National Security Journal

http://nationalsecurityjournal.nz

Published by:
Centre for Defence
and Security Studies,
Massey University

ISSN: 2703-1926 (print) *ISSN: 2703-1934 (online)*

Maintaining social licence for Government use of false social media personas.

Author/s: Olivia Cleaver and Germana Nicklin

To cite this article: Cleaver, O. & Nicklin, G. (2020). Maintaining social licence for Government use of false social media personas. National Security Journal, 2 (1). doi:10.36878/nsj20200201.04

To link to this article: https://doi.org/10.36878/nsj20200201.04

View CrossRef data: https://search.crossref.org/?q=10.36878%2Fnsj20200201.04

Journal Article published 12 June 2020 in National Security Journal.

MAINTAINING SOCIAL LICENCE FOR GOVERNMENT USE OF FALSE SOCIAL MEDIA PERSONAS

Olivia Cleaver and Germana Nicklin[1]

Governmental collection of unprotected information from social media platforms via social media intelligence (SOCMINT) techniques enable the detection and prevention of unlawful and malicious activity for law enforcement purposes. Relatively new, these techniques have come under public scrutiny. Recognised as valuable tools for security, law enforcement and regulatory agencies, how government SOCMINT policies align with public expectations is less clear. This article addresses the gap by comparing New Zealand public expectations about the use of false social media personas as a SOCMINT technique with government policies. 248 individuals were surveyed, establishing initial understandings of public expectations. Findings were compared with policies of key oversight agencies - the State Services Commission and Privacy Commission. This article argues that to maintain social licence, governments using false social media personas need to appropriately balance public protection with personal privacy interests. Transparent policy frameworks are needed to maintain trust and confidence in SOCMINT governance.

Keywords: SOCMINT, social media policy, Facebook, false personas, social licence, privacy, public expectations, trust and confidence, security, intelligence

Introduction

Governmental use of information from social media platforms for law enforcement purposes is relatively new. As such, this use has come under scrutiny in New Zealand in recent years, highlighting new challenges for the privacy of personal information. For example, the State Services Commission's 2018 inquiry into the use of external security consultants Thompson and Clark[1] noted that the use of false social media personas was a breach of reasonable expectations of privacy.[2] These personas are fictional profiles created to protect the identity of staff undertaking SOCMINT collections. After the

1 Olivia Cleaver is a student in the Master of International Security degree programme at Massey University; Dr Germana Nicklin is a Senior Lecturer in the Centre for Defence and Security Studies at Massey University, Wellington. Contact: g.nicklin@massey.ac.nz

mosque attacks of 15 March 2019, the Government sought urgent advice from the SSC regarding agencies' uses of social media; this points to a potential lack of clarity about SOCMINT and false persona activity.[3]

The SSC has also questioned Ministry of Business, Innovation and Employment (MBIE) staff over their use of false social media personas.[4] MBIE stated that this use is to provide online safety for workers involved in investigations. MBIE's official position is that some undercover activity such as the use of social media personas is sometimes necessary as long as their use meets the relevant necessary privacy requirements.[5] Accident Compensation Corporation also argues their need for the use of social media pseudonyms to carry out investigations.[6] The growing prevalence of persona use by government agencies is likely a reflection of the affordability of and ease with which they can access this new source of valuable information. Previously, this type of collection and investigation technique was limited to formal Intelligence Communities.[7]

The views of these government agencies on using social media intelligence methods are clear, but acceptance by the public is not. This article begins to fill the gap in understanding between public expectations and government activity by providing an initial picture of public perceptions about the use of covert social media personas by government agencies and the implications for government policies. It argues that to maintain the social licence for governments to covertly use false social media personas, they need to appropriately balance the need for public protection with the need for personal privacy. Social license refers to the social, political, legal, community and market acceptance of an action or activity.[8]

The article begins by explaining what false social media personas are and how they are used and establishes the international position on their use by law enforcement agencies. It focuses solely on the use of false personas created by agencies for non-invasive, reactive SOCMINT purposes.[9] It does not explore wider international and local concerns about the management of data, terms and conditions of social media site use and the proactive "big-data scanning" carried out by platform owners such as Facebook. While noteworthy, they are outside the scope of this article. Through a mixed method research approach, the article compares public perceptions of government use of covert social media personas with government agencies' policies and guidelines. The article concludes that while indicative research shows a high level of public acceptance, transparent policy frameworks are needed to maintain the public trust and confidence in SOCMINT governance. It highlights the lack of clarity regarding what is deemed public information and what is deemed private information. This lack of clarity creates barriers in understanding what effective governance of SOCMINT techniques might look like. The article concludes by suggesting the need for further research to validate and extend these findings.

