Electronic Frontiers Australia Inc.
ABN: 35 050 159 188
W www.efa.org.au
E email@efa.org.au
@efa_oz

Electronic Surveillance Reform Branch
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

11 February 2022

By web form

Dear Sir/Madam,

RE: Electronic Surveillance Reform

EFA welcomes the opportunity to comment on the Electronic Surveillance Reform discussion paper.

EFA's submission is contained in the following pages.

About EFA

Established in January 1994, EFA is a national, membership-based, not-for-profit organisation representing Internet users concerned with digital freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political, and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,

Justin Warren
Chair
Electronic Frontiers Australia

Introduction

EFA welcomes the government's intention to reform Australia's electronic surveillance framework. The existing framework is by parts complex, archaic, confusing, and not fit for purpose. The work to replace it will be complex, but necessary, and EFA welcomes the government's commitment to undertaking this task with the required dedication of time and resources to do it well.

Australia's future as a liberal democracy depends in no small part on our ability to get these reforms right. A global trend towards authoritarianism, secrecy, and fear must be resisted. We are encouraged by the long-term trend towards greater transparency and oversight of surveillance powers, and the understanding of many agencies that their social licence to operate depends on Australians' continued support for their work.

We have no desire to repeat the embarrassing failures of the past that have left Australia vulnerable, and damaged the reputations of the agencies whose very existence relies on Australians' continuing to believe they are necessary. The extraordinary powers these agencies are granted must always be used, and be seen to be used, in service of the best version of Australia we can imagine.

EFA is pleased to participate in the process of restoring trust in Australia's surveillance powers.

Summary of Recommendations

1. **Electronic surveillance should not be used to establish a library; any surveillance should be connected with a specific, not general, intended use.**
2. **That the legislative framework for surveillance clearly states the principles of liberal democracy on which it is based, the better to test the proportionality, necessity, and propriety of any surveillance powers.**
3. **Any framework should start from a blank slate and not simply continue to grant existing powers that are neither proportionate nor necessary.**
4. **Consideration should be given to including a federally enforceable Human Rights Act or equivalent human rights protections in any new legislative framework.**
5. **The target timeframe for draft legislation should be extended by at least a year—to 2023—to allow for appropriate levels of consultation with the Australian community.**
6. **The principles of Australia as a liberal democracy should take precedence over military, economic, or law enforcement interests.**
7. **Past failures of safeguards and oversight should be explicitly acknowledged and specific measures adopted that will reduce or eliminate a repeat of past mistakes.**

8. **Any claim of administrative burden should be supported by specific, clear evidence of the magnitude and scope of the claimed burden.**

9. **Oversight bodies' attention should be drawn to any use of new powers, or the use of powers in novel or unique circumstances.**

10. **Safety thresholds should be set for all powers before they are granted. If mistakes or deliberate abuse rises about this threshold, the powers should be automatically revoked for all agencies implicated in the mistakes or abuse.**

11. **When unlawful surveillance or data access occurs, the person(s) affected should be notified and informed of what surveillance was performed and what data was unlawfully accessed, and by which agency.**

12. **Set up a compensation scheme for persons subject to unlawful surveillance with statutory payment amounts aligned to the seriousness of the harm caused.**

13. **Collection of information must be addressed separately from use of information.**

14. **Information should only be collected using covert surveillance powers in connection with a defined and specific primary purpose, and once that purpose has been fulfilled, the information collected should be destroyed.**

15. **Information should only be accessed in connection with the same defined and specific primary purpose for which it was collected.**

16. **A human rights-based approach should be used to account for emerging technologies.**

17. **There should be no distinction made between content and non-content information.**

Outline of Submission

Before engaging with the specifics of the discussion paper, EFA has chosen to draw attention to certain foundational principles that should underpin the development of a future electronic surveillance framework. We are particularly grateful for the work of Dennis Richardson AC and the Comprehensive Review of the Legal Framework of the National Intelligence Community (2019)[1] to which we refer often.

EFA considers that any surveillance framework needs to be constructed with a firm commitment to Australia as a liberal democracy, and certain fundamental ideals that should not be sacrificed to fulfil some temporary or illusory notion of security.[2]

We then turn our attention towards safeguards and oversight, which we feel is fundamental to the successful operation of a framework that respects human rights while also providing for Australia's national security. EFA believes that human rights and national security are not in opposition; while there may, at times, be tensions between them that need careful consideration, ultimately the best resolution places human rights at the centre of our thinking.

We then address each of the major sections of the discussion paper in turn.

[1] Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (2019).
[2] Orin S. Kerr, 'A Theory of Law' (2012) 16(1) *Green Bag* <http://www.greenbag.org/v16n1/v16n1_ex_post_kerr.pdf>.

Foundational Principles

Before looking in detail at specific proposals made in the discussion paper[3], EFA submits that time should be spent agreeing on the foundational principles that will guide development of the proposals. The Richardson Review[4] spent considerable time discussing the foundational principles on which the legal framework for lawful surveillance is based.

