Introduction: OSINT limitations in Australian NIC

Open Source Intelligence (OSINT) is “the production of intelligence through the collection and enrichment of publicly available information” (Baker, 2023. p 3). This means everyday unvetted indiviudals could access this kind of data and effect intelligence analysis… kind of.

OSINT takes practice, methodology, and awareness. There are lots of extraneous data in OSINT and the shuffling of the ‘real’ from the ‘fake’ is not clear cut. There are limitations. This paper is an introduction to the kinds of limitations in the use of OSINT by the Australian National Intelligence Community (NIC). It will highlight that OSINT may require its own place in the suite of intelligence tools even when the 5-eyes project can effect much greater intelligence analysis than that solely available to OSINT, specifically OOSI and Big Data.

The key limitations for the use of OSINT by the NIC includes;

1. the legal context in Australia,
2. the current use of OSINT relegated solely as a support intelligence tool by various bureaus in the NIC,
3. the scale of data types and volume needed to effect OSINT,
4. and the individuals skilled in this space.

TLDR

The NIC uses OSINT in combination with a variety of other sourced material. The impact of OSINT (individually) is quite small to the rest of the NIC material, currently. However, by following the suggestions in the Scott (2023) occasional paper, Australia might be better off with an OSINT devoted department alongside a suite of consultant activities.

1. The legal context of OSINT in Australia

A limitation to the use of OSINT for the NIC is the current legal context around data collection and use according to the Australian Privacy Act (and amendments) and the Telecommunication Act (and amendments). Legally, in Australia, the gathering of

personal data on individuals is illegal. The OSINT methodology of passive data scraping runs counter to the Privacy Act and Telecommunications Act. Therefore, OSINT collections of these kinds are in breach of the legal context in Australia. Specifically, the Australian legal context sets limits regarding 'personal information' and its use in telecommunication information. The act defines personal information broadly as:

'Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a. *whether the information or opinion is true or not; and*
b. *whether the information or opinion is recorded in a material form or not.' (AP. 2024; OAIC. n.d.)*

The Telecommunications amendment Bill (2022) also refines this data by defining who can collect and under what conditions that data must be stored (AP, 2022).

This legislative context stipulates that OSINT information such as health, tax file, credit, and employee records are all encompassed as personal information can only be collected under specific conditions. An enforcement body including the NIC, Federal Police, and Immigration Department can gather personal information if "*the department reasonably believes that collecting the information is reasonably necessary for... one or more enforcement related activities*" (OAIC, 2022. Section 3.49). This means that the collection of identifiable information requires *reasonable suspicion* on the part of the collection agency that those individuals are a risk.

This is a targeted type of data gathering, yet targeted data gathering is only one type of data collection strategy. Robust OSINT uses a passive collection strategy with a discovery method rather than this targeted collection. There is a legal limitation (Cybertrace, 2024) for the NIC therefore that OSINT might be in breach of legal frameworks. As an example, one OSINT tool which works passively is Maltego. It can be set to pool together various types of data and, depending on the access used, automatically scrape new data in an untargeted way; this casts a broader net of data collection than what a targeted collection would normally include. Both the collection of and storage of vast amounts of this kind of data might be in breach of the legal

context for the NIC. As suggested by Scott (2023), NIC might be limited by the legal context and need to outsource OSINT gathering and analysis (discussed in section 5. below).

2. Historical habits in intelligence analysis of the NIC organisations

A limitation to the use of OSINT for the NIC is the historical and habitual use of OSINT as a support intelligence stream amongst the NIC, leading also from structural changes and its historical use. Structural changes in the NIC have relegated OSINT to a bureau within one organisation creating a structural limitation to its use. This relegation creates a practical negative impact on OSINT capabilities. Recent changes in the Australian intelligence community shifted the open-source capability from DFAT to ONA and onto to the newer ONI and a specialised branch called the Open-Source Intelligence Branch (OSIB) (Scott, 2023. p 21-23). Currently OSINT work is performed in this singular branch and disseminated to other partners in the NIC. With these changes, OSINT is relegated to a support role for other intelligence analysis. This is a structural limitation to the use of OSINT.

