# Submission to the Department of Home Affairs

Responding to the

## *Reform of Australia's electronic surveillance framework discussion paper*

22 February 2022

DIGITAL RIGHTS WATCH

# Overview

We welcome this opportunity to provide comments to Home Affairs responding to the discussion paper on the *Reform of Australia's electronic surveillance framework*.[1] Digital Rights Watch has a long track record of campaigning on and engaging with government policy and consultations on surveillance policy, including the Assistance and Access Act (TOLA), the Metadata Retention Act, the Identify and Disrupt Act, and the International Production Orders (IPO) Bill.

We recognise the legitimate interest in simplifying and streamlining the complex landscape of surveillance legislation, but at the moment the review does not include several key pieces of legislation (some mentioned above) which have fundamentally impacted the surveillance landscape. These include:

- Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015
- Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA)
- Surveillance Legislation Amendment (Identify and Disrupt) Act 2018
- International Production Orders Act 2021

Further, given the timing of the government's current review of the Privacy Act, we believe the primary objectives of this review – to better protect Australians' rights – would be best served by the introduction of a Federal human rights framework. In the absence of this, the objectives of a simplified *Electronic Surveillance Act* should be coupled with clear requirements for the use of its powers to reflect and comply with Australia's human rights obligations under the *International Covenant on Civil and Political Rights* and the *Universal Declaration of Human Rights* and as further guided in supplementary documents such as the *The Necessity and Proportionality Principles on the Application of Human Rights to Communications Surveillance*.[2]

## Digital Rights Watch

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, and advocate for a digital environment where individuals have the power to maintain their human rights.[3]

[1] Referring to the discussion paper published by Home Affairs: https://www.homeaffairs.gov.au/reports-and-pubs/files/electronic-surveillance-framework-discussion-paper.pdf

[2] The N&P Principles can be found in full at: https://necessaryandproportionate.org/principles/

[3] Learn more about our work on our website: https://digitalrightswatch.org.au/

# General remarks

Over the recent years, the Australian government has introduced several key pieces of legislation to enable and ease the surveillance of Australians in the name of our collective security. The extent of the powers granted to Australian intelligence agencies and law enforcement far outpace countries with similar legal frameworks, such as the United Kingdom, and serve to enable international operations where other jurisdictions would face restrictions on human rights grounds, like the United States.[4]

During our extensive consultations on the Assistance and Access Act (TOLA) with Dr James Renwick in his time as the Independent National Security Legislation Monitor (INSLM), the UK's Investigatory Powers Act was of particular relevance given its parallels to the investigatory powers sought by Australian agencies. It should be noted that in his final report evaluating TOLA, Dr Renwick made several recommendations regarding how Australia should strengthen the oversight and transparency of this legislation to give individuals the same certainty as those in the UK enjoy. Moreover, he noted that the legislation faces ongoing challenges in front of UK and EU Courts – an avenue to assert individuals' rights which is not available to Australians.[5]

In June 2021, Australian intelligence agencies made headlines for participating in Operation Ironside – an intelligence operation conducted over the course of several years with the United States Federal Bureau of Investigation (FBI) – where Australia's lack of legal protections for the privacy of individuals was a key component of the feasibility of the operation. Australian law enforcement was able to operate outside of the legislative bounds which the FBI is subject to under US law, resulting in great success for this intelligence operation, as well as a grim spotlight on Australia's ongoing disregard for human rights protections and continued increase of state surveillance.[6]

Given the above, one of the primary objectives of the electronic surveillance review - to "better protect individuals' information and data, including by reflecting what it means to communicate in the 21st century" - should be first and foremost addressed as a part of the broader ongoing Privacy Act review.[7] While it is important for the new surveillance framework to specifically recognise the rights of data subjects, more generally, it should operate within a system which holds robust privacy protections for individuals, granting them rights towards government as well as private entities.