The Review noted:

> Intelligence, therefore, must have a *purpose*. It is not acquired for its own sake; its acquisition is determined by its intended use.[5]

The Review also quoted Justice Hope:

> Intelligence is not collected in order to establish a library. Its collection is only justified by its use.[6]

EFA submits that this principle is particularly important, given the push by many agencies to allow them to collect ever larger data troves justified by the assertion that it may become useful one day.

Recommendation: Electronic surveillance should not be used to establish a library; any surveillance should be connected with a specific, not general, intended use.

The Review also noted:

> Perhaps the most effective yardstick for evaluating the ethical purpose of an intelligence activity is if the activity's authoriser—whether that person is a minister or an official—could justify the legality and propriety of the activity to wider society if the activity were to be made public. This is not to say that the public must approve of the action—it is difficult to find universal approval for any government activity or policy, let alone intelligence activities. But the authoriser must be so convinced of its importance that they can accept public criticism and establish a credible defence of their decisions.
>
> The benefit of this test is that it goes directly to the propriety of an activity—whether it is not just lawful, but also proportionate and necessary to achieve a legitimate objective.

---

[3] Department of Home Affairs, 'Reform of Australia's Electronic Surveillance Framework' (Commonwealth of Australia, 2021) <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/reform-of-australias-electronic-surveillance-framework-discussion-paper> ('Electronic Surveillance Framework Discussion Paper').
[4] Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (n 1).
[5] Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (2019) vol 1 [7.10].
[6] Justice Robert Hope, 'Royal Commission on Intelligence and Security Third Report' (Commonwealth of Australia, 1976) [13] <https://recordsearch.naa.gov.au/SearchNRetrieve/Interface/DetailsReports/ItemDetail.aspx?Barcode=30091090&isAv=N> ('RCIS').

> This test can include the national interest—Australia's security and prosperity as a liberal democratic society—and it can accommodate wider, more mutable, considerations that might also bear on the test, such as prevailing social values, ethical norms, fundamental human rights, or the judgement of other countries.[7]

EFA notes that the long-term historical trend of surveillance has been towards more legislated controls, oversight, and transparency, both in Australia and in comparable liberal democracies.

The Review endorsed the following principles:

> The constraints of the legal regime under which these activities are conducted are also critical. In our view, to ensure agencies act lawfully and for proper purposes, the legal regime should ensure:
>
> - ministerial accountability: the elected officials ultimately responsible for the agencies and their activities are held accountable to the Parliament
> - an authorisation process that operates according to the principles of lawfulness, propriety, necessity and proportionality
> - independent oversight of the legality and propriety of agencies' activities: oversight must be completely separate from authorisation; the overseer must have complete access to agencies' information and activities; and it must be statutorily independent, and
> - political impartiality: the agencies must be entirely independent of the political process.[8]

The Review also noted that "Australia has made a number of deliberate, principled choices to manage and limit the powers and activities of some of the NIC agencies" which include:

- the separation of security intelligence and law enforcement the separation of intelligence collection and assessment the distinction between foreign intelligence and security intelligence
- the distinction between operations that occur onshore and those that take place offshore, and
- the distinction between Australians and non-Australians.[9]

These principles, as the Review notes, were considered and endorsed some 40 years ago by the Hope Royal Commissions and have remained fundamental to the legal framework since. Despite this lengthy period of time with which to become familiar with the principles, the Review noted that:

> It is important that those working in NIC agencies, and particularly AIC agencies, understand these principles and the balance that Government and Parliament seek to find

[7] Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (n 5) [7.47].
[8] Ibid [7.49].
[9] Ibid [7.50].

> in such legislation. As discussed in Chapter [3], this was not universally the case among the agencies and staff we engaged with, including at senior leadership levels.[10]

This statement is alarming for a number of reasons.

Firstly, it indicates that there are senior leaders within the intelligence agencies that are actively working against the national interest (as determined by the process of democracy) due to their own mistaken understanding. This is unacceptable.

Secondly, it indicates systemic failures within the intelligence agencies to recruit and train staff so that they can effectively fulfil the mission assigned to them by the democratically elected government. Given the highly secretive nature of the agencies in question, it raises questions about just how widespread these misunderstandings are.

EFA submits that clearly articulated principles underpinning Australia as a liberal democracy should be front and centre of the process for reforming the electronic surveillance regime. Any legislative framework should include clear language that sets out fundamental principles that must be considered before any surveillance power is granted or authorised.

Recommendation: That the legislative framework for surveillance clearly states the principles of liberal democracy on which it is based, the better to test the proportionality, necessity, and propriety of any surveillance powers.

Agency overreach and the need for a reset

As noted in the Richardson Review, too often agencies ask for more power than they actually need, and for spurious reasons.