Covert use of False Social Media Personas

SOCMINT is a form of intelligence that focuses on the collection and analysis of information produced and exchanged through social media networking sites.[10] The use of false social media personas is a SOCMINT collection technique[11] that enables organisations or states to scan and monitor social media networks in a covert manner.[12] This technique is used in two main ways. The first, which is the subject of this article, is using false personas to reactively and non-invasively access information about a particular person - information that they have made visible to anyone with a social media login account. Persons under surveillance in this manner have no visibility of the false persona. The second is to use the false persona to gain access to a social media group. This involves the group members having visibility of and believing the false persona to be a real identity. The latter traverses deeper ethical considerations and requires extensive research in its own right.

Omand, a leading critical thinker in the field of SOCMINT, suggests that public institutions, including the police and intelligence services, have a responsibility to adapt to changing demands and culture; that SOCMINT collections are a part of this change and they provide necessary contributions to community safety and security.[13] Much of the international literature draws on Omand, with a strong theme of the need for governance frameworks. Omand argues that SOCMINT use comes with the need for proportionality, balancing its use against public good. Importantly, Omand also argues that states may struggle to keep up with changing attitudes and habits if SOCMINT frameworks are not incorporated into state activities. What Omand's work does not give weight to are public expectations and transparency about the use of SOCMINT. These omissions reflect a need for ongoing research and development on the topic, looking more broadly into expectations of use and how these are reflected in policy.

Governance of SOCMINT is complex and heavily debated. On the one hand, social media networking sites and the information they hold are privately owned;[14] on the other, individuals may feel they, as users, have the right to control by whom and how their own information is accessed. This creates debates about whether data owned by social media companies is public or private. There is no clarity in law or practice on whether the information held on social media sites is public or private, creating uncertainty about rights to access and use information and data gathered.[15] The ambiguity of private and public information rights creates complexities in governance of information collected from social media networking sites.

Edwards and Urquhart suggest citizens assume social media communications, for example, public posts, are open to being searched, and therefore not restricted to "Facebook friends".[16] Edwards and Urquhart argue that if the information is self-disclosed, it is open to being viewed and searched. However, they were unable to

provide a definitive answer to the question of whether accessing personal information placed openly on a social media platform is a breach of individual privacy. The issue is therefore less about access to the data, some of which is available for all to see once a login account has been created, and more about who has control over how this information is used. Perceptions of whether social media profiles and published information are public or private and how that data is subsequently used are likely to play a part in how the public perceives social media use by government agencies. Government uncertainty about whether social media is rightly situated in the public or private domain provides a likely reason for the absence of legislative direction on SOCMINT use to date. Fewer regulations would be expected for the public than the private domain. Ivan et al argue that the intrusive nature of reviewing an individual's social media posts must be governed by legislation, yet to date no state has succeeded in formulating a legal framework.[17] They emphasise that the challenges linked to SOCMINT use are confidentiality, consent and understanding the boundary between what is public and what is private.

Edwards and Urquhart also outline the need to review United Kingdom legislation governing social media intelligence collections.[18] They ask valid questions about the ethics and legality of state regulators using SOCMINT. The key question is whether the public interest in policing outweighs the private interests of those monitored. They conclude that the existing law does not provide adequate protection for government SOCMINT use and there is a significant lack of well-defined expectations of privacy. What they mean by 'adequate protection' is policy or guidelines that protect both agencies' legal use of the data, and the public's rights to privacy.

Privacy is a recurring theme in SOCMINT literature. Questions include the meaning of privacy in public spaces, and how it can be measured, assessed and understood. A key problem is the lack of a single definition or meaning of the word 'privacy' – a word that is in common use by the public as well as in philosophical, political and legal domains.[19] For example, Privacy International raised concerns about a 2017 submission to the Department of Homeland Security's Privacy Office seeking the expansion of immigration records to include social media names and associated identifiable information and search results.[20] They argued the Department's proposal was without sufficient justification, and emphasized the gross intrusion into the individual's right to privacy. They suggested agencies must comply with "international principles of legality, necessity, and proportionality." This argument resembles the New Zealand SSC statement that covert social media use is a "breach of individuals' reasonable expectation of privacy."[21]

The lack of understanding of privacy is further outlined in a 2012 Canadian study on cybersecurity.[22] This study is notable for being from a comparable nation to, and therefore pointing to a possible course of action for, New Zealand. The article aims to find

a way to manage the significant pressures of establishing policy along with enabling practitioners to use SOCMINT in their day to day work. It also questions the interactions of the state and private companies in line with the interest of society, business, and the imperatives of security.[23] It states that the lack of a regulatory framework intensifies complexities.

There is limited academic research about New Zealand perspectives of SOCMINT, and what there is derives from government agencies. The Office of the Privacy Commissioner (OPC) provides insights into public perceptions about privacy in a 2011 study. It reveals the public's willingness to use social media is based on their having autonomy and control over who sees their data.[24] This need for control suggests government agencies may have difficulty in implementing policies if they do not meet public expectations. In 2018, the OPC conducted a survey about perspectives of privacy in a general sense.[25] The study showed that people are concerned about their privacy and feel vulnerable when sharing personal information over social media. However, there remain gaps in understanding what this means for practices of agencies undertaking SOCMINT collections. Media and political discourse further indicate an appetite for a better understanding of SOCMINT and covert social media use by government agencies.[26] The public scrutiny surrounding social media intelligence suggests a need for further research and understanding of the topic.

