 from: https://s3.documentcloud.org/documents/20860682/social-media-cover-14416-june-2021.pdf

Response to Official Information Act request from Scott (27 April 2021), New Zealand Police, file number IR-01-21-6567. Retrieved 9 April 2024 from: https://fyi.org.nz/request/14794/response/57984/attach/3/Scott%20FYI%20signed%20lettter.pdf

"Review of the Search and Surveillance Act 2012" (n.d.), Ministry of Justice. Retrieved 5 June 2024 from: https://www.justice.govt.nz/justice-sector-policy/key-initiatives/ssa/

The Review: Policing of the Protest and Occupation at Parliament 2022 (April 2023), Independent Police Conduct Authority. Retrieved 6 May 2024 from: https://www.ipca.govt.nz/includes/download.ashx?ID=164247

Risius, Marten and Stan Karanasios, "Terrorist content lurks all over the internet – regulating only 6 major platforms won't be nearly enough", *The Conversation*, 20 March 2024. Retrieved 5 June 2024 from: https://theconversation.com/terrorist-content-lurks-all-over-the-internet-regulating-only-6-major-platforms-wont-be-nearly-enough-226219

Rivlin-Nadler, Max, "How Philadelphia's social media-driven gang policing is stealing years from young people", *The Appeal*, 19 Jan. 2018. Retrieved 1 May 2024 from: https://theappeal.org/how-philadelphias-social-media-driven-gang-policing-is-stealing-years-from-young-people-fa6a8dacead9/

RNZ, "Government to question MBIE over fake persona training", 9 Jan. 2019. Retrieved 5 April 2024 from: https://www.rnz.co.nz/news/political/379727/government-to-question-mbie-over-fake-persona-training

RNZ, "ACC boss 'personally sorry' for privacy breaches made by staff", 15 June 2022. Retrieved 30 May 2024 from: https://www.rnz.co.nz/news/national/469146/acc-boss-personally-sorry-for-privacy-breaches-made-by-staff

RNZ, "MBIE tight-lipped over not consulting Privacy Commissioner on using spy firm Cobwebs", 20 Oct. 2022. Retrieved 1 May 2024 from: https://www.rnz.co.nz/news/national/477016/mbie-tight-lipped-over-not-consulting-privacy-commissioner-on-using-spy-firm-cobwebs

RNZ, "Immigration NZ says internal oversight of Cobwebs Technology is adequate", 23 Oct. 2022. Retrieved 1 May 2024 from: https://www.rnz.co.nz/news/national/477201/immigration-nz-says-internal-oversight-of-cobwebs-technologies-is-adequate

RNZ, "Anti-transgender activist Posie Parker to be allowed into New Zealand", 22 March 2023. Retrieved 30 May 2024 from: https://www.rnz.co.nz/news/national/486489/anti-transgender-activist-posie-parker-to-be-allowed-into-new-zealand

Robinson, Sara, "When a Facebook like lands you in jail", *Brennan Center for Justice*, 6 July 2018. Retrieved 24 April 2024 from: https://www.brennancenter.org/our-work/analysis-opinion/when-facebook-lands-you-jail

Romano, Aja, "How the Christchurch shooter used memes to spread hate", *Vox*, 16 March 2019. Retrieved 5 May 2024 from: https://www.vox.com/culture/2019/3/16/18266930/christchurch-shooter-manifesto-memes-subscribe-to-pewdiepie.

Roy, Eleanor Ainge, "Ihumātao sacred site bought by New Zealand government for $30m," *The Guardian*, 17 Dec. 2020. Retrieved 29 April 2024 from: https://www.theguardian.com/world/2020/dec/17/ihumatao-sacred-site-bought-by-new-zealand-government-for-30m

Royal Society Te Apārangi (Dec. 2023), *Mana Raraunga | Data Sovereignty* (Wellington). Retrieved 5 May 2024 from: https://www.royalsociety.org.nz/assets/Mana-Raraunga-Data-Sovereignty-web-V1.pdf

Ruckstuhl, Katharina (2023), "Data is a *Taonga*: Aotearoa New Zealand, Māori Data Sovereignty and Implications for Protection of Treasures", 12 *NYU Journal of Intell Prop & Ent Law* 392. Retrieved 4 June 2024 from: https://jipel.law.nyu.edu/wp-content/uploads/2023/05/JIPEL-Ruckstuhl-Special-Issue-2023.pdf

Shwartz, Vered, "Artificial intelligence needs to be trained on culturally diverse datasets to avoid bias", *The Conversation*, 14 Feb. 2024. Retrieved 11 June 2024 from: https://theconversation.com/artificial-intelligence-needs-to-be-trained-on-culturally-diverse-datasets-to-avoid-bias-222811