> Too often during the Review, proposals to 'clarify' or 'streamline' legislation amounted to no more than a bid to extend powers or functions. Government should be sceptical of calls for legislative clarity—very often such claims do not withstand even modest inquiry.[11]

Agencies also "had a tendency to suggest that legislative provisions presented barriers to their effective operation."[12] Yet these 'barriers' were often non-existent and more an issue of agency culture, policy or practice.

At other times, agencies ask for legitimate safeguards to be removed, sometimes claiming they present an 'administrative burden'. As the Review noted:

> The term 'administrative burden' tends to be thrown around too loosely by NIC agencies. Government should be wary of, and properly test, such claims.[13]

---

[10] Ibid [7.52].
[11] Ibid [3.19].
[12] Ibid [3.12].
[13] Ibid [3.14].

EFA submits that the fact that these attitudes were prevalent enough for the Review to highlight in such detail indicates that they have been present for some time. Indeed, it is likely that they were present for most—if not all—of the period since 11 September 2001 where 124 Acts making some 14,500 individual amendments to the legislative framework for the National Intelligence Community were made. Agencies have pushed hard for increased powers during this time, and for the most part their requests were granted, sometimes with unseemly haste.

EFA submits that while many of the adverse outcomes[14] predicted by civil society have come to pass[15], the dire predictions used to justify the granting of extraordinary powers have turned out to be somewhat overblown.

It is time to pause and re-assess.

In formulating any new legal framework we must keep the foundational principles of Australia as a liberal democracy firmly in mind. We must start afresh, and not mindlessly continue with a regime based on demands for powers that were built on shaky foundations. Failing to do so risks continuing an incentive structure where agencies make ambit claims for more power than they need, but which are nonetheless granted by an overly credulous Parliament, violating the principles of proportionality and necessity that should underpin the legal framework governing electronic surveillance.

Recommendation: Any framework should start from a blank slate and not simply continue to grant existing powers that are neither proportionate nor necessary.

A human rights framework

Australia stands alone as the only comparable liberal democracy that lacks federally enforceable human rights protections. EFA has long advocated that Australia needs a federally enforceable human rights framework to provide adequate safeguards against abuse of power.

Comparisons to other jurisdictions are often made, yet every other member of the Five Eyes surveillance alliance has these fundamental human rights protections; Australia does not. Countries such as the Netherlands and France also benefit from over-arching protections provided by the EU of which they are a member. Again, Australia lacks these fundamental protections.

In the absence of these fundamental protections, even greater care must be taken when granting surveillance powers to ensure they truly are necessary and proportional, and that the threat of abuse is taken more seriously. Australians lack protections and opportunities for redress that are available to citizens of other countries, and so law-makers must take greater care to ensure Australians' are sufficiently protected against abuse.

---

[14] 'Australian Police Can See More Of Your Metadata Than You Think', *Gizmodo Australia* (10 February 2020) <https://www.gizmodo.com.au/2020/02/australian-police-metadata-retention/>.
[15] '"Scarily Accurate": What You Found in Our Reporter's Metadata', *ABC News* (Text, 24 August 2015) <http://www.abc.net.au/news/2015-08-24/metadata-what-you-found-will-ockenden/6703626> ('*"Scarily Accurate"*').

Recommendation: Consideration should be given to including a federally enforceable Human Rights Act or equivalent human rights protections in any new legislative framework.

Take the time to get things right

The discussion paper states that "the Government intends to develop a new modernised and streamlined electronic surveillance legislative framework by 2023."[16] This is less than a year away.

The Richardson Review very clearly articulated, at some length[17], the complexity of the challenge of reforming Australia's electronic surveillance framework.

> Taking into account overseas experiences, we expect that it would take between two and three years to design and draft a comprehensive reform Act, before introducing it into the Parliament. Once passed, we would expect a minimum two-year implementation period.[18]

The discussion paper seems to suggest a timeframe that is substantially less than the timeframe suggested by the Review. This suggests that the government has failed to adequately appreciate the complexity of the undertaking and risks introducing fatally flawed legislation.

EFA notes that the discussion paper review period was open over the Australian summer holiday period. EFA also notes that multiple other government inquiries and requests for submission were simultaneously run during this same time period.

The discussion paper itself outlines, on page 8, ten separate review reports relevant to the scope of the discussion paper, not including the Richardson Review which itself consists of four volumes and approximately 1300 pages. Familiarity with this volume of material sufficient to provide an informed response to the discussion paper is not a simple undertaking.

Reforming Australia's electronic surveillance framework is important and should be treated with the seriousness it deserves.

Recommendation: The target timeframe for draft legislation should be extended by at least a year—to 2023—to allow for appropriate levels of consultation with the Australian community.

What should be protected, and why?

The essence of liberal democracy is the empowerment of ordinary people: not just the power to select the lesser of two evils every three years, but the power to make decisions about all aspects of their personal lives and to determine, collectively, what Australia means and what its future should be.

---

[16] Department of Home Affairs (n 3) 3.
[17] See, e.g. Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (2019) vol 2 ch 26.
[18] Ibid [26.146].