Another limitation is the historical limitation in its use. Historically OSINT has been heavily integrated with other classified intelligence in the Australian intelligence context. This limits the utility of OSINT to a support tool (Scott, 2023. p 21). NIC historical intelligence consumption habits limit the use of OSINT because OSINT capabilities are much broader now. Thus, these capabilities, if left unleveraged, present limitations to the NIC intelligence product. OSINT leverages open-source information at scale, collecting data from social media posts, photos, manifestos, internet ports, satellite images, mapping, and a variety of other sources. With such data collections, OSINT creates a yet unknown data architecture. One such repository consists of open ports across internet linked devices specifically tailored to the Internet of Things (IoT); this was not available historically as ports and the IoT was simply not a leverageable intelligence space. We clearly see the change in the use case for OSINT, especially the sub-field Online Open-Source Information (OOSI). OSINT is already part of the NIC intelligence product because it has always been useful.

To counter this limitation, Scott (2023) suggests that OSINT deserves its own organisation in the NIC or outside consultancy. There are distinct disciplines for using OSINT (discussed later) which, when integrated with secret intelligence, would create more optimal intelligence resources. Although this integration is meant to 'effect greater integration of open-source material into assessment' (Flood report as cited in Scott, 2023. p 21) it may be better to have a dedicated OSINT organisation to improve intelligence for NIC.

The Scott (2023) white paper further suggests that using more outsourced OSINT would afford stronger analysis. Known outsourcing may have already occurred within the NIC. Several organisations and groups are known to be secure and vetted by NIC for security reasons. Such outsourceable organisations may include OSINT Combine (a sponsor and exhibitor at this year's AIPIO Sydney Conference, and a head office in Sydney), OSINT Industries, Trace Labs, and Bellingcat. Although these groups are not all situated within Australia, they all leverage OSINT skills and expertise internationally, and have known consultancy roles with other member nations of the 5 eyes.

3. OSINT as part of the intelligence product in NIC

A limitation to the use of OSINT for the NIC is the change in the use-cases for OSINT data given a habitual use of it as support intelligence. Open-source data is readily available, and it has been shown to be highly effective across various arenas of intelligence (Baker, 2023). Ransom (1970. p 19-20) suggests that over 80% of the material collected for intelligence purposes historically came from "overt, above-board methods". Contrastively, above-board and overt are starkly different to secret and covert collection methods, which subsume most of the activity of the Australian Intelligence community (Medcalf, 2023). OSINT has always been part of the regular intelligence gathering operations offering refinement and targeting for covert and secret intelligence sourced material. The Australian intelligence community has relied on both open and classified intelligence historically because they offer different strengths and weaknesses (Scott, 2023. p 24), yet OSINT has been historically used in support of these secret and covert data sources (Taylor, 2023; and Aly, 2008).

Over time, the use case for OSINT has changed. OSINT has undergone a revolution as major journalists and citizen intelligence officers have shown links and trends previously not available for intelligence analysis (Higgins, 2021. p 60). While previously OSINT was the domain of documents and text, the changes in internet connectivity means the data is inundated with interactions, pictures, videos, and surrounding discoverable intelligence including devices like Strava watches. Additionally, there has been a constant threat of open-source activities affecting Australia from various domains (Fitriani, & Shih 2023). In direct comparison to classified intelligence sources, OSINT uses open-source data.

4. Outsourcing OSINT; the individuals with the skills and expertise

A limitation to the use of OSINT for the NIC is the integration of types of data, at scale, by outsourced groups could lead to a confusing intelligence product. The strength of outsourcing comes from leveraging skills already in use by individuals, but with that comes the limitation of unvetted individuals, operating within a slim ethical window.

Data type/scale:

Suggested by Scott (2023 is the potential for the NIC to outsource OSINT. This comes with various limitations. These limitations include a set of legal and technical issues, skills and training variability, and an omni-present ethical concern for the use of OSINT.

