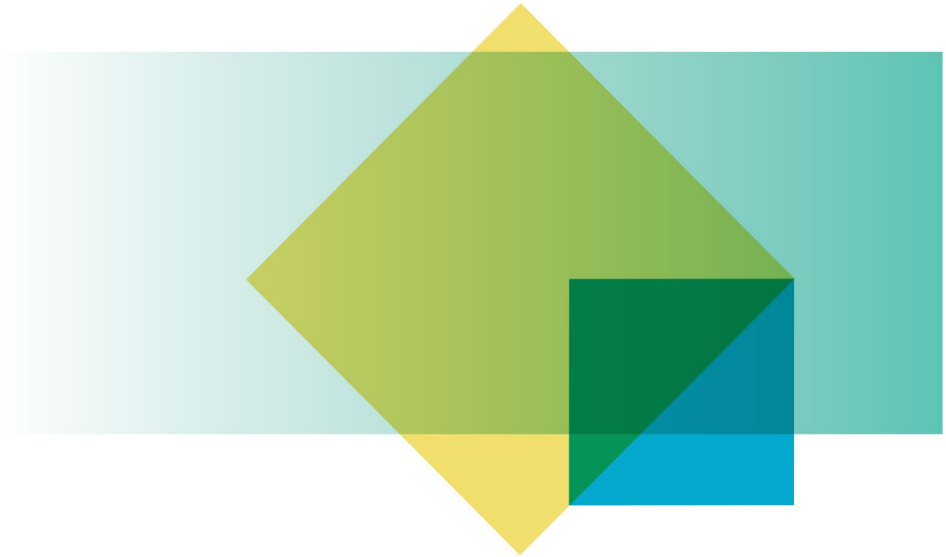
Australian Government

Office of the Australian Information Commissioner

Reform of Australia's electronic surveillance framework

Submission by the Office of the Australian Information Commissioner



Angelene Falk

Australian Information Commissioner and Privacy Commissioner

18 February 2022

OAIC

Contents

Introduction

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission on the *Reform of the electronic surveillance framework Discussion Paper* (the Discussion Paper) released by the Department of Home Affairs on 6 December 2021.

In our view, these reforms present a timely opportunity to ensure Australia's electronic surveillance laws provide a strong, robust framework where privacy protections for individuals are at the forefront.

The Discussion Paper highlights that the current framework is long, complicated and difficult for intelligence agencies, oversight bodies and industry to understand and comply with. This in turn puts at risk the effectiveness of protections for personal information.[1] The OAIC therefore supports the objective to create a single Act clarifying the application and use of electronic surveillance powers in Australia.

Electronic surveillance powers are highly intrusive and have a significant impact on an individual's privacy. This is particularly apparent in today's society as technology means that an increasing amount of information and data is accessible and available. This has created a complex digital and communications landscape. Changes to the current framework that result in new areas of surveillance expand the potential to intrude on an individual's privacy. As such, these powers must be subject to strict controls and be precise enough to provide the Australian community with transparency about how these powers are expected to be exercised.

Whilst the right to privacy is not absolute, any adverse impact on privacy must be subject to a critical assessment of its necessity, legitimacy and proportionality.[2] Further, any framework which provides for the intrusion of an individual's privacy must be accompanied by increased oversight, accountability and transparency. This will also assist in ensuring community trust and confidence in the framework.

The OAIC is Australia's national privacy regulator and has engaged with the Australian Government over several years on matters related to privacy and electronic surveillance. As the Discussion Paper identifies, Australia's current framework has been the result of a 'patchwork' of amendments across several decades. At each stage of these developments, the OAIC has advocated for consistent, comprehensive regulatory frameworks which help regulated entities understand their rights and obligations.[3] The OAIC considers that the electronic surveillance framework should be underpinned by strong privacy protections and that individual privacy should be at the core of the framework.

---

[1] Reform of Australia's electronic surveillance framework Discussion Paper, page 3.

[2] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* UN Doc A/HRC/27/37 (2014), paragraph 23, https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx.

[3] Australia's 2020 Cyber Security Strategy: A call for views – submission to the Department of Home Affairs, 11 November 2019, OAIC submission to the Comprehensive Review of the legal framework of the National Intelligence Community, 31 January 2019, Public consultation on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 — submission to Department of Home Affairs, 13 September 2018.

This submission sets out five recommendations for consideration by Home Affairs as it works to develop the reformed framework.

As these reforms develop, it will be crucial to ensure that an appropriate balance is struck between the exercise of electronic surveillance powers and the protection of the privacy of individuals. The OAIC welcomes engagement from Home Affairs as it undertakes this reform process.

Guiding principles for reform

A key objective of this reform process is to modernise Australia's electronic surveillance laws to reflect technological developments. However, this has the potential to result in new and expanded approaches to surveillance which present new risks to privacy.