A great deal of recent "national security" legislation deliberately undermines the security and privacy of ordinary Australians, making it harder for us to be confident that our accounts are secure, our personal communications remain private, and our location and other personal data are not exposed and used against us. Legislation marketed as targeting terrorists and paedophiles has also been used against journalists who dared to report on war crimes allegations.[19]

Recent trends in Australian "national security" legislation undermine Australia's liberal democracy in two distinct but related ways: liberalism and democracy. They undermine individual freedom because they exacerbate the power imbalance between ordinary citizens and more powerful entities such as government officials and large tech companies - people change their behaviour when they are not sure whether their private choices and communications are actually being monitored. When invoked to threaten journalists, scientists, whistleblowers or others, they also undermine the open, public, democratic communication necessary for a healthy democracy.

National Security

EFA has noted that discussions of law enforcement and surveillance powers often invoke somewhat nebulous notions of *national security* to justify extraordinary powers.

We include here our understanding of what is meant by *national security* as defined in existing legislation to aid greater understanding of the term.

National security is defined in section 8 of the National Security Information Act.[20] It is defined to mean:

> Australia's defence, security, international relations or law enforcement interests.

We note that *defence* is undefined in the Act and thus takes on its ordinary meaning.

Security is defined by reference to section 4 of the ASIO Act:

> (a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:
>
> (i) espionage;
> (ii) sabotage;
> (iii) politically motivated violence;
> (iv) promotion of communal violence;
> (v) attacks on Australia's defence system; or

[19] 'I Live-Tweeted the Raids on the ABC — and It Was a First for the AFP', *ABC News* (online, 8 June 2019) <https://www.abc.net.au/news/redirects/backstory/investigative-journalism/2019-06-08/federal-police-raid-abc-office-john-lyons-live-tweeting/11192898> The "add, copy, delete or alter other data" wording was added to the Crimes Act by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.

[20] *National Security Information (Criminal and Civil Proceedings) Act 2004*.

(vi) acts of foreign interference;
whether directed from, or committed within, Australia or not; and
(aa) the protection of Australia's territorial and border integrity from serious threats; and
(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).

International relations is defined to mean 'political, military and economic relations with foreign governments and international organisations'.[21]

Law enforcement interests means:

(a) avoiding disruption to national and international efforts relating to law enforcement, criminal intelligence, criminal investigation, foreign intelligence and security intelligence;

(b) protecting the technologies and methods used to collect, analyse, secure or otherwise deal with, criminal intelligence, foreign intelligence or security intelligence;

(c) the protection and safety of informants and of persons associated with informants;

(d) ensuring that intelligence and law enforcement agencies are not discouraged from giving information to a nation's government and government agencies.[22]

EFA submits that this framing of national security preferences the needs of intelligence and law enforcement agencies over the human rights of the people of Australia to the detriment of Australia as a whole. For example, calls to undermine secure encryption attempt to privilege law enforcement interests over the security of Australians, placing the very notion of national security in tension with itself.

Recommendation: The principles of Australia as a liberal democracy should take precedence over military, economic, or law enforcement interests.

An Australia Worth Securing

EFA submits that a broader view of what keeps Australia secure is needed, and the views of agencies should not take precedence over the views of civil society. An Australia that places the desires of law enforcement and intelligence agencies over those of civil society would no longer be a liberal democracy worth the name.

"It became necessary to destroy the town in order to save it"[23] should not be the approach we take. To avoid this fate, we need to be very clear on what vision of Australia we are trying to

[21] Ibid s 10.
[22] Ibid s 11.
[23] Originally reported by Peter Arnett of the Associated Press in 1968, quoting an unidentified American officer during the Tet Offensive, there are now doubts about the quote's authenticity.

protect. Indeed, rather than attempting to preserve a static version of Australia from the past, we should be supporting measures to build the version of Australia we would prefer it to be.

However, in order to do this, we all—civil society, government, and the intelligence agencies included—need to have a common view on what that version of Australia looks like. EFA submits that the work on this foundational task is yet to be done.

Safeguards and Oversight

Unlike the discussion paper, EFA considers that safeguards and oversight are of such importance that they should be contemplated before other matters. As the Richardson Review noted, governance and oversight should be foundational to the development of any new legislative framework:

> The Review agrees that oversight should be integrated into legislative amendments in the early stages of their development. Oversight is an integral part of Australia's intelligence system. Consideration of oversight late in the development process is likely to impede the adoption of best practice or well integrated oversight. Oversight is also more than simply inspecting records, and must be more systematic than own-motion inquiries initiated by oversight authorities – it should be ingrained in all aspects of agencies' activities. This is unlikely to occur unless oversight is considered in the initial stages of developing legislation.[24]

The fact that electronic surveillance powers are extraordinary must be kept front of mind. As the Review noted:

> Electronic surveillance powers are among the most intrusive powers available to government agencies in Australia. They enable agencies to covertly collect information about people's private activities and behaviours, their private communications, and information they would wish to keep confidential.[25]

Covert access to an Australian's information and data is generally prohibited.[26] Any covert access to an Australian's information is therefore exceptional, and so safeguards and oversight of the circumstances of that access, and the process used to grant exceptional access, is of fundamental importance.