In an interview in 2018, in response to the SSC inquiry about the Thompson and Clarke case, the Privacy Commissioner (John Edwards) expressed a hope that there will be an improvement in SOCMINT type activities across government, noting an apparent lack of oversight for policy in government agencies.[27] Edwards also states that when agencies step across the line into pre-emptive intelligence gathering on citizens who are exercising their democratic right to freedom of expression, there is a need for a "brighter light". In other words, more public scrutiny is required to shine a light on gathering information from open and free areas. Edwards' comments exemplify the gaps in the regulatory framework to help guide government policy outside the *Privacy Act 1993*, and the need for this gap to be filled.

The literature makes clear that there is limited understanding of how SOCMINT should be governed, partially driven from difficulties in defining whether social media information is sourced from a private or a public sphere. Inconsistent and underdeveloped structures for SOCMINT policy and legislation point to gaps in SOCMINT knowledge, opening up governments to intensified scrutiny from media and the public. A key gap is that there is no true understanding of public expectations of social media intelligence use, most likely because social media is a new tool. The lack of research into public expectations of and perspectives about government SOCMINT use suggests they have been undervalued as a means to influence future governance practices.

Methodology

This study incorporated quantitative and qualitative research methods in a mixed method approach. The first layer was to develop an initial baseline of public perceptions, understood through the use of quantitative research in the form of a survey. The survey enabled the formation of generalisations about public perspectives of SOCMINT use in New Zealand. Analysis of comments made in the survey enabled a deeper assessment of overall perspectives.

The survey was assessed to be low risk by Massey University ethics processes, and so did not go before a committee but was instead assessed online.[28] The survey included a mix of Likert scales and scenario-based questions, followed by demographic questions to assist in further analysis. The survey was disseminated via Google Forms and went live between 04 June and 21 June 2019. These dates are important because survey answers may have been influenced by the March 2019 terrorist attacks in Christchurch. The survey was disseminated via Facebook, through Massey University pages and shared on personal Facebook platforms to encourage participation. The survey generated 248 responses, more than twice the baseline of 100.[29] While more in-depth research is required to confirm these conclusions, sufficient evidence has been considered here for important indicative findings.

An assessment of themes from the 87 comments was made. Structured analytical techniques, common in the field of intelligence, assisted in developing key findings. This included the use of the inference development model. The inference development model uses deductive and inductive knowledge to develop an inference building on indicators, which can include facts and assumptions.[30] Indicators combine to create a premise, which informs an inference. Inferences build into overall findings which work to show what the New Zealand public expectations of social media intelligence are. Establishing the root cause and inferences contributed to overall findings on understanding public expectations of the use of covert social media by government agencies. The assessment of themes enabled a depth of understanding about them and provided a better understanding of survey participants' expectations.

A discourse analysis compared survey results with relevant provisions of the *Privacy Act 1993* and aspects of the *State Sector Act 1988*. Input from the OPC further assisted in formulating overall findings.[31] A discourse analysis also meant that current governance of SOCMINT could be measured against the survey findings. There is no overarching framework for SOCMINT; however, the *Privacy Act 1993* and the *Public Sector Act 1988* play a part in how agencies manage use.

To further assess the current use of SOCMINT, policies outlining procedures and practices were obtained from MBIE and the New Zealand Police via the Official Information Act. The documents were summarised and assessed in conjunction with other findings

from survey results and the themes assessment of survey comments. Comparing policies and procedures against findings from the survey and the OPC commentary triangulated the research results.

Analysis

Survey

Overall, there was general support for the use of false social media personas by government agencies even though, at the start of the survey, 62.3% of the 248 respondents stated they were not aware that government agencies use false social media personas. This lack of knowledge suggests a possible lack of understanding of how data and information from Facebook can be utilised by governments and organisations. Results may also indicate a degree of apathy or indifference about government agency access to information on Facebook. This inference is supported by the fewer than 30% of respondents showing any concern about the New Zealand government use of false social media profiles.