"Sensitive personal information and the Privacy Act 2020" (n.d.), New Zealand Office of the Privacy Commissioner. Retrieved 3 May 2024 from:

https://www.privacy.org.nz/assets/New-order/Your-responsibilities/Privacy-resources-for-organisations/Sensitive-Personal-Information-and-the-Privacy-Act-2020.pdf

Sepulvado, John, "Black Lives Matter Report: Tweet Quoting Public Enemy Prompted DOJ Investigation", *Oregon Public Broadcasting*, 12 April 2016. Retrieved 3 May 2024 from: https://www.opb.org/news/article/black-lives-matter-report-tweet-quoting-public-enemy-prompted-doj-investigation/.

Shenkman, Carey, Dhanaraj Thakur and Emma Llansó (May 2021), *Do You See What I See?*, Center for Democracy and Technology (Washington, DC). Retrieved 28 May 2024 from: https://cdt.org/wp-content/uploads/2021/05/2021-05-18-Do-You-See-What-I-See-Capabilities-Limits-of-Automated-Multimedia-Content-Analysis-Full-Report-2033-FINAL.pdf

"Social cohesion straining at the seams" (13 June 2023), Media release, Koi Tū: The Centre for Informed Futures, University of Auckland. Retrieved 5 June 2024 from: https://informedfutures.org/media-release-social-cohesion-straining-at-the-seams/

Social Media Monitoring in K-12 Schools: Civil and Human Rights Concerns (17 Oct. 2019), Brennan Center for Justice and Center for Democracy and Technology (Washington, DC). Retrieved 5 May 2024 from: https://www.brennancenter.org/our-work/research-reports/social-media-monitoring-k-12-schools-civil-and-human-rights-concerns

"Social Networking, Open Source Information and Online Practitioner" (2022), New Zealand Police. Retrieved 7 May 2024 from: https://fyi.org.nz/request/26223-police-manual-chapter-on-social-networking-open-source-information-and-online-practitioner?nocache=incoming-99440#incoming-99440

Solove, Daniel (2006), "A Taxonomy of Privacy", 154 *U Pa L Rev* 477. Retrieved 13 May 2024 from: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2074&context=faculty_publications

"Submission: Gangs Legislation Amendment Bill" (6 April 2024), New Zealand Council for Civil Liberties. Retrieved 25 April 2024 from: https://nzccl.org.nz/submission-gangs-legislation-amendment-bill/

Sunday Star Times, "The activist who turned police informer", *Stuff*, 25 April 2009. Retrieved 24 May 2024 from: https://www.stuff.co.nz/sunday-star-times/features/760466/The-activist-who-turned-police-informer

"System shake-up to tackle youth and gang crime" (17 July 2023), press release, Beehive.govt.nz. Retrieved 5 June 2024 from: https://www.beehive.govt.nz/release/system-shake-tackle-youth-and-gang-crime

Taiuru, Karaitiana (2022), *A Compendium of Māori Data*. Retrieved 27 May 2024 from: https://ndhadeliver.natlib.govt.nz/delivery/DeliveryManagerServlet?dps_pid=IE80920816

Tan, Lincoln, "Chief of police called in over spies", *New Zealand Herald*, 15 Dec. 2008. Retrieved 24 May 2024 from: https://www.nzherald.co.nz/nz/chief-of-police-called-in-over-spies/B4KJMTY7HSGGIDVQS5DE4EEJ7U/

"The classification process" (n.d.) Te Mana Whakaatu | Classification Office. Retrieved 2 May 2024 from: https://www.classificationoffice.govt.nz/classification-info/the-classification-process/

Thompson, Nicholas, "Instagram's Kevin Systrom wants to clean up the &$%$@! Internet", *Wired*, 14 Aug. 2017. Retrieved 24 May 2024 from: https://www.wired.com/2017/08/instagram-kevin-systrom-wants-to-clean-up-the-internet/

Todd, Katie, "NZers' social media comments scanned to inform Covid-19 response," *RNZ*, 30 April, 2022. Retrieved 1 May 2024 from: https://www.rnz.co.nz/news/political/466208/nzers-social-media-comments-scanned-to-inform-covid-19-response

Tolley, Philippa, "Ignored by the state — How Muslim women tried to warn of impending danger", *RNZ*, 8 March 2020. Retrieved 26 May 2024 from: https://www.rnz.co.nz/national/programmes/insight/audio/2018737122/ignored-by-the-state-how-muslim-women-tried-to-warn-of-impending-danger