**We believe that recognising the right to privacy at the federal level is critical in ensuring the privacy of all Australians remains protected.** Enshrining an enforceable right to privacy at the federal level would create a rights-based relationship to govern how Australians' data

[4] More about the UK's Investigatory Powers Act and how it impact human rights can be found here: https://www.libertyhumanrights.org.uk/issue/legal-challenge-investigatory-powers-act/

[5] Privacy International challenge of the IP Act over mass surveillance mandate was successful: https://privacyinternational.org/legal-action/cjeu-bulk-challenge

[6] In June 2021 headlines were made in all major publications over how Ironside was only possible due to the legal loopholes provided by the Australian legal system: https://www.theguardian.com/australia-news/2021/jun/11/act-giving-afp-powers-to-monitor-an0m-devices-did-not-become-law-until-after-fbi-operation-began

[7] From the discussion paper: https://www.homeaffairs.gov.au/reports-and-pubs/files/electronic-surveillance-framework-discussion-paper.pdf

and privacy are treated online, as opposed to an economic or value-driven model which has been the case to date.[8] While other amendments to the Privacy Act will play a key role in improving the protections against arbitrary infringements upon Australians' privacy by private companies, without a right to privacy the impact of the reforms made to the Privacy Act will remain limited. **DRW is of the view that Australia needs a comprehensive federal charter of human rights**, and a right to privacy is an essential and long-overdue component of an increasingly digital world and ecosystem. This right should be applicable as against both private entities and state agencies, including surveillance and law enforcement agencies.

In line with this, in our submission to the Privacy Act review, we urged the government to enshrine in law a federal level right to privacy in line with Article 12 of the United Nations (UN) Universal Declaration of Human Rights, to which the Australian government is a signatory. Article 12 states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".[9] Article 12 is well established and recognised around the world, and Australia is a signatory to the UN Universal Declaration of Human Rights. This would bring Australia into line with comparable jurisdictions and align with community expectations.

Anchoring the Australian surveillance reform in human rights law and best international practices for legality, proportionality, and necessity, is key in preventing an international race to the bottom with other state and non-state actors.

We further note the growing challenge of criminal and state-sponsored hacking and ransomware. Our view is that **digital security is a right of all citizens, and should not be sacrificed for surveillance purposes.** Too often, there is an assumption that national security is synonymous with state surveillance powers and capabilities. Individuals need to have the capacity to protect their communications, and our digital systems need to have access to tools like strong cryptography to resist unwanted intrusions. We acknowledge that no rights are absolute, but consistent with human rights principles, impositions on rights must be necessary and proportionate. Too often, in respect to state surveillance, there is little, if any attempt to articulate justifications for violations of human rights.

Lastly, we refer to the comments made by our colleagues at Electronic Frontiers Australia that there is likely to be little utility in rushing the process for developing a new framework. We would encourage the department to take the necessary time to get this right, which we expect will be longer than the current timetable.

We refer to the joint organisation letter to the Hon Karen Andrews MP dated 14 February 2022 and reiterate the submissions made in that letter. We address further specific matters raised by the discussion paper below.

---

[8] The emphasis on Consumer Data Rights (CDR) is evidence of this, as is the consideration by the Australian Bureau of Statistics to merge privately held datasets into the public census data to improve results and the "economic contribution" of the census. This value-driven calculation of privacy infringement vs economic benefit fundamentally shifts when we consider a rights-based system.

[9] Universal Declaration of Human Rights, *United Nations*. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights

**Private companies and state surveillance**

The discussion paper noted that: "The framework will have some impact on industry. The need to protect the integrity and security of communications and networks will be front of mind. Industry assistance will continue to be required – for example, in intercepting communications and accessing telecommunications data."

Private companies do not exist to enable and expand the potential of government surveillance. This is not why individuals use private services and they do not expect their engagement of these services to have this effect. Given the constantly deteriorating cybersecurity landscape, the primary role of all companies operating online services is to protect and secure the information of individuals travelling through their services and networks. Utilising this private infrastructure as a de facto space for intelligence and law enforcement agencies increases the threats that companies already face, and, notably, erodes the trust that Australians, as well as trading partners abroad, have in our systems and infrastructure.

During the INSLM review of TOLA, the issue of placing private companies at the centre of protecting individuals' rights from government overreach was brought up by several civil society representatives. For example, when the powers under TOLA are exercised, private companies can, to varying extents, challenge the validity of the request from the agency. As was noted in the final report by Dr Renwick, a situation may arise where a judge is faced with a representative from the government and a representative from industry to assess the matter, and no one present to argue on behalf of the individual.[10] Companies cannot and should not be the only vehicle through which individual rights can be considered in the process of considering applications for warrants and authorisations. While large international companies may have the resources and the business incentive to justify doing so, small and medium sized businesses are ill equipped to do so. Moreover, since individuals are not notified of the surveillance, before or after the fact, the absence of a public interest or human rights advocate is a startling omission. This structural problem puts privacy and security at risk (and is considered further below).