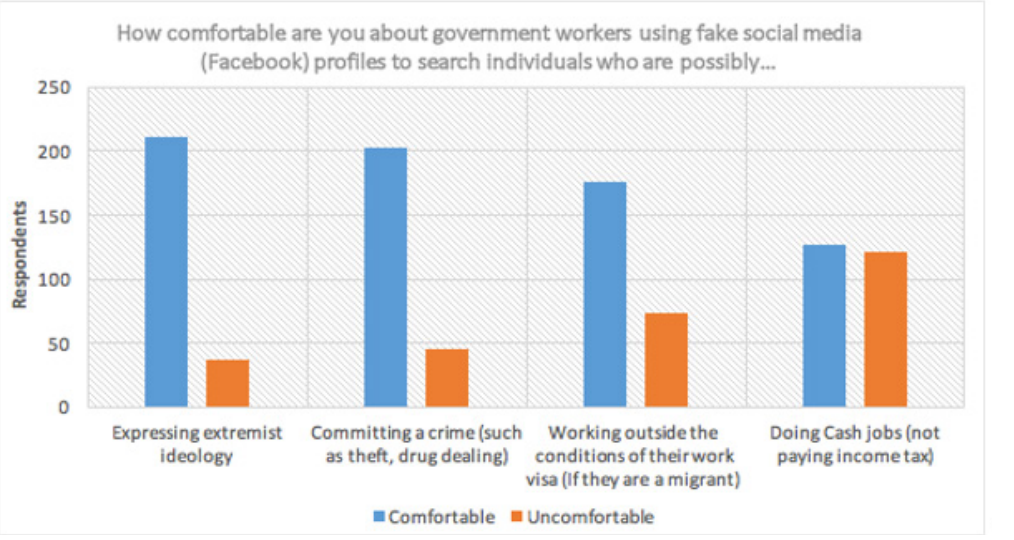
91% of respondents believed the use of social media is important for detecting crime, and 71% of respondents were concerned that the New Zealand government might fail to detect crime, or a security threat, if social media searching is not utilised. These results suggest a public expectation that government agencies undertake the actions necessary for ensuring safety, including the use of false social media personas.

Scenario-based questions were used to distinguish variations in opinions about different government purposes, such as national security, policing, immigration and tax related offending. These questions aimed to investigate proportionality, and what purposes were considered acceptable for SOCMINT searches. The results indicated that respondents were more comfortable about SOCMINT searches to mitigate against extremist ideology and criminal activity. Respondents were comfortable but to a lesser degree with searches for migrant work visas and those undertaking cash jobs.[32] Figure 1 below shows the scenarios relating to the different types of government purposes for false social media personas, and the results.

From the survey comments, 10 themes emerged. The strongest was privacy, followed by public safety and transparent and trusted government. The proportion of comments on privacy indicates maintaining privacy is an issue, despite 69.4% of respondents suggesting they did not feel the use of false social media personas to be an invasion of privacy. Respondents' concerns revealed the fine line between privacy and what can be searched for by regulatory and law enforcement bodies. This fine line reinforces that, for government agencies using SOCMINT, dealing with privacy is not straightforward and requires proportionality, balancing privacy with protection. Respondents' concerns point to a need for strict regulatory guidelines and policy surrounding the use and

management of information collected from social media. Of note, many respondents considered the use of false social media personas should be a Police-only capability, consistent with the scenario-based results in the survey that showed a greater social licence for police searches than for other types of search.

Figure 1: Scenario-based question on types of government purpose

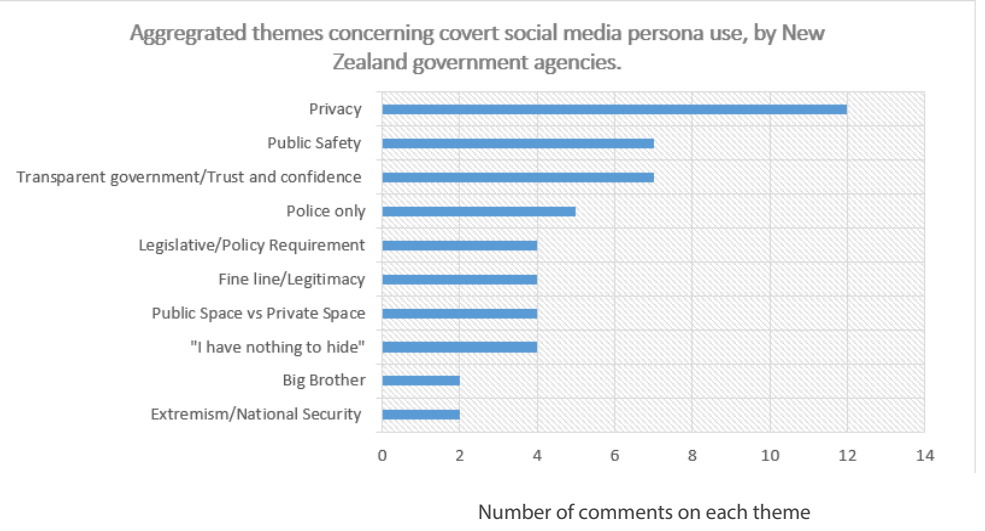


A recurring comment of "I have nothing to hide", suggests that respondents consider their social media profile to be open to searches, and thus public. The OPC considers data found on social media networking sites to be open source and publicly available.[33] This could possibly be contested by social networking companies, which assert in their terms and conditions that they own the right to access and use social media data, indicating it is private.[34] Understanding the dynamics of whether social media is private or public could have a significant effect on the legislative and policy concerns surrounding social media data collection, and warrants considerable further research.