Toward an understanding of Aotearoa New Zealand's adult gang environment (June 2023), Office of the Prime Minister's Chief Science Advisor | Kaitohutohu Mātanga Pūtaiao Matua ki te Pirimia. Auckland: The University of Auckland. Retrieved 30 April 2024 from: https://www.dpmc.govt.nz/sites/default/files/2024-01/PMCSA-23-06-03-V3-Gang-Harms-Long-Report-V3.pdf

"Transparency Statement" (n.d.-a), Ministry of Business, Innovation and Employment | Hīkina Whakatutuki. Retrieved 11 June 2024 from: https://www.mbie.govt.nz/about/open-government-and-official-information/transparency-statement

"Transparency Statement" (n.d.-b), Te Tari Taiwhenua | Department of Internal Affairs. Retrieved 10 June 2024 from: https://www.dia.govt.nz/Transparency

Transparency Statement — Integrity Services (Information gathering and public trust) (n.d.), Accident Compensation Corporation. Retrieved 10 June 2024 from: https://www.acc.co.nz/assets/corporate-documents/transparency-statement-integrity-services.pdf

"Trial or adoption of new policing technology" (n.d.), New Zealand Police. Retrieved 30 April 2024 from: https://www.police.govt.nz/sites/default/files/publications/trial-or-adoption-new-policing-technology-130722.pdf

Trial or adoption of new technology — Police Manual chapter (July 2022), New Zealand Police. Retrieved 5 June 2024 from: https://www.police.govt.nz/about-us/publication/trial-or-adoption-new-policing-technology-police-manual-chapter

Vanian, Jonathan, "Meta sues Voyager Labs, saying it created fake accounts to scrape user data", *CNBC*, 12 Jan. 2023. Retrieved 5 May 2024 from:

https://www.cnbc.com/2023/01/12/meta-sues-voyager-labs-over-scraping-user-data.html.

Wagenseil, Paul, "'Destroy America' Tweet Gets British Tourists Booted From U.S.", *NBC News*, 31 Jan. 2012. Retrieved 28 May 2024 from: https://www.nbcnews.com/id/wbna46193069.

Waitoa, Joanne Helen (2013), *E-whanaungatanga: The role of social media in Māori political engagement*. Palmerston North: Te Kunenga ki Purehuroa: Massey University. Retrieved 29 April 2024 from: https://mro.massey.ac.nz/server/api/core/bitstreams/e4de9705-2bbd-4b7c-a5b9-89dae27c6f1a/content

Wakefield, Jane, "Christchurch shootings: Social media races to stop attack footage", *BBC*, 17 March 2019. Retrieved 6 May 2024 from: https://www.bbc.com/news/technology-47583393

Walters, Laura, "Team of 6 million: how NZ can harness the power of Kiwis living overseas," *The Spinoff*, 10 Aug. 2021. Retrieved 29 April 2024 from: https://thespinoff.co.nz/business/10-08-2021/team-of-6-million-how-nz-can-harness-the-power-of-kiwis-living-overseas

Webster, Michael (21 Oct. 2022), Open Source Intelligence Conference Keynote Address. Retrieved 5 May 2024 from: https://www.privacy.org.nz/publications/speeches-and-presentations/open-source-intelligence/

"What is Data Scraping?" (n.d.), Cloudflare. Retrieved 11 June 2024 from: https://www.cloudflare.com/learning/bots/what-is-data-scraping/

Wilson, Alex, Bronwyn Carlson and Acushla Sciascia (2017), "Reterritorialising Social Media: Indigenous People Rise Up", *Australasian Journal of Information Systems*, Vol. 21. Retrieved 27 May 2024 from: https://journal.acs.org.au/index.php/ajis/article/view/1591/781

Wilson, Chris (2022), *Hate & Extremism Insights Aotearoa*. Auckland: University of Auckland. Retrieved 28 May 2024 from: https://www.dpmc.govt.nz/sites/default/files/2022-12/hate-and-extremism-insights-aotearoa.pdf

Wilson, Chris, Ethan Renner, Jack Smylie and Michal Dziwulski, "Christchurch terrorist discussed attacks online a year before carrying them out, new research reveals", *New Zealand Herald*, 21 Feb. 2024. Retrieved 5 May 2024 from: https://www.nzherald.co.nz/nz/christchurch-terrorist-discussed-attacks-online-a-year-before-carrying-them-out-new-research-reveals/WVGRDI2BG5FEBIFDJZUZK2CO7A/

Winkelmann, Hon. Justice Helen (Nov. 2018), Sir Bruce Slane Memorial Lecture. Retrieved 30 April 2024 from: https://www.courtsofnz.govt.nz/assets/speechpapers/Bruce-Slane-Privacy-lecture.pdf

