Te Pourewa Mātaki
Inspector-General of Intelligence and Security

Review of NZSIS and GCSB Open Source Intelligence Collection

Public Report

Brendan Horsley
Inspector-General of Intelligence & Security

July 2024

Contents

INTRODUCTION

1. Open source intelligence (OSINT) can be defined as the collection, analysis and use of data from openly available sources for intelligence purposes. OSINT can involve online searches of publicly available information and the use of specialist tools to gather such information.

2. Historically OSINT has not been a major focus of intelligence and security agencies, but use of the internet and social media has increased the opportunities for OSINT in both scale and scope. In 2014 James Clapper, then United States Director of National Intelligence, described social media as "huge for intelligence purposes".[1] As at January 2023, Facebook, YouTube, WhatsApp, and Instagram all had more than two billion users and WeChat 1.3 billion.[2] A vast and increasing amount of personal data is now publicly available. Compared to covert surveillance and interception, information from open sources is more accessible and less costly to collect. It has been estimated in the United States that, since the early 2000s, 90-95 per cent of intelligence comes from open sources.[3]

3. OSINT continues to evolve and is now largely driven by the development of tools that can simultaneously scan hundreds of sources and platforms. Results can be analysed concurrently and displayed quickly and clearly. The tools' sources may also include datasets obtained through a data broker or from hacks and leaks.[4]

REVIEW SCOPE AND CRITERIA

4. This review examined OSINT activities carried out by the NZSIS and GCSB. I particularly focused on the use of specialised tools and methods to collect OSINT, rather than general searches of publicly available information.

5. My review looked at how both the NZSIS and GCSB:

    5.1. approached the legal issues that arise with OSINT collection;

    5.2. conduct OSINT collection; and

    5.3. ensure their activities meet legal and policy requirements.

---

1 Lilian Edwards and Lachlan Urquhart 'Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?' (2016) International Journal of Law and Information Technology 24 (3) at 281.

2 Statistica "Most popular social networks worldwide as of January 2023, ranked by number of monthly active users (in millions" statistica.com/statistics/272014/global-social-networks-ranked-by-number-of-users.

3 Richard A Best & Alfred Cumming *CRS Report for Congress Open Source Intelligence (OSINT): Issues for Congress* (5 December 2007) fas.org/crs/intel/RL34270.pdf at 4.

4 Review Committee on the Intelligence and Security Services (CTIVD) *Automated OSINT: tools and sources for open source investigation* (22 December 2021) at 4-5.

LEGAL AND POLICY FRAMEWORK FOR OPEN SOURCE ACTIVITIES

6. The intelligence and security agencies' statutory functions include collecting and analysing intelligence in accordance with the New Zealand Government's priorities.[5] Collecting information from publicly available sources such as the internet is generally lawful.

7. Ministerial policy requires the agencies, when collecting and using publicly available information, to have regard to the principles of respect for privacy, necessity, proportionality, use of the least intrusive means available, respect for freedom of expression (including the right to advocate, protest or dissent), legality, and facilitation of effective oversight.[6]

8. Certain OSINT activities are potentially unlawful. The agencies consider the use of automated tools to collect information from public websites is generally lawful, except when used to collect information subject to privacy settings and/or where the activity is specifically prohibited by the terms and conditions of a website. It might then breach s 252 of the Crimes Act 1961, which relates to unauthorised access of a computer system. Additionally, if intelligence is collected from datasets that have been hacked or leaked, the agencies consider that might amount to the offence of receiving stolen property (s 246 Crimes Act).

9. To carry out potentially unlawful activities the agencies can and do obtain intelligence warrants under Part 4 of the Intelligence and Security Act 2017 (ISA).

THE SELECTION AND ADOPTION OF OSINT TOOLS

10. A key issue is how the agencies should approach the adoption and use of OSINT collection tools, particularly those that are commercially available. A risk of commercially available tools is the lack of information available to the user about how they work. Often users are limited in their agency and influence over how a tool functions.[7]

11. The Dutch intelligence oversight body has held that the acquisition of OSINT tools called for a "careful weighting process" with regard to the rights of data subjects, proportionality, and a duty of care for data processing.[8] It recommended the Dutch intelligence services develop an assessment framework to be implemented by policy, procedures and work instructions.[9]

12. Similarly, I consider that when considering adopting a third party tool for OSINT collection a New Zealand intelligence and security agency should carry out a thorough assessment of the tool, distinct from the warrant process. This would underpin assurances to warrant issuers that the agency has "satisfactory arrangements" in place for minimising impacts on members of the public from use of the tool and ensuring any information collected is lawfully retained, used and disclosed, as required by the ISA.[10] I see a robust assessment framework as particularly

---

5 Intelligence and Security Act 2017 (ISA), s 10(1)(a). "Intelligence and security agency" is defined in s 4 of the ISA to include the NZSIS and the GCSB.