Trust, confidence and transparency are further key themes identified in the survey. These issues are interdependent because transparent policy tends to generate public trust and confidence. This trust and confidence may reinforce a positive perception of the utilisation of covert social media persona for regulatory and law enforcement purposes. Even so, or even because of this positive perception, there is a need for policy and safeguards that consider privacy, best practice and where the "fine-line" of use sits.

Overall, the comments revealed that respondents expect government agencies to ensure the regulatory requirements of their agency are met and that they are obliged to do so. This expectation is interpreted to mean the state has a duty of care to ensure citizens' safety. If this is the case, the expectation of a duty of care further reinforces the social licence for the use of SOCMINT as a necessary function to ensure the care and safety of the community. The aggregated themes are represented in Figure 2 below.

Figure 2: Themes from survey comments



The theme analysis suggests the public will perceive the use of false social media personas by government agencies in a positive light if used for regulatory and enforcement purposes. In other words, the study established there is a social licence for government use of false social media personas. A social licence incorporates practices and actions that are not only legally and ethically responsible, but that also meet society's demands.[35] A social licence can reflect the meaningful partnerships between operations, activities, communities, and governments.[36] These partnerships are important for ensuring collective benefits, providing safe communities and ethical government practices. In the case of this research, the social licence reflects community acceptance of SOCMINT, and demonstrates a first layer of understanding of public expectations of covert social media use.

Discourse analysis

The OPC works to protect New Zealanders' personal information, providing guidance on how agencies collect, use, disclose, store and give access to information. The *Privacy Act 1993* and its principles require personal information to be collected, stored and disclosed in ways that protect the privacy of that information. OPC oversight is relevant to the question of SOCMINT because its collection is not disclosed. Understanding the OPC involvement in agencies' information gathering activities from private citizens is therefore important.

The OPC were consulted about the findings from the survey and agency practices. They advised that they review agencies' policy and procedures for the collection, use and disclosure of information, usually at the request of the agency. It is each agency's responsibility to determine, when, how and what information is required to be collected, in line with the *Privacy Act 1993* and its principles.

Three principles of the Privacy Act are relevant to this research - principles one, two and four. Principle one requires the collection of information from social media to be for a lawful purpose related to a function of the agency. Collection must also be necessary. If an agency can determine that the use of social media is lawful, necessary and aligns with the requirements of its regulatory function, then there is no theoretical reason why it should not be able to collect information from social media platforms. The contested issues often come down to determining which actions are unlawful within the context of agencies' regulatory functions.

Principle two, 'Source of personal information' highlights the importance of clarifying whether social media collection is done in the private or public space. This principle states agencies can only collect information directly from the individual, unless it is publicly available and the individual concerned authorises collection. Collections are also permitted for maintenance of the law. The OPC definition of publicly available information is "information in a magazine, book, newspaper, public register, or other publication that is (or will be) available to members of the public. This can include internet sites that are available to the public, such as social media sites".[37] While "public information" includes social media, it is silent on the manner of collection – in the current case, via false social media personas.

Principle four addresses the manner of collection. It states that information cannot be collected unlawfully, unfairly or in a way that intrudes on the personal affairs of the individual concerned. The test for intrusion is the breach of reasonable expectation of privacy. The survey results provide an indication of the extent of "Reasonable expectation" for SOCMINT collection.

In summary, the Privacy Act and principles work as an enabler for government agencies to carry out their regulatory functions in a way that meets the best interests of New Zealanders. Despite this, there is possibly confusion about whether the use of false social

media personas meets the reasonable expectations of privacy for New Zealanders, as per definitions in the *Privacy Act 1993*. This is because it is difficult to define what is considered a reasonable expectation of privacy and a reasonable expectation of how information is collected.

Security and Intelligence Act 2017

The OPC referred to the *Security and Intelligence Act 2017* (the Act) in reference to specific SOCMINT collections. The Act provides comprehensive oversight of the activities of New Zealand's security and intelligence agencies - Government Communication Security Bureau (GCSB) and Security Intelligence Service (SIS).

The purpose of the Act is to protect New Zealand as a free and open democratic society. It is focused specifically on the protection of New Zealand against national security threats, to ensure international relations and the economic and general wellbeing of New Zealand. All aspects of the Act relate to the requirement for the security and intelligence agencies in New Zealand to be transparent about their activities. It provides clear definitions of various intelligence techniques including Signals Intelligence. Interestingly, it fails to include a definition of SOCMINT, or any assessment of social media use. This exclusion suggests that SOCMINT may require less oversight than more traditional forms of intelligence collections.[38] It could also indicate a lack in maturity of understanding about the multifaceted elements and concerns connected with SOCMINT use. It may further indicate the SOCMINT is not regarded as an intelligence method in its own right.