To guide this reform, the Discussion Paper identifies five principles which the Government will seek to balance throughout this reform process. These guiding principles seek to ensure that the reformed framework:

- better protects individuals' information and data, including by reflecting what it means to communicate in the 21st century
- ensures that law enforcement agencies and ASIO have the powers they need to investigate serious crimes and threats to security
- is clear, transparent and usable for operational agencies and oversight bodies, as well as industry who need to comply with the obligations of the framework
- is modernised, streamlined and as technology-neutral as possible, by updating key concepts and clearly identifying the agencies that can seek access to this information
- contains appropriate thresholds and robust, effective and consistent controls, limits, safeguards and oversight of the use of these intrusive powers.

The OAIC is supportive of these guiding principles but considers that there is a tension between them, which will require careful consideration as to how they can be appropriately balanced.

This submission sets forward a number of recommendations which are intended to help inform Home Affairs' work in ensuring these principles are appropriately proportioned when developing the new framework.

Community expectations on government access to data

Public confidence can be difficult to obtain and maintain where agencies exercise intrusive powers in secret. Individuals may not precisely know how or when powers are being utilised. This creates a unique challenge in securing public trust in electronic surveillance, and heightens the need for privacy to be properly considered at the outset in the design of the reformed framework.

The OAIC's Australian Community Attitudes to Privacy Survey 2020 (ACAPS) found that Australians are more comfortable with the government using their personal information than businesses[4] but that most individuals (83%) would like government to do more to protect the privacy of their data. The survey found that privacy is a major concern for the majority of Australians (around 70%) and 84% of Australians believe that personal information should not be used in ways that cause harm, loss or distress.

Between 2007 and 2020, the survey showed a 14% decline of trust in Australian Government personal information handling. The percentage of respondents who agreed that the government was trustworthy with regards to how they protect or use personal information dropped from 64% to 51% in that period.

The OAIC's research demonstrates declining levels of trust among the community and a desire for more to be done to protect individuals' privacy in the face of new and emerging risks.

Individuals expect that the government will take robust steps to secure and protect their data, expectations which may be above and beyond those of other entities that have access to their information. The OAIC considers that this reform presents an opportunity to ensure public confidence in government access to data is maintained, especially in light of the covert nature of the powers being legislated.

We recommend that privacy safeguards be enshrined in the reformed framework and that the Act clearly articulate the expectation that privacy is a primary consideration when deciding whether to exercise electronic surveillance powers. This includes providing evidence to demonstrate necessity and ensuring that the scope of the warrant is clear and transparent.

We further recommend that the protection of privacy be included as a main objective of the new Act. Recognising privacy in this way will assist in shaping the reformed framework and ensuring that the interpretation and application of powers by intelligence organisations occurs through this lens – as the community expects.

Recommendation 1: Strong privacy safeguards should be embedded in the reformed framework to meet the community's privacy expectations and give individuals confidence in the operation of the framework. The concept of privacy should be included as a main objective of the framework.

Adopting a proportionate approach to electronic surveillance

Home Affairs has identified improving the protection of individual's information and data as a guiding principle for this reform. Home Affairs also seeks to ensure that a reformed framework provides

[4] See Australian Community Attitudes to Privacy Survey 2020 pp 32–34.

enforcement agencies with powers to investigate serious crimes, is technology neutral and reflects modernised methods of communication.

Whilst these guiding principles can present a tension, they can both be achieved by adopting a proportionate approach to ensuring the need for surveillance does not overshadow the right to privacy.

The OAIC acknowledges the importance of intelligence agencies having access to electronic surveillance powers to protect national security and prevent serious crime, such as child sexual abuse and cybercrime. The right to privacy is not absolute, however, any interference with privacy must be subject to a careful and critical assessment of its necessity, legitimacy and proportionality.[5] It is important to ensure that privacy intrusive powers provided to intelligence agencies are limited to only what is necessary.

Part of taking a proportionate approach is considering what safeguards can be implemented to mitigate privacy risks. To achieve a proportionate approach, we provide a number of recommendations below.

The Discussion Paper proposes to simplify provisions where necessary in order to ensure the reformed framework is consistent and entities are aware of their obligations. The OAIC supports this proposal and acknowledges that the current framework has been outpaced by technology and is complex, with different thresholds applying to equivalent powers.[6]

The OAIC further acknowledges the desire to 'future-proof' Australia's electronic surveillance framework, by introducing technology neutral provisions and amending the definition of communication to address new and emerging types of information. While this approach might allow for greater flexibility in adapting to technological advances, the lack of specificity could allow future impacts on privacy that are not yet known or contemplated. In our view, the exercise of intrusive powers requires a degree of precision that technology-neutral definitions may not allow.