Key limitations for outsourcing OSINT by the NIC include the data types themselves, their scale and the people who have the skills to process it. Firstly, with vast arrays of data sources capture-able by OSINT tools and techniques comes vast types of data. The scale of the data types collected is seemingly endless, meaning the utility of the data collected is equally broad providing a difficult challenge for a small team within a single NIC Organisation. As mentioned, OSINT can collect geolocation data as well as Social Media Intelligence (SOCMINT), Dark Web Intelligence (DWINT) and other intelligence types. These data types and reports might not align easily with NIC traditional secure and covert intelligence data, leading to disparate intelligence products. Secondly, large collections of data types also come at scale. After changes in

the internet's structure, Online Open-source Intelligence (OOSI) has taken on a whole new aspect; super-massive datasets. Using data at this volume has its own kinds of problems. Housing large volumes of data equates to a security risk and is potentially in breach of legal frameworks in Australian (discussed earlier). In addition, at scale, reliability and data security are an issue (Hwang et al, 2022. p 2-4). Due to the volume, it is impossible to verify and keep secure every individual source (ibid. p 4). The volume of data, perception and prejudice of that data, technical constraints, and potential for misuse are all key disadvantages of OSINT (ibid. p 4-5). For the NIC context, data collection at scale requires dedicated space and compute power. Data volumes of this size, even if outsourced the NIC, could lead to legal ramifications for independent organisations. Finally, OSINT is, by definition, in the public domain, and individuals who have the skills to process it tend to also be. External OSINT expertise, groups, and individuals are not vetted security officers although their reputation in OSINT relies on their publishing of their findings. NIC intelligence succeeds historically because they remain outside of the public domain. These are key limitations to their utility for NIC departments.

Skills mismatch:

OSINT requires a specific set of skills and expertise. A limiting factor for outsourcing OSINT is the inhomogeneous output of individual analysts. There are no current homogenous workflows for OSINT which all individuals follow. Although various workflows abound in online toolkits, these are not always shared methodologically. In parallel with this, the skills and tools used are not shared amongst all individuals. While someone using Google Maps and NASA FIRMS will be able to navigate geolocation data fluently, they may not be well versed in navigating open ports, shipping, or munitions databases. Some OSINT groups offer training across these entry level tools, but more advanced levels do not share methodological workflows. This may frustrate and elongate the selection process for the NIC agencies in outsourcing OSINT to various practitioners, making some call for more training within the NIC for OSINT specific skilled individuals (Murray, 2025).

Ethical risks:

The biggest limitation regarding outsourcing OSINT for the NIC is the slippage between intelligence gathering and black-hat hacking. Some OSINT tools very closely resemble Red-Team or Black-Team tools, but OSINT itself should remain ethical and passive (according to both Botwright, 2024, and Baker, 2023). While some groups promote strong ethical standards in OSINT data collection and analysis, others promote a more active approach. Any outsourcing of OSINT would necessarily come with standards, but any outsourcing specialist may pose an integrity risk for NIC. Botwright (2024) suggests that there is a fine line between using OSINT tools in an ethical way, and an unethical way. Baker (2023) similarly shows that slippage exists when using tools for malicious or unethical motivations, offering a list of ethical standards promoted by many OSINT practitioners.

Who would maintain ethical standards while effecting strong OSINT

The OSINT community, including groups like Bellingcat, can affect impressive investigations across a range of intelligence domains from shipping, munitions, cold cases, criminal networks, and terrorist networks. We have seen Bellingcat track munitions and individuals, find hidden people using tools like Strava, and effect awareness of false media through open data sharing and reporting (Baker, 2023; Higgins, 2021). These groups are therefore well positioned to operate in support of the NIC, especially because they are not beholden to Australian legal limitations.

In corollary to this, a strong shared ethos guides public OSINT practitioners of this kind which might not guide other agents and agencies. Though a less ethical cadre of groups and individuals abound, those affiliated with ethical OSINT meet the needs of the NIC. There exists a permeable and delicate ethical awareness shared by most (but not all) OSINT enthusiasts, yet the practices are highly contingent with the potential for black hat hacking.