Significantly, no specific legislation governs the activities of intelligence services beyond the Security Intelligence Service and Government Communications Security Bureau. The Act protects only these two agencies undertaking covert collections, including the use of false identities.[39]

State Services Commission (SSC)

The SSC plays a major role in providing guidance on how agencies establish social media practices and policies.[40] The SSC is responsible for advising, monitoring and developing public services in New Zealand. A key part of their role is ensuring appropriate public service integrity and conduct, with the aim of building public trust in state servants. This is of importance when considering SOCMINT. The SSC is guided by the *State Sector Act 1988*, which is to be replaced by a new Public Service Act. The new Act will most likely maintain, if not strengthen, the integrity provisions.

The level of oversight the SSC has over the way agencies govern their SOCMINT is high level, with no specific policy or procedure guidelines. Each agency is therefore left to create their own policies and procedures for use. As with the *Privacy Act 1993*, it remains agencies' responsibility to align their policies and activities with the *State Sector Act 1988* or its replacement. Of note is an absence of a specific auditing function for SOCMINT

use. Further research might consider whether the auditing and overarching policy for agencies should be managed by SSC because of that organisation's involvement in social media intelligence gathering reviews. Future research might also consider if an auditing and governing capability would be better suited to another government agency, focused on digital security requirements.

Agencies' Policies

The policies on covert social media were requested from MBIE and New Zealand Police (Police) via the Official Information Act to assess whether these agencies' activities align with the public expectations revealed in the survey. Key areas of inquiry were how agency policies addressed the issues of proportionality and overall social licence.

MBIE's 2018 social media policy document shows that MBIE considers the use of social media information collection to be a high risk, and that its use needs to be proportionate.[41] Privacy and risk considerations feature strongly. The document directly references the *Privacy Act 1993*, stating that collection of information must be done lawfully and in a manner that does not unreasonably intrude. It also states that the collection of information is necessary for the lawful purpose connected to the function of the agency. The document further reinforces that staff must be able to evidence these requirements and clearly document intent in case of challenge or audit. These requirements meet what OPC considers a reasonable expectation of privacy and mostly reflect the perspectives outlined in the survey results.

However, the document is strongly focused on reputational risk and privacy and does not address the necessity of SOCMINT use, nor how to ensure public safety. As MBIE represents an amalgamation of 17 regulatory bodies responsible for their own practices, the definition of proportionality might also differ from body to body.

The Police provided sections of their undated social media policy document[42] and a covert backstopping policy.[43] The social media policy document focuses on social media for overt and covert investigation. The latter part of the document emphasises the importance of integrity and procedures that are consistent, ethical and legal. The backstopping policy does not specifically mention "social media", indicating its newness as an information gathering platform.

The Police policy documents fail to specifically discuss privacy and proportionality. However, proportionality can be inferred from their focus on the public safety goals of their organisation. A portion of survey respondents believe that covert social media use should be a Police-only capability. These results suggest Police may enjoy a level of public trust and confidence in their activities that afford them less public scrutiny of social media intelligence actions than for other government agencies. Even so, these attitudes do not exempt the Police from, or may even reinforce the need for, having adequate policies and procedures in order to maintain that trust and confidence.

The MBIE and Police documents align with the *Privacy Act 1993* and *State Sector Act 1988*, and in a general sense indicate good practice for the use of covert social media. They take the use of covert social media seriously and have policies in place guiding its use. Nevertheless, the survey results point to several areas where these agencies could strengthen their social media policies. The first is transparency.[44] More clarity is needed on balancing the need for the use of SOCMINT with the need for privacy. Second is that the fine line between privacy and proportionate use of covert social media personas is not addressed in the policies examined. One solution may be for agencies to outline how the use of covert social media meets their regulatory requirements, to ensure that the use is proportionate with the potential harm. Another could be to provide overarching, publicly available statements about the rationale for agencies' social media use. How agencies can ensure activities are transparent, while meeting legal requirements and the demands of their regulatory purpose, requires considerable further research.

Conclusions

This article set out to discover public expectations about the use of covert social media use by government agencies in New Zealand. Indicative results suggest members of the public generally accept, and even expect, SOCMINT use by regulatory and enforcement agencies and consider it to be valuable.

However, SOCMINT use is growing fast and involves a delicate balancing of interests. This article has shown public concerns about transparency, privacy, proportionality and the fine line in balancing them need to be addressed in agencies' policies. Internationally, SOCMINT is recognised as a valuable collection tool for law enforcement agencies to interpret the criminal and social environment and assist in preventing harm. Drawing on international research and practices, New Zealand government agencies can clearly argue the case for using covert use of false social media personas as part of their regulatory functions, in order to prevent harm and keep New Zealand safe. The survey results have shown that however justifiable the use, it can only be successful if the public whose social media use is being covertly tracked has trust and confidence in the agencies tracking them.