6 Ministerial Policy Statement "Publicly Available Information" (1 March 2022).

7 Review Committee on the Intelligence and Security Services (The Netherlands) *Automated OSINT: tools and sources for open source investigation* (22 December 2021) at 25.

8 Above n 7.

9 Above n 7 at 25-26.

10 ISA, s 61(1)(d).

important for any use of advanced artificial intelligence tools, as they become more prevalent and relevant to intelligence activities. The framework could address:

12.1. the intelligence gap and how the OSINT tool could fill that gap;

12.2. the functionalities of the tool and what activities may be unlawful;

12.3. any use of artificial intelligence;

12.4. any use of assumed identities or bots;

12.5. the underlying (or suspected) data sources;

12.6. expectations of privacy in targeted data and the intrusiveness of the tool;

12.7. the assessed reliability and accuracy of the data obtained and analysis provided;

12.8. a due diligence assessment of the company providing the tool;

12.9. how the tool retains and stores data;

12.10. logging and auditability of searches; and

12.11. whether use of the tool adds to the intelligence holdings of the private company supplying it.

13. I comment further on this in relation to each agency later in this report.

THE INTELLIGENCE AND SECURITY AGENCIES' OSINT ACTIVITIES

14. As expected I found the NZSIS and GCSB had different approaches to OSINT collection. While OSINT collection is a regular part of the NZSIS' intelligence efforts, it is less important to the GCSB, given its signals intelligence capabilities.

15. Given the differing role that OSINT collection plays for each agency, some issues are more relevant to the NZSIS and are discussed here in more depth.

NZSIS OPEN SOURCE COLLECTION

Authorisation

16. NZSIS has warrants covering OSINT collection, including collection that may breach the terms and conditions of a website or, by use of sophisticated tools, amount to an otherwise unlawful search.

NZSIS policies and procedures for OSINT collection

17. At the beginning of my review the Service had no finalised standard operating procedures for the use of open source tools, or for internal requests for OSINT searches. I was notified in September 2023 that NZSIS had adopted a procedure outlining the processes for these activities.

NZSIS OSINT collection operations

18. OSINT collection is a regular part of NZSIS' activities. As the details of this collection are classified, I am unable to provide much information in this report.

19. My classified report detailed:

    19.1. the personnel responsible for undertaking OSINT activities within the Service;

    19.2. the infrastructure that enables these activities;

    19.3. the process the Service has in place for requesting and approving OSINT collection to be carried out;

    19.4. how the Service carries our OSINT collection and reports on the results internally; and

    19.5. some of the purposes for which the Service has carried out OSINT collection (eg target discovery and investigating leads and persons of interest).

20. I also examined two OSINT tools, one the Service has used historically and one currently used. The latter tool enables targeted collection across a range of social media sites. It can carry out automated ongoing collection and provide analysis of searches powered by artificial intelligence.

Assessment of NZSIS OSINT activities

Authorisation for OSINT collection

21. During this review I identified several concerns with Service warrants covering open source collection. In my view the applications needed to give clearer information on the tools used, the individuals who could be targeted under the warrants, and the full range of OSINT activities NZSIS intended to carry out.

22. I raised these matters with the NZSIS and most of my concerns have been addressed in the most recent warrant application. In particular the Service has provided the warrant issuers with fuller descriptions of the tools and the purposes for which they are used, along with a more specific process for determining who may be targeted using an OSINT tool.

23. I still consider that the warrant and application could provide more detail on the types of data collected using the tools, given the variety of data available on public internet infrastructures. The NZSIS advised that it would consider my comments in the next renewal of the warrant.

Selection and adoption of OSINT tools

24. NZSIS has considered factors such as operational security and cost before developing or procuring OSINT tools. These assessments appear to have been mostly informal and ad hoc, however. While a warrant application must address the necessity, proportionality and privacy impact of the proposed use of OSINT tools, it is not the place for a detailed examination of issues such as reliability of the data, due diligence on a company providing a tool, use of artificial

intelligence, and storage and use of personal information that contributes to machine learning. I did not see these issues considered in assessments of the Service's OSINT tools.

25. Given the importance of OSINT to the NZSIS I concluded it should have a robust assessment framework, as at [12] above.

26. **I recommended** NZSIS develop and formalise an assessment framework for the acquisition and use of specialised open source intelligence collection tools.

27. The NZSIS advised that it would develop an assessment process for acquiring such tools, taking into consideration the factors outlined in this report.