To protect against this, the OAIC recommends that a reformed framework should provide clear, specific requirements about the collection, use and disclosure of an individual's communications. This should include what data can be accessed, how this access occurs and what the data can be used for. It will be important that these rules are appropriately prescriptive and do not allow for a high degree of discretion. This baseline standard of privacy should be reflected in the primary legislation. Any necessary specificity can then be outlined in subordinate legislation in consultation with stakeholders.

One way of building this baseline standard of privacy, is to ensure that the consideration of privacy is mandatory before a warrant is issued, or an authority is able to exercise applicable powers. This is especially important given the intrusive nature of electronic surveillance powers and the impact they

[5] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* UN Doc A/HRC/27/37 (2014), paragraph 23, https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx.

[6] The current electronic surveillance framework contains more than 35 different warrants and authorisations spanning multiple Acts including: the *Telecommunications (Interception and Access) Act 1979* the *Surveillance Devices Act 2004*, parts of the *Australian Security Intelligence Organisation Act 1979* and parts of the *Telecommunications Act 1997*.

have on individuals. This should also apply to third parties implicated in the execution of warrants or authorisations.

Further, checks and balances should be built into the reformed framework to manage the associated risks and protect against potential harms. For example, we consider that issuing authorities must have the appropriate level of seniority to make a decision regarding an application for a warrant or authorisation to exercise covert surveillance, and that this should be consistent across all equivalent warrants or authorisations.

The OAIC also recommends that consistent thresholds for warrants are set across all intelligence agencies.

Further, to assist in ensuring transparency and accountability, appropriate oversight should also be included, as well as embedded review mechanisms within the Act.

Recommendation 2: The reformed framework should provide clear and specific requirements to ensure privacy of individuals' communications is protected

Recommendation 3: The reformed framework should require the impact on an individual's privacy be considered before a warrant is issued or an authority exercises their powers

Recommendation 4: The reformed framework should provide for appropriate oversight and embedded review mechanisms

International privacy standards for intelligence agencies

The six Australian intelligence community agencies have generally been wholly exempt from the *Privacy Act 1988* (Privacy Act) and the Australian Privacy Principles (APPs).[7] The Privacy Act remains applicable to the Australian Federal Police and Home Affairs.

The OAIC's role includes regulating these entities and more broadly, promoting the objects of the Privacy Act and the privacy of all Australians.

In our view, the approach to privacy and electronic surveillance should be informed by international developments.

We note that in 2017, New Zealand amended the *Privacy Act 1993* (NZ) to require the New Zealand Security Intelligence Service and the Government Community Security Bureau to comply with most of the information privacy principles.

[7] See s 7(1) of the *Privacy Act 1988*. However, they are regulated by Part VIIIA of the *Privacy Act 1988* which has broad application and relates to, amongst other things, the collection, use and disclosure of COVID app data.

In 2018, the United Kingdom created a new framework in the *Data Protection Act 2018* (UK) which introduced six data protection principles for data processing by intelligence services.

The Canadian Security Intelligence Service also has obligations under the *Privacy Act 1985* (Canada).

This reform presents a timely opportunity to consider introducing consistent privacy safeguards for intelligence agencies that more closely align with those in the APPs, rather than to continue agency-specific privacy frameworks.

We acknowledge the unique statutory functions of each intelligence agency, and their particular operating environments, may make compliance with all aspects of the APPs impractical.

However, minimal departure from the APPs across the intelligence agencies will give individuals greater confidence that their personal information will be managed in a consistent, accountable and transparent manner.

In our view, it is important that Australia look to comparable jurisdictions regarding their treatment of electronic surveillance information as a part of this reforms and ensure that it meets best practice.

Recommendation 5: Consideration should be given to the APPs to form the basis of consistent privacy requirements across intelligence agencies in line with other comparable jurisdictions.

Conclusion

The OAIC recognises that intelligence agencies require electronic surveillance powers to protect Australia from security threats and prevent serious crime. We support the objectives of the proposed framework, however we also consider that there is a degree of risk that these reforms will expand the potential for privacy impacts by pushing into news areas of surveillance.

Therefore, careful consideration will need to be given to ensure that an appropriate balance is struck between the need for electronic surveillance and the privacy of Australians.

We consider that intelligence agencies should be held to consistent standards when it comes to individual's information and data and that the reformed framework should be subject to appropriate checks and balances. In our view, covert powers are more likely to be necessary, reasonable and proportionate when provided for in a strong, robust framework that restricts power where needed.

Research shows that Australians value their privacy highly and believe that the government should be doing more to protect them. This reform presents an opportunity to build community trust by enshrining robust privacy safeguards.

The OAIC looks forward to examining this proposal further to protect the privacy of individuals, while meeting the need to prevent threats to Australia's security and combat serious crime.

We welcome engagement with Home Affairs as they work to develop this framework and the Exposure Draft legislation.