A key theme of these findings has been managing the fine line between protection versus privacy interests. The survey results indicate there is a social licence for government agency use of SOCMINT, with a public perception that agencies use it to assess increasing security threats and unlawful activity in New Zealand. Not using SOCMINT exposes agencies to the risk of being perceived as failing to protect the public. However, agencies must mediate SOCMINT use, including the use of false social media personas, with privacy requirements.

The findings indicate the public expects government agencies to have a transparent policy in place when undertaking covert social media collections. The OPC and SSC are the primary bodies for ensuring government agencies align their use of SOCMINT with the interests of New Zealanders through elements of the *State Sector Act 1988* (soon to be the Public Service Act) and the *Privacy Act 1993*. However, these Acts do not ensure SOCMINT governance. There is no specific legal framework or auditing body overseeing SOCMINT use across the public service. In the absence of such a framework, the responsibility for robust and transparent policies lies with individual agencies.

The lack of a specific auditing function and specific SOCMINT governance leaves agencies having to develop their own approaches to SOCMINT use. The examples from MBIE and the Police show different approaches that align with key oversight Acts but that exhibit gaps. First, the absence of the need to report on the level of proportionality and ensure best practice likely affects agencies' levels of transparency. Second, a limited maturity in knowledge of public expectations and international best practices for SOCMINT use makes their task even more difficult. Specific governance mechanisms that create consistency of policies, supportive legislation and regular monitoring and reporting of SOCMINT, backed by the social licence revealed in this research, would likely mitigate opportunities for misuse and ensure continued public support.

The overall findings in this article demonstrate the importance of SOCMINT and social media governance as a topic for future research. A number of questions for further research suggest themselves:

- Does social media data sit in the public sphere or private sphere? If it is considered to be in the public domain, perspectives about privacy requirements, and thus policies, might need to change.
- What comprises "legitimate reason", as quoted in the survey, and how can proportionality be measured? Legitimate reasons were not specifically explored in the survey. Assumptions can be made suggesting that legitimate reasons are for compliance and/or law enforcement purposes, but how these can be measured against harm to ensure proportionality requires further research.
- What effect does the government's partnership obligations with Māori have on the use of SOCMINT? It was not assessed, and would be worthy of consideration, particularly regarding privacy values and proportionality in New Zealand.
- What effect would a more diverse sample of the population have on the results, particularly from those who are vulnerable?
- Would the results be the same for pro-active social media scanning? The research considered only reactive searches of social media data, based on an assumption of unlawful activity. Pro-active scanning of social media data, including "big data" or "mega data", warrants considerable further research.
- How can government agencies manage relationships with owners of social media platforms, such as Facebook?

In conclusion, evidence that social licence for the use of false social media personas for law enforcement purposes now exists. However, this evidence is indicative only and needs to be validated by more in-depth research, as outlined above. At a time when security issues such as the 15 March 2019 mosque attacks and the more recent Covid-19 pandemic are directly affecting New Zealand and other societies, it is critical that public confidence in the intelligence collection carried out by regulatory and law enforcement agencies is maintained.

---

1 Thompson and Clark is a private security and risk management organisation

2 Doug Martin and Simon Mount QC, "Inquiry into the Use of External Security Consultants by Government Agencies", 2018. Available at https://www.ssc.govt.nz/sites/all/files/Report%20of%20the%20inquiry%20into%20the%20use%20of%20external%20security%20consultants%20by%20government%20agencies_0.pdf

3 "Government seeks urgent advice on social media after Christchurch shootings," 20 March 2019. Stuff.co.nz. Available at https://www.stuff.co.nz/national/christchurch-shooting/111440499/government-seeks-urgent-advice-on-social-media-after-christchurch-shootings

4 "Immigration NZ, MBIE use fake social media profiles," 27 September 2017. Radio New Zealand. Available at https://www.radionz.co.nz/news/national/340384/immigration-nz-mbie-use-fake-social-media-profiles

5 "MBIE Defends Training Staff to Create Fake Identities Online," 1 September 2019. Newshub.co.nz. Available at https://www.newshub.co.nz/home/new-zealand/2019/01/mbie-defends-training-staff-to-create-fake-identities-online.html

6 "Immigration NZ, MBIE use fake social media profiles," 27 September 2017.

7 A government Intelligence Community is responsible for gathering intelligence for national security and foreign policy purposes. See, for example, the New Zealand Intelligence Community: https://www.gcsb.govt.nz/about-us/the-new-zealand-intelligence-community/

8 Joel Gehman, Leanne M. Lefsrud and Stewart Fast, "Social license to operate: legitimacy by another name?", *New Frontiers, Canadian Public Administration*, 60 (2) (2017), pp.293–317.