Publicly Available Information request and reporting process

28. My review found that the Service's internal processes for requesting and reporting on OSINT collection had improved since first implemented. Prior to the current warrant and standard procedure I was concerned there was not enough rigour in documenting how activity was tied to the NZSIS's functions and an intelligence warrant. It also appeared that some requesting and reporting occurred verbally. Email records were inconsistent. Towards the end of my review the adoption of a new procedure addressed my concerns.

Ongoing collection for online monitoring

29. The Service's use of OSINT tools for ongoing collection on individuals and groups, rather than single instances of collection, raised several concerns. I found limited operational planning and documentation had been done before ongoing collection. No request forms had been submitted for the ongoing collection activities I reviewed. The requesting and reporting of ongoing collection usually occurred verbally, which is not amenable to oversight.

30. NZSIS might have a legitimate need for ongoing collection, particularly for discovering previously unknown threats. But collection must always be as targeted as possible, with a proper justification set out before it begins.

31. Again, many of my initial concerns were addressed by recent changes in NZSIS procedure for the use of its OSINT tools. The new procedure does not explicitly cover the requesting and registering of ongoing collection, but internal guidance addressed the key considerations.

32. **I recommended** NZSIS amend its standard operating procedure for OSINT collection to incorporate requirements for initiating, recording and reviewing automated ongoing collection.

33. The Service advised that it would include requirements for ongoing collection when it next updates its procedure, likely alongside the renewal of the relevant warrant.

GCSB OPEN SOURCE COLLECTION

Authorisation

34. The GCSB has a warrant covering OSINT collection, including collection that may breach the terms and conditions of a website or amount to an otherwise unlawful search. The warrant application sets out a process for the Bureau to determine whether data can be obtained, on the basis of relevance to an authorised intelligence purpose. The Bureau then has a specified time in which to assess whether data acquired is in fact relevant and can be retained.

GCSB policies and procedures for OSINT collection

35. The use of GCSB's warranted OSINT tools is guided by operational documentation that collates the relevant legal and policy requirements. These include checking for alignment with registered intelligence requirements; recording and explanation of why the collection is necessary; and using only approved tools, which must record what has been done and by whom.

36. The Bureau's general policies and procedures on retention of data apply to data obtained through OSINT collection. This means such data must be categorised, with consequent timeframes for retention and review for relevance.

GCSB OSINT collection operations

37. My classified report examined the tools that the GCSB uses to conduct OSINT collection, which I am unable to detail in this report. This included consideration of:

    37.1. how OSINT tools were evaluated by the GCSB;

    37.2. how the tools work and the type of data that they may collect;

    37.3. the processes followed by various GCSB teams to carry out OSINT collection; and

    37.4. how data from the tools is retained.

Assessment of GCSB OSINT activities

Authorisation for OSINT collection

38. I concluded from my review that the Bureau has approached the use of open source collection tools reasonably carefully and within strict parameters. It has a robust warrant framework governing use of the tools and handling of collected data. I considered the GCSB could provide more information in warrant applications on the tools it uses for open source searches. It undertook to review the relevant material at the next opportunity.

Policy and guidance

39. I found that GCSB operational documentation provided a succinct overview of the relevant intelligence warrants and organisational policies, but needed updating in some areas to reflect current practice.

40. The Bureau also had a variety of guidance material available to staff on how to conduct OSINT. This was generally appropriate, although I found the guidance for one of the tools needed expansion to cover data retention and assessment. The tool was retaining copies of all search results, which was at odds with the legal and policy requirements for collected information to be assessed for relevance and destroyed as soon as practicable if irrelevant.[11] While I understand this was partly due to the technological constraints of the tool, I could find no recorded justifications for retaining all the information.

41. **I recommended** that the GCSB:

- update the operational documentation; and
- review the search results retained by the tool at issue, to assess the information for relevance and comply with s 103 ISA and GCSB data retention policy.

42. The GCSB advised that it had included in its 2024 audit plan an audit of activity using the relevant OSINT tool, which would include consideration of its retention of collected data.

Selection and adoption of open source tools

43. Similarly to the NZSIS, I found that the GCSB had considered factors such as operational security and cost before developing or procuring OSINT tools, but these assessments appeared to have been informal and ad hoc. They did not consider factors such as the background of the provider, how a tool stores data, what algorithms it would use, or how artificial intelligence would be applied within the tool and what it might learn from GCSB inputs.

44. While I recommended that the Service develop a formal assessment framework for prospective OSINT tools, I did not find it necessary to make the same recommendation for the GCSB, considering its likely approach to OSINT collection for the foreseeable future. I would expect such a framework to be used, however, if the GCSB's approach changes.

Oversight

45. My review required access to certain GCSB records on OSINT collection. I considered that routine access to these records was necessary for oversight.

46. **I recommended** the GCSB enable this and the Bureau agreed to arrange it.

[11] ISA, s 103.