We have an opportunity to rethink when covert access should be provided, and when it should not, rather than continue to be bound by historical precedents from a previous era. We should not be bound by thinking that suggests that what was previously acceptable to deal with an imminent threat at that time should continue to be acceptable now that the threat has passed.

---

[24] Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (2019) vol 3 [40.114].
[25] Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (n 17) [28.16].
[26] Department of Home Affairs, 'Reform of Australia's Electronic Surveillance Framework' (Australian Government, 2021) 16.

Continuing to grant more and more exceptions to the law renders the term *exceptional access* essentially meaningless.

We must start with a clear understanding of past failures of safeguards and oversight if we are to ensure that protections against abuse are designed into any future surveillance regime.

Recommendation: Past failures of safeguards and oversight should be explicitly acknowledged and specific measures adopted that will reduce or eliminate a repeat of past mistakes.

Previous Protection Failures

There are numerous examples in recent years where protections and safeguards have manifestly failed. Examples include:

- An AFP officer abused data access to stalk their ex-girlfriend[27]
- Queensland police accessing contact tracing data[28]
- Widespread unauthorised access to telecommunications data across 20 agencies[29]
- Unlawful access to stored metadata by ACT Police over 3,000 times.[30]
- A facial surveillance tool used without proper authority[31]
- A police officer abused their access to police systems to stalk potential Tinder dates[32]
- ASD breaches of surveillance laws[33]

EFA notes that these are just examples of the failures *that we know of*. It is highly likely, given the covert nature of surveillance and the 'excessive devotion' to secrecy of Australian intelligence

---

[27] 3 Jun 2015 at 22:54 and Richard Chirgwin tweet_btn(), 'AFP Officer Abused Data Access to Stalk Ex' <http://www.theregister.co.uk/2015/06/03/afp_officer_pleads_guilty_over_stalking/>.
[28] Matt Dennien, 'Queensland Police Use of Check-in Data Sparks Reform Calls', *Brisbane Times* (28 June 2021) <https://www.brisbanetimes.com.au/national/queensland/queensland-police-use-of-check-in-data-sparks-reform-calls-20210628-p584x8.html>.
[29] Chris Duckett, 'Commonwealth Ombudsman Finds Instances of Telco Data Accessed without Authority at All Agencies Inspected', *ZDNet* (9 February 2021) <https://www.zdnet.com/article/commonwealth-ombudsman-finds-instances-of-telco-data-accessed-without-authority-at-all-20-agencies-inspected/>.
[30] 'ACT Police Admit They Unlawfully Accessed Metadata More than 3,000 Times', *the Guardian* (26 July 2019) <http://www.theguardian.com/australia-news/2019/jul/26/act-police-admit-unlawfully-accessed-metadata-more-than-3000-times>.
[31] *Commissioner initiated investigation into Clearview AI, Inc (Privacy)* [2021] AICmr 54.
[32] Frances Bell, 'Officer Used Police Computer Network to Stalk Dozens of Potential Tinder Dates', *ABC News* (Text, 1 February 2019) <https://www.abc.net.au/news/2019-02-01/officer-used-police-computer-to-look-up-tinder-dates/10771958>.
[33] Paul Karp, 'Australian Signals Directorate Reports Breaches on Spying, Wire Taps', *The Guardian* (online, 30 October 2019) <https://www.theguardian.com/australia-news/2019/oct/30/australian-signals-directorates-repeated-legal-breaches-unacceptable-senator-says>.

agencies[34], that there are many more failures that we do not know about. The Witness K and Collaery[35] cases illustrate the lengths that some agencies and their government enablers will go to keep their activities secret, no matter how unlawful or immoral they may be.

The sheer number and volume of failures indicates a systemic failure of safeguards, which demands a rethink of how safeguards are designed, and how systemic failures are addressed.

Power should be hard to use

Power that is easily used is also easily abused. As discussed above, far too many agency requests centre on making power easier to use. Power over others *should be difficult to use* because that difficulty provides an inbuilt safeguard against abuse.

> Our laws are not constraints or barriers to operational effectiveness as they are sometimes perceived. Rather, they are the guardians of valuable principles and enablers assisting agencies to perform their functions.[36]

Administrative convenience is not an acceptable justification for the removal of necessary safeguards, nor is it sufficient evidence that those safeguards are unnecessary. EFA recommends that

Recommendation: Any claim of administrative burden should be supported by specific, clear evidence of the magnitude and scope of the claimed burden.