Witton, Bridie, “Dame Jacinda Ardern’s Christchurch Call grows — but where are Meta and Google?”, *RNZ*, 12 Nov. 2023. Retrieved 5 June 2024 from: https://www.rnz.co.nz/news/national/502243/dame-jacinda-ardern-s-christchurch-call-grows-but-where-are-meta-and-google

Wukich, Clayton and Alan Steinberg (2016), “Social Media for Emergency Management”, in *Social Media for Government: Theory and Practice*, Staci M. Zavattaro and Thomas Z. Bryer, eds., New York: Routledge. Retrieved 15 March 2024 from: http://lib.lemhannas.go.id/public/media/catalog/0010-012200000000003/swf/7057/Social%20Media%20for%20Government.pdf

Yalden, Phillipa, “Youth gangs use social media to recruit members”, *Stuff*, 16 Aug. 2018. Retrieved 30 May 2024 from: https://www.stuff.co.nz/national/crime/106161778/youth-gangs-use-social-media-to-recruit-members

“Zavy proposal — we asked, they said, we did” (n.d.), New Zealand Police. Retrieved 5 June 2024 from: https://www.police.govt.nz/sites/default/files/publications/zavy-proposal-we-asked-they-said-we-did.pdf

Appendix 1: New Zealand Police form: "Consent to assume 'online identity' — Temporary"

CONS OID TMP 02/22

Consent to assume 'online identity' - Temporary

I, _____, hereby authorise New Zealand Police to take over control of, and use the following online identities and/or accounts of mine:

IDENTITY	PLATFORM/PROGRAM	PASSWORD/2FA

This authorisation permits New Zealand Police to use my online identity and/or accounts for the following purpose/s only:

_____

_____

_____

I understand:

- My identity and/or accounts will only be used for the above specified purpose/s relating to an investigation by the New Zealand Police.
- The use of my online identity and/or accounts by New Zealand Police will end once no longer required for the above specified purpose/s.
- While every effort will be made to return my accounts to me, there may be situations where this is not possible.
- My online identity and/or accounts may be used by New Zealand Police to send and receive e-mails or carry out any other electronic communications and access any

stored information relevant to the purpose/s specified above, including photographs and videos.

- Any electronic communications sent or received by New Zealand Police while using my online identity and/or accounts, and any stored information accessed by New Zealand Police, may be used and disclosed if required for the above specified purpose, related investigation or during the course of any prosecution or related court proceedings.
- I may not be able to access or use the above identity and/or accounts until they are no longer required by New Zealand Police for the above specified purpose/s.
- New Zealand Police may need to change the password(s) to these identities and/or accounts and I may not have access to these while they are required for the specified purpose/s.
- I can revoke this authorisation at any time, but I acknowledge New Zealand Police may retain information obtained from the use of my identity and/or accounts.
- It is not mandatory that I give authorisation to New Zealand Police to take over control of and use my internet identity and/or accounts.

This authorisation is subject to the following additional conditions (if relevant):

_____

_____

_____

I have been advised that I may consult a lawyer before deciding whether or not to give authorisation. I give this authorisation voluntarily.

Signature:_____ Officer signature:_____

Name:_____ Name:_____

Date:_____ QID:_____

Contact number:_____

If individual is under 16 a parent or guardian must give authorisation:

Appendix 2: New Zealand Police form: "Consent to assume 'online identity' — Permanent"

CONS OID PRM 02/22

Consent to assume 'online identity' - Permanent

I, _____, hereby authorise New Zealand Police to take over control of, and use the following online identities and/or accounts of mine:

IDENTITY	PLATFORM/PROGRAM	PASSWORD/2FA

I understand:

- My online identity and/or accounts may be used by New Zealand Police to send and receive e-mails or carry out any other electronic communications and access any stored information including photographs and videos.
- Any electronic communications sent or received by New Zealand Police while using my online identity and/or accounts, and any stored information accessed by New Zealand Police, may be used and disclosed for law enforcement purposes.
- I will no longer be able to access or use the above specified identity and/or accounts.
- New Zealand Police will change the password(s) to these accounts so that I will no longer have access.
- It is not mandatory that I give authorisation to New Zealand Police to take over control of and use my internet identity and/or accounts.

I have been advised that I may consult a lawyer before deciding whether or not to give authorisation. I give this authorisation voluntarily.

Signature:_____

Name:_____

Date:_____

Officer signature:_____

Name:_____

QID:_____

Contact number:_____

If individual is under 16 a parent or guardian must give authorisation:

Signature:_____

Name:_____

Date:_____