**Access by agencies**

We are concerned about the broad range of agencies that currently have access to warrants and authorisations under the relevant legislation. It is common, when a new national security reform is proposed, that the government will emphasise the seriousness of the offences that give rise to a need for such reforms. However, in practice, the availability of these powers to a broad range of agencies goes beyond what many members of the public would expect, and there is little evidence to demonstrate that this represents an effective balance between the rights of individuals and the needs of agencies. The discussion paper also acknowledges, with respect to the metadata retention regime, that 'concerns have been raised that the current effect of these sections may go beyond what was intended by Parliament.'

Any proposed new framework ought to confine authorisations and warrants to the minimum necessary number of agencies. This list of agencies should only be added to via a clear and transparent process, so the public is in a position to properly judge and debate whether the

[10] The final report by the INSLM on TOLA: https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf

justification provided demonstrates that this addition is necessary and proportionate. It would also provide the opportunity to assess whether the agency has appropriate security arrangements in place to manage any data that could be obtained as a result.

**Broadening the definition of communication**

In setting out what information can be accessed, the discussion paper identifies the need to update the current definition of "communications" – which is at the moment limited to the content/text of a message – to a much broader set of categories. It attempts to do this under the guise of forming a technology-neutral definition, stating: "The reform aims to replace the outdated concept of 'communications' with a term and definition that reflects the range of information and data transmitted electronically. The definition will be as technology-neutral as possible so that it can apply to future information and communications technologies."

The proposed expanded categories include an egregious amount of data that agencies cannot currently access, including email/message drafts, a variety of metadata and activity records generated on phones, computers and other digital technology, files which have not been transmitted to another person altogether, and even data generated or inferred from services that an individual may be using. It also will likely encompass data from internet connected devices (that is, the Internet of Things). The scope of this is clearly intrusive, and further, generated or inferred data is likely to be flawed, biased or otherwise inaccurate.[11] There remain outstanding questions about whether data collected in this way would be able to be held by the relevant agencies in a secure manner, given the range of agencies involved. It increases the surface attack for criminal hacking both for companies (required to hold communications data) and agencies (who seek access to it).

Any definitional change towards an overly general term risks obscuring important nuances that may be required to properly respect individual rights and tailor different powers to a demonstrated need by surveillance agencies.

**Warrants, authorisations and powers under surveillance law**

We note the following comments from the discussion paper: "the Government will further consider how the new framework could best integrate the ability of law enforcement to obtain warrants to collect intelligence, disrupt offending and collect evidence. In this regard, the Government intends to incorporate the existing powers introduced by the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (SLAID Act) to allow the Australian Federal Police (AFP) and the ACIC to obtain intelligence in relation to criminal networks and for the purposes of disrupting or preventing offending."

Simplifying warrants should not come at the expense of the individuals' rights.

It is not clear what is meant by the integration of frameworks, but we remain concerned about the broad ranging activities that can be undertaken under the SLAID Act, and would not support expansion of these powers without justification. When the government introduces expansive powers on the promise that they will only be used by a narrow set of agencies in

[11] Privacy International is one of many organisations who have documented the flaws of using derived data to infer information about individuals: https://privacyinternational.org/explainer/1310/big-data

very specific circumstances, only to shortly afterwards seek to expand these criteria, it undermines public trust.

We support the emphasis on privacy as a component of the new framework for the purposes of warrants and authorisations, and think this ought to be made explicit. There are other considerations that ought to be included in the process of agencies seeking warrants and authorisations, including the integrity and security of digital systems. We refer to our comments below about the need for judicial consideration as standard for all warrants and authorisations and the need for a public interest advocate to participate in this process.