EFA supports the recommendation of the Richardson Review that oversight bodies' attention should be drawn to the use of new powers, or the use of powers in novel or unique circumstances:

> For example, the use of a particular power may benefit from additional scrutiny when it is first conferred on an agency, because the agency may still be developing their systems, processes and expertise. In such a situation, an oversight body would benefit from being alerted to every use of that power. However, the need for additional scrutiny may decline over time, as the agency develops systems and processes that are shown to appropriately safeguard the use of the power.[37]

Recommendation: Oversight bodies' attention should be drawn to any use of new powers, or the use of powers in novel or unique circumstances.

---

[34] Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (n 5) [6.58].
[35] 'Witness K Lawyer Bernard Collaery's Appeal against Secret Trial Upheld', *ABC News* (online, 6 October 2021) <https://www.abc.net.au/news/2021-10-06/witness-k-lawyer-bernard-collaery-has-win-in-bid-for-open-trial/100517818>.
[36] Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (n 5) [3.15].
[37] Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (n 24) [40.136].

Power that can't be safely used should be removed

EFA recommends that before powers are granted, we must grapple with the level of abuse that we will accept before those powers are deemed unsafe and must be removed. By wrestling with this difficult calculus, we will be forced to reckon with the challenging tensions of extraordinary surveillance powers in a liberal democracy.

If an individual is found guilty of drink-driving, their licence to drive is revoked, if only temporarily. This functions partly as a harm reduction measure: it reduces the danger to others in the community pending a behaviour change by the individual concerned.

EFA accepts that mistakes happen, but in other contexts we do not accept that an infinite number of mistakes—and the associated harms—should be accepted before power to harm is removed. Yet in the numerous examples cited above of widespread, systemic failure, the community seems to be expected to accept that the harm must continue until compliance improves.

EFA does not accept this as a reasonable expectation. If agencies cannot use the extraordinary powers they have been granted safely, they must be removed.

Fail Safe

EFA recommends that for each power granted, we should set a safety threshold. A rate of mistakes, or deliberate abuse, that moves above this threshold indicates that Parliament has misunderstood the situation and failed to properly design safeguards that protect Australia's values and way of life.

While Parliament reconsiders the design of the safeguards, the regime should 'fail safe' and the dangerous power that has been granted should be automatically removed. The power can be reinstated after Parliament reconsiders the situation, and the ability of agencies to safely use the powers they have been granted in service of the community.

This fail safe should be agency wide, rather than based on the notion of individual 'bad apples'[38]. As the cases above illustrate, mistakes are caused by poorly designed systems more often than they are by individual misdeeds.

These well-documented past failures should inform the design of safeguards and oversight in the new framework. We should seek to avoid a repeat of these failures, rather than continue to pretend that these failures are somehow unavoidable and unforeseeable. The previous lack of foresight has been more due to a lack of imagination, and a failure to heed warnings from organisations such as EFA. Parliament should strive not to repeat these mistakes yet again.

[38] We note that the meaning of the idiom is to warn of how an individual bad apple will cause an entire barrel of otherwise good apples to be spoiled. The detection of a single bad apple does not exonerate the rest of the barrel as being acceptable; it does quite the opposite.

Recommendation: Safety thresholds should be set for all powers before they are granted. If mistakes or deliberate abuse rises about this threshold, the powers should be automatically revoked for all agencies implicated in the mistakes or abuse.

Notification of unlawful access

EFA does not believe any of the people whose data was unlawfully accessed by agencies[39] have been informed that their data was so accessed. This curtails their ability both to protect themselves from further harms that may result, based on their own individual assessment of the risks they may face, and their ability to seek redress for the harm they have suffered.

Electronic surveillance is highly invasive. The risks to individual privacy are substantial, and the powers granted to agencies are extraordinary; they are reserved for use only for very serious matters. Mistakes should therefore be taken just as seriously, and those affected by agency mistakes informed so that they can decide what action, if any, should be taken.

It is unreasonable for agencies to presume that they know the individual circumstances of those they have unlawfully surveilled and can accurately assess the harm that may have been caused. Individuals should, therefore, at least be notified when unlawful access has occurred.

Recommendation: When unlawful surveillance or data access occurs, the person(s) affected should be notified and informed of what surveillance was performed and what data was unlawfully accessed, and by which agency.

Redress for harm

Judicial review is expensive and time consuming. As the Richardson Review noted:

> Resort to the Federal Court or High Court is simply beyond the reach of most people and should not be considered an accessible or realistic review option.[40]

Electronic surveillance powers are extraordinary. Abuse of these powers must be treated with the seriousness it deserves. EFA submits that individuals are currently unable to seek redress for harms to privacy they have suffered partly because they are not notified that their information has been unlawfully accessed.[41]

Rather than requiring affected individuals to seek redress through the courts, consideration should be given to setting up a statutory compensation scheme similar to the Compensation for Detriment caused by Defective Administration scheme.[42]

---

[39] Duckett (n 29).
[40] Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (2019) vol 4 [44.93].
[41] We note that a theft that has not yet been detected by the victim is still treated as a crime.
[42] 'CDDA Scheme | Department of Finance' <https://www.finance.gov.au/cdda-scheme>.