9 The research considered only reactive searches of social media data, based on an assumption of unlawful activity prompting requirements for searching. It does not examine proactive SOCMINT techniques.

10 Marco Lombardi, Todd Rosenblum & Alessandro Burato, "From SOCMINT to digital HUMINT: Re-frame the use of social media within the Intelligence Cycle", *Sicurezza, Terrorismo e Società*, 2 (2015), pp. 101-107.

11 Awais Rashid, Alistair Baron, Paul Rayson, Corinne May-Chahal, Phil Greenwood, and James Walkerdine. "Who Am I? Analyzing Digital Personas in Cybercrime Investigations", *Computer,* 46, no. 4 (April 2013), pp.54–61. DOI:10.1109/MC.2013.68

12 "Social Media Intelligence". Privacy International, 2017. Available at https://privacyinternational.org/explainer/55/social-media-intelligence

13 Sir David Omand, Jamie Bartlett, and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)", *Intelligence and National Security* 27, no. 6 (December 1, 2012). pp. 801-23. DOI:10.1080/02684527.2012.716965

14 Omand et al., pp.801–23.

15 Omand et al., pp. 801-23.

16 Lillian Edwards & Lachlan Urquhart, "Privacy in public spaces: What expectations of privacy do we have in social media intelligence?", *International Journal of Law & Information Technology*, *24*(3) (2016), pp.279–310. DOI:10.1093/ijlit/eaw007

17 Adrian Liviu Ivan, Claudia Anamaria Iov, Raluca Codruta Lutai, & Marius Nicolae Grad, "Social Media Intelligence: Opportunities And Limitations", *CES Working Papers*, *7(2A)* (2015), pp. 505–510.

18 Regulation of Investigatory Powers Act 2000; and the Data Retention and Investigatory Powers Act 2014.

19 Judith DeCew, "Privacy." In *The Stanford Encyclopedia of Philosophy*, Edward N. Zalta, ed. (Metaphysics Research Lab, Stanford University Spring 2018 Edition). Available at https://plato.stanford.edu/archives/spr2018/entries/privacy/

20 "Social Media Intelligence", 2017.

21 Martin and Mount QC, 2018.

22 "Fundamentals of Cyber Security for Canada's CI Community". Public Safety Canada, 21 December 2018. Available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx

23 "Fundamentals of Cyber Security for Canada's CI Community", 21 December 2018.

24 "People care about privacy on social networking sites: Survey by international privacy commissioners". Privacy Commissioner, 8 December 2011. Available at https://www.privacy.org.nz/news-and-publications/statements-media-releases/people-care-about-privacy-on-social-networking-sites-survey-by-international-privacy-commissioners-media-release/

25 "People care about privacy on social networking sites: Survey by international privacy commissioners", 8 December 2011.

26 "Immigration NZ, "MBIE use fake social media profiles", 27 September 2017.

27 Edwards & Urquhart, pp. 279–310.

28 Ethics Number: 4000021116

29 There could be a potential bias in the results. Many respondents were recruited through the primary author's own networks, and could therefore indicate the values and attitudes of her particular demographic.

30 Richards J. Heuer and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, CQ Press, 2010.

31 Email Communication: 01 September 2019.

32 MBIE (Immigration New Zealand) and Inland Revenue

33 "What Is Publicly Available Information?". Privacy Commissioner, 2013. Available at https://privacy.org.nz/further-resources/knowledge-base/view/251

34 "Who Owns the Content on Social Media," Newsroom.unsw.edu.au, October 28, 2019. Available at https://newsroom.unsw.edu.au/news/business-law/who-owns-content-social-media.

35 Richard Parsons and Kieren Moffat, "Constructing the Meaning of Social Licence," *Social Epistemology* 28, no. 3–4 (October 2, 2014), pp.340–63, DOI:10.1080/02691728.2014.922645

36 Alyson Warhurst, "Corporate Citizenship and Corporate Social Investment: Drivers of Tri-Sector Partnerships", *Journal of Corporate Citizenship*, no. 1 (2001) pp.57-73. https://www.jstor.org/stable/10.2307/jcorpciti.1.57

37 "What Is Publicly Available Information?", 2013.

38 It could also mean that legislation and policy are lagging behind practice, although the date of the Act is recent enough for social media practices to be included.

39 s67(f) taking any action to protect a covert collection capability AND s23 assumed identity may be acquired, used and maintained

40 "Integrity and Conduct," State Services Commission, 2020. Available at https://ssc.govt.nz/our-work/integrityandconduct/

41 MBIE, "Procedures for MBIE Staff Using Social Media for Verification and Investigation Purposes to Support Regulatory Compliance and Enforcement Needs," (2018).

42 New Zealand Police, "Social Media Policy," n.d.

43 New Zealand Police, "Covert Backstopping Policy," n.d.

44 Of note is that parts of the procedure documents were redacted – the opposite of transparency.