In general, we support the idea that powers exercised under the new framework (including via warrants and authorisations) be subject to a necessary and proportionate test (at page 51 of the discussion paper). In addition to the proposed approach, consideration ought to be given to valuing a time limited approach surveillance, and rigorous guarding against the temptation of ongoing, bulk mass surveillance. There must also be evidence that the relevant agency has the capacity to store the information securely and has a plan for deletion. Without this assurance, there is a real risk that such data could attract malicious actors.

**The 'serious crime' threshold**

The justification for intrusive surveillance is framed as a requirement to respond to and prevent crimes such as terrorism and child sexual exploitation. We are concerned, however, that intrusive surveillance powers are routinely used for crimes that do not meet the level of severity that may justify such an intrusion.

It is inappropriate to widen access to surveillance powers beyond agencies that respond to the most serious of crimes.

We are of the opinion that the definition of a "serious criminal offence" should be specifically defined at a higher threshold than it is currently set. Further community consultation is required to more meaningfully determine a threshold of a "serious crime."

**Accountability, transparency, and oversight**

We support the statement set out in the discussion paper that "the new Act will set out clear principles for, limits on and expectations of agency powers. ... The Act will be complemented by detailed and transparent policies, procedures or rules to deal with matters that are too specific to appear in legislation or are subject to frequent change."

We support a UK 'double lock' system as a general principle - that is, that an independent judicial commissioner (iwe, a judge or magistrate) should be involved in approving activities conducted by surveillance agencies that violate the privacy of individuals. We acknowledge (as per the Richardson Review) that this may not be required where it would involve adding the relevant Minister to the process (as opposed to adding a judicial commissioner), however we note that many powers are currently free from judicial scrutiny, and we remain concerned about this tendency. The metadata retention regime, various requests and notices under TOLA, among others, are not currently subject to review by a judicial commissioner and ought to be.

Independent review by a judge or magistrate of warrants, authorisations and other privacy-breaching powers should be standard, and is essential to avoid overreach by agencies.

The Necessary and Proportionate Principles define (in principle 6) a competent judicial authority as one that is:

1. separate and independent from the authorities conducting Communications Surveillance;
2. conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights; and
3. have adequate resources in exercising the functions assigned to them.[12]

We recommend that for powers exercised under the new framework, the relevant Minister should provide an annual (or more frequent) report that details the number of warrants and authorisations issued. Without such information, it is impossible to assess whether agencies have sufficient powers at their disposal, and whether the impositions on rights created by these warrants and authorisations are justified.

Publication of judicial decision records for the issue of warrants would enhance transparency and accountability, and increase public trust and confidence in the use and oversight of surveillance powers. A reasonable level of transparency would be achievable by publicising the legal principles of warrants issued, rather than specific facts or details.

**Public interest advocate**

Intrusive surveillance powers should be used sparingly, and limited to exceptional and significant circumstances with full regard to human rights as enjoyed by all individuals. One of the reasons that overreach becomes possible is that the process for approving warrants lacks transparency and, in an adversarial system, there is no party that seeks to advance the interests of the public.

One of the recommendations of the PJCIS in relation to the Identify and Disrupt Act was to introduce a 'public interest advocate' in the decisions regarding warrants. We are of the view that the role of a public interest advocate should be prescribed in the new framework. A public interest advocate with a statutory mandate to defend human rights would play an essential role in ensuring that such rights are actively considered when issuing warrants to use intrusive surveillance powers. The advocate should be independent and selected from a judicially established panel of legal practitioners.

[12] See Principle 6 of the N&P Principles for more details: https://necessaryandproportionate.org/principles/

# Recommendations

The new surveillance framework should:

1. confine authorisations and warrants to the minimum necessary number of agencies and only add to this to via a clear and transparent process;

2. avoid an overly general definition for communications that does not permit nuance, respect individual rights and the capacity to tailor different powers to an demonstrated need by surveillance agencies;

3. simplify warrants but not at the expense of the individuals' rights, and subject them to a necessary and proportionate test;

4. raise the threshold in the definition of a "serious criminal offence;"

5. introduce a double lock system as standard;

6. provide for the relevant Minister should provide an annual (or more frequent) report that details the number of warrants issued under national security legislation and publish judicial records of these decisions; and

7. prescribe an independent public interest advocate to make submissions on any warrant application.

## Contact

Lizzie O’Shea, Chair, Digital Rights Watch

[redacted]