Recommendation: Set up a compensation scheme for persons subject to unlawful surveillance with statutory payment amounts aligned to the seriousness of the harm caused.

Who should access information?

EFA submits that the Richardson Review comprehensively dealt with the issue of which agencies should be granted extraordinary surveillance powers and its recommendations should be heeded.[43] The current level of access to information and data is too broad and should be tightly controlled. We should not see a repeat of organisations such as local councils, racing agencies, and Australia Post accessing telecommunications data under the data retention regime.[44]

At all times the foundational principles outlined above should guide decisions about the proportionality, necessity, and propriety of granting extraordinary powers to covertly access Australians' private information.

EFA further endorses the recommendation of the Australian Law Reform Commission (ALRC) to introduce a single, consistent, national prohibition on the unauthorised use of surveillance devices, to replace inconsistent protections under state and territory laws.[45]

Collection and Access

EFA notes that the discussion paper focuses on the question of *access* to information but does not deal with the question of *collection*. Collection and access may be separate in time, and involve different parties. Both collection and access must each be carefully dealt with.

Recommendation: Collection of information must be addressed separately from use of information.

As discussed above, intelligence is not collected in order to establish a library. Undirected collection of information that is not linked to a defined and specific primary purpose should be prohibited. Only the minimal amount of information proportionate and necessary to fulfil that primary purpose should be collected or accessed, and only by those parties with a clear and genuine need for access to that information. Once the primary purpose has been fulfilled, the information should be destroyed.

---

[43] See Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (n 17) [27.23]-[27.61].
[44] Harriet Alexander, 'Councils Pry into Residents' Metadata to Chase down Fines', *The Sydney Morning Herald* (14 November 2018) <https://www.smh.com.au/business/consumer-affairs/councils-pry-into-residents-metadata-to-chase-down-fines-20181114-p50fxr.html>.
[45] *Serious Invasions of Privacy in the Digital Era* (No 123, Australian Law Reform Commission, 3 September 2014) <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/> ('*ALRC Report 123*') Recommendation 14-1.

EFA strongly objects to the use of intrusive surveillance powers to collect information that is then used for other than the primary purpose.

Recommendation: Information should only be collected using covert surveillance powers in connection with a defined and specific primary purpose, and once that purpose has been fulfilled, the information collected should be destroyed.

Recommendation: Information should only be accessed in connection with the same defined and specific primary purpose for which it was collected.

Comparing Australia to other democratic nations

Australia's most extreme deviations from democratic norms have simply been omitted from the discussion paper's tables of "key provisions" (Attachment A) and comparisons with other five-eyes countries (Attachment B). This makes Australia appear to be much less of an outlier than it actually is.

For Australian technologists, some of the most frightening provisions of Australian surveillance law are the sections that permit ASIO, AFP or Australian Crime Commission officers to force a "person with knowledge of computer systems" to do "acts or things" or be punished with years of imprisonment. For example, the ASIO Act, Subdivision J—Assistance relating to access to data, states

> **34AAD Person with knowledge of a computer or a data storage device to assist access to data**
>
> (1) The Director-General may request the Attorney-General to make an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the Organisation to do one or more of the following:

There then follows a list of data access, duplication, or conversion actions, with no restriction on how long the person can be required to work for in order to achieve them.

This is simply not mentioned in the Discussion Paper, not even in the "key provisions" table (pp.83-4). The AFP and ASIS have similar powers under related legislation, though their orders have some judicial oversight.

The table of comparisons with other Five Eyes countries also omits other details that reflect unfavourably on Australian rules. For example, it does not mention that the UK's Technical Capability Notices are constrained by much stronger judicial oversight than Australia's.

Overall, the Discussion Paper, and the discourse around this topic generally, underplays the serious risks to Australian individuals of an excessively invasive surveillance regime.

What information should be accessed?

As discussed above, only the minimum amount of information necessary and proportionate with fulfilling the primary purpose of collection should be accessed.

EFA recognises the challenge of technological change outpacing legislation. EFA recommends that the legislation be principles based and technology-neutral, rather than attempt to create an exhaustive list of technologies and circumstances covered by the Act. A human rights-based approach should be used to account for emerging technologies, as recommended in the Human Rights Commission's Human Rights and Technology report.[46]

Recommendation: A human rights-based approach should be used to account for emerging technologies.

What is a communication?

EFS submits that a broad and inclusive definition of communication, rather than an exhaustive list of specific forms of communication, would be preferable as a baseline. A communication could be simply defined as "any exchange or record of information, made in any form, between two or more locations or entities".

Where specific nuance is required in particular circumstances, clarifications of what is and is not a communication could be included where absolutely necessary. The goal should be to provide legislative clarity and certainty in ambiguous circumstances, rather than to attempt to account for every future eventuality as "[a]ny attempt to exhaustively define what is, or is not, a communication would almost certainly become obsolete within a short period of time."[47] A backstop of principles-based legislation will provide the most flexible mechanism to account for future technologies and unforeseen circumstances.