In summary

The use of OSINT data sources is not new for the NIC. It has been noted that OSINT by other names is a key aspect of intelligence historically and still makes up a significant proportion of the work of various organisations in the NIC, like the ONI. While the Scott (2023) paper rigorously indicates the benefits of the NIC using OSINT skills and intelligence, it is aware of several limitations. It is suggested in this paper that a key limitation is the legal framework in Australia not aligning with the discovery methodology for general OSINT data collection. Additionally, as OSINT is inherently in the public domain, there is a risk to covert analysis to the NIC. Finally, if outsourced, OSINT practitioners may present their own limitations. Individuals tend not to be uniformly skilled, practiced, or aligned in workflows. Additionally, the slippage between OSINT and hacking is always apparent, risking the ethical framework of the NIC if outsourcing. While there are these key limitations to using OSINT to the NIC, its analytical power and achievements make it an important part of the intelligence makeup. By following Scott (2024) and Murray (2025) suggestions, these limitations to the use of OSINT by the NIC can be overcome by training individuals specifically in their use and allocating an organisation specifically for OSINT intelligence gathering and analysis.

Bibliography:

1. Aly, W. (2008). *Axioms of aggression: Counter-terrorism and counter-productivity in Australia*. *Alternative Law Journal, 33*(1), 20–25.
2. Australian Parliament (AP). (2022). *Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022* (Bill No. r6943). *Parliament of Australia*. Retrieved July 30, 2025, from https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6943
3. Australian Parliament (AP). (2024). *Privacy and Other Legislation Amendment Act 2024 (No. 128, 2024)*. Federal Register of Legislation. https://www.legislation.gov.au/Details/C2024A00128
4. Baker, R. L. (2023). *Deep Dive: Exploring the real-world value of open source intelligence*. Wiley.
5. Botwright, R. (2024). *OSINT Cracking Tools: Maltego, Shodan, Aircrack-Ng, Recon-Ng*. Pastor Publishing Ltd.
6. Cybertrace. (2024, May 30). *Is OSINT legal?* Cybertrace. Retrieved July 15, 2025, from https://www.cybertrace.com.au/is-osint-legal/
7. Fitriani, & Shih, S. (2025, May 7). *Mapping a decade's worth of hybrid threats targeting Australia. The Strategist.* Australian Strategic Policy Institute. https://www.aspistrategist.org.au/mapping-a-decades-worth-of-hybrid-threats-targeting-australia/
8. Higgins, E. W. (2021). *We Are Bellingcat: An Intelligence Agency for the People*. Bloomsbury Publishing.
9. Hwang, Y.W., Lee, I.Y., Kim, H., Lee, H., and Kim, D. (2022). Current Status and Security Trend of OSINT. *Wireless Communications and Mobile Computing, 2022.* https://doi.org/10.1155/2022/1290129
10. Medcalf, R. (Host). (2023, June 15). *Australia's intelligence leaders in conversation* (No. [episode number, if known]). [Audio podcast episode]. In *National Security Podcast*. Australian National University. https://shows.acast.com/the-national-security-podcast/episodes/australias-intelligence-leaders-in-conversation
11. Murray, C. (2025). *We can do better with OSINT: It needs structured training and careers*. The Strategist – Australian Strategic Policy Institute. https://www.aspistrategist.org.au/we-can-do-better-with-osint-it-needs-structured-training-and-careers/
12. Office of the Australian Information Commissioner (OAIC). (2022, December). *Australian Privacy Principles guidelines: Combined* (Version 1.4). https://www.oaic.gov.au/__data/assets/pdf_file/0028/8736/app-guidelines-combined-December-2022.pdf

13. Office of the Australian Information Commissioner (OAIC). (n.d.). *The Privacy Act* (Privacy legislation). Retrieved August 3, 2025, from https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act

14. Ransom, H. H. (1970). The intelligence establishment. Harvard University Press.

15. Scott, B. (2023). *Adapting Australian intelligence to the information age* (Occasional Paper, December 2023). ANU National Security College. https://nsc.crawford.anu.edu.au

16. Taylor, C. (2023, August 2). *An inflection point for Australian intelligence: Revisiting the 2004 Flood Report*. Australian Strategic Policy Institute. https://www.aspi.org.au/report/inflection-point-australian-intelligence-revisiting-2004-flood-report/