Content vs. non-content

EFA submits that the distinction between content and non-content information is no longer meaningful and should be abolished in favour of an assessment of the invasiveness of the surveillance. This will avoid the current situation where forms of surveillance that are disproportionately invasive are permitted by using a lower authorisation threshold than would otherwise be required.[48]

Recommendation: There should be no distinction made between content and non-content information.

---

[46] Sophie Farthing et al, *Human Rights and Technology: Final Report* (Australian Human Rights Commission, 2021) <https://tech.humanrights.gov.au/downloads> ('*Human Rights and Technology*').
[47] Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (n 17) [29.17].
[48] *Ben Grubb and Telstra Corporation Limited* [2015] AICmr 35.

Invasive surveillance undermines security

Throughout the drafting of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, many contributors expressed concern that Technical Capability Notices could force changes that jeopardised the security and privacy of other users of the same system. After much discussion, some very vague, weak and ambiguous protections were incorporated into the bill. The discussion paper greatly overstates these protections, claiming

> These requests and notices may not introduce a systemic weakness or vulnerability *to the carriage service* – section 317ZG [our emphasis]

This is entirely different from the protections actually given in section 317ZG, which states

> (1) A technical assistance request, technical assistance notice or technical capability notice must not have the effect of:
>
> (a) requesting or requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, *into a form of electronic protection*; or
>
> (b) preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, *in a form of electronic protection* [our emphasis].

There is nothing prohibiting the forced introduction of a systemic weakness into the carriage service (for example, access to its database), as long as the weakness is not introduced into a form of electronic protection itself.

This misrepresentation is part of a pattern of downplaying the security risks associated with invasive surveillance. Risks to individual (or corporate) security are a consequence of the forced account-takeover provisions of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* also, but were also not adequately considered at the time and are not identified in the Discussion Paper.

We cannot build a surveillance framework that adequately balances the risks to individual security against 'national security' if the risks to individual security are not adequately identified and considered.

How should information be accessed?

EFA recommends that all collection and access to surveillance information should require a judicially issued warrant. EFA endorses the views of Dr Keiran Hardy and Professor George Williams AO as submitted to the Richardson Review that "given the close relationship between ministers and their respective agencies, there is a question as to whether responsible ministers

'will bring a sceptical, critical approach to the authorisation of intelligence gathering powers'."[49]

When should information be accessed?

EFA concurs with the recommendations of the Richardson Review that covert surveillance powers should only be available for the most serious matters. EFA endorses the view that the powers should not be available for investigation of any offence punishable by less than five years imprisonment.[50]

As discussed above, such powers should only be permitted after an assessment that use of the powers is both necessary and proportional, and an appropriate judicial warrant has been issued.

EFA submits that the discussion of standard warranted access[51], emergency access[52], joint intelligence activities[53], and when direct effects against Australians are likely to result[54] have been canvassed thoroughly in the Review and are worth considering in detail.

Industry and Government

EFA submits that private industry should not be coerced or compelled to become a quasi-secret police operating at arms' length from the government. Totalitarianism is anathema to the notion of Australia as a liberal democracy, and private enterprise should not be consumed to become a mere extension of State power.

An important role of governments is to implement robust regulations that protect people from abusive practises by others, including corporations. Many democracies have strong privacy laws that empower citizens by limiting the extent of data collection, and the uses to which that data may be put. The desires of agencies to have easy access to surveillance data should not take precedence over Australians' right to privacy. Government failure to protect Australians from the exploitative practises of surveillance capitalism should not be used as a justification for government surveillance. Government should protect Australians from the likes of Facebook, not attempt to become more like Facebook.

As discussed above, if the government believes participation of industry to conduct surveillance is in the national interest, let it make its case on each occasion. If the intelligence activity has an ethical purpose, its proposer should be confident enough of the legality and propriety of the

---

[49] Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (n 17) [18.92].
[50] Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (n 1) Recommendation 87.
[51] Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (n 17) chs 18–20.
[52] Ibid ch 21.
[53] Ibid ch 22.
[54] Ibid ch 23.

activity to provide industry with the ability to make an informed choice whether or not to participate.

In a healthy liberal democracy, the fact that industry may sometimes choose not to become the covert surveillance arm of the government should be expected. It should not undue alarm or frustration on the part of agencies that have failed to make a compelling case for invasive surveillance.

Interaction with other legislation and reviews

EFA recommends engaging closely with the details of the Richardson Review.

EFA further recommends that the development of the electronic surveillance legislation should closely coordinate with the review of the Privacy Act currently being conducted.[55]

EFA also notes that the Data Availability and Transparency Bill (DAT Bill)[56] may have profound implications for access to data collected using covert surveillance powers. EFA strongly rejects any suggestion that information collected using covert surveillance powers should be made available using any alternate pathways proposed by the DAT Bill.

[55] 'Review of the Privacy Act 1988', *Attorney-General's Department* (5 November 2020) <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>.
[56] *Data Availability and Transparency Bill 2020*.