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

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600

8 November 2022

By email

Dear Secretary,

RE: Inquiry into the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

EFA welcomes the opportunity to comment on proposed Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (the Bill).

EFA's submission is contained in the following pages. Due to the limited time provided for submissions, we have kept our submission brief.

About EFA

Established in January 1994, EFA is a national, membership-based, not-for-profit organisation that promotes and protects human rights in a digital context.

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
Board Member
Electronic Frontiers Australia

Introduction

EFA welcomes government action on privacy as a long overdue first step in updating Australia's privacy regulations to be fit-for-purpose in a modern, connected nation. Australians have long demanded, asked, and even begged for their government to value their privacy more. We congratulate the government for deciding to listen to them.

We look forward to the long-anticipated major updates to the Privacy Act. We expect that our recommendations to numerous previous consultations and inquiries will be adopted. There is now voluminous, concrete proof of what happens when such recommendations are not adopted.

Summary of Recommendations

1. Grant the OAIC the power to independently levy fines for breaches of privacy law, with such actions subject to standard administrative review processes by the AAT and the courts.
2. Dramatically increase the funding provided to the OAIC so that it can effectively perform its regulatory function.
3. Enact a tort of serious breach of privacy as recommended by the ALRC in 2014.
4. Repeal laws that require over-collection and retention of personal information.
5. Consolidate existing legislation and clarify legal obligations to collect and retain personal information.
6. Legislate to prioritise privacy-preserving mechanisms over surveillance.
7. The eSafety Commissioner should not be made an alternative complaint body.
8. Close the Australian Link loophole as proposed in the Bill.

Changing the incentives

EFA notes that the Bill has focused on increasing fines for behaviour that is already illegal. While EFA agrees that the incentives need to be altered so that there is a systemic change in behaviour to prioritise privacy over surveillance, we are concerned that the measures proposed will be largely symbolic and ineffective.

Regulators that cannot regulate

Enforcement of existing privacy law relies on regulators that are willing and able to enforce the law, and do nothing to compensate individuals for the harm they suffer when a data breach occurs. We see nothing in the Bill that alters this arrangement.

The primary regulator—the Office of the Australian Information Commissioner—is already underfunded, overworked, and unable to meet its existing obligations. It is difficult to see how adding additional responsibility to this same agency will somehow allow them to successfully levy the proposed fines on those who failed to comply with privacy legislation.

The OAIC must currently ask the Federal Court to levy these fines, and the proposed Bill does not change this situation.

Recommendation: Grant the OAIC the power to independently levy fines for breaches of privacy law, with such actions subject to standard administrative review processes by the AAT and the courts.

To be effective, regulators must be adequately resourced to fulfil their responsibilities, and staffed with people willing and able to protect the privacy of all Australians.

Recommendation: Dramatically increase the funding provided to the OAIC so that it can effectively perform its regulatory function.

Tort of serious breach of privacy

EFA would prefer to see power given to all Australians to seek redress for the harm they've suffered, such as through a tort of serious breach of privacy as recommended by the Australian Law Reform Commission 8 years ago, in 2014.[1] History shows us that

[1] 'A Statutory Cause of Action for Serious Invasion of Privacy', *ALRC* <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-dp-80/4-a-new-tort-in-a-new-commonwealth-act/summary-138/>.

relying solely on government regulators means many Australians are ignored, dismissed, and abandoned.

A private right of action such as a tort would also complement action by regulators. Regulators cannot deal with every single breach of the law; there are simply too many. They generally choose, given their limited resources, to focus on systemic issues and significant breaches. While this helps to deter the most egregious behaviour, it provides little comfort to those whose suffering is deemed too insignificant to attract regulator attention and effort.

A tort would allow individuals to seek redress from harm without waiting for a regulator to act. Individuals could also band together as a class to seek collective redress for collective harm. Fines levied by a regulator do nothing to assist individuals to deal with the fallout after a data breach, even assuming they are eventually levied.[2]

A tort would also act as a systemic counterbalance to poor privacy practices by organisations. If complainants were awarded a mere $500 each for an individual breach of their privacy, this would be equivalent to a fine of $5 billion for a data breach at the scale of the Optus breach.[3]

Recommendation: Enact a tort of serious breach of privacy as recommended by the ALRC in 2014.

Make privacy the priority

Privacy, once lost, cannot easily be regained. It is relatively trivial to cancel a credit card and get a new one. It is far more difficult to obtain new fingerprints. This reality must be taken into account when drafting legislation.

The risk of a loss of privacy is not the same for all people. For some, publication of their home address may not alter their risk very much. For others, such as those fleeing domestic abuse, publication of their home address could be life-threatening. This, too, should be front of mind when drafting legislation.

---

[2] 'Optus Customers, Not the Company, Are the Real Victims of Massive Data Breach', *The Guardian* (online, 28 September 2022) <https://www.theguardian.com/commentisfree/2022/sep/28/optus-customers-not-the-company-are-the-real-victims-of-massive-data-breach>.

[3] Josh Taylor, 'Optus Data Breach: Everything We Know so Far about What Happened', *The Guardian* (online, 28 September 2022) <https://www.theguardian.com/business/2022/sep/29/optus-data-breach-everything-we-know-so-far-about-what-happened> ('Optus Data Breach').

Surveillance is not safety

Successive governments have legislated in favour of enforcement agencies' obsession with surveillance. The over-collection and retention of personal information is a direct contributor to the amount of data that is available to be obtained in a data breach. It has created a substantial incentive for bad actors to obtain this information.

These massive honeypots of data have placed all Australians at greater risk. Beyond the individual risks, Australians are also now at greater collective risk as foreign adversaries seek to access and exploit this information. The obsession with surveillance has created a national security risk.

Recommendation: Repeal laws that require over-collection and retention of personal information.

In the recent data breaches, companies have made various claims that they are required to collect and retain information about customers. It can be difficult to tell if these claims are accurate, as the law is often unclear.

Individuals and organisations alike would benefit from the law being clear. There should be no ambiguity about what personal information the law says must be collected and how long it must be kept for.

Recommendation: Consolidate existing legislation and clarify legal obligations to collect and retain personal information.

Where existing laws require collection of personal data that is not absolutely necessary, those laws should be repealed.

The legal framework should be changed to prioritise the limited collection, storage, and use of personal information. The systemic incentives should be changed to favour privacy over surveillance.

Recommendation: Legislate to prioritise privacy-preserving mechanisms over surveillance.

The eSafety Commissioner

EFA is concerned that the Bill proposes to add the eSafety Commissioner to the list of alternative complaints bodies. EFA considers that the eSafety Commissioner has already been granted far too much power with insufficient oversight. The explanatory memorandum does not adequately explain why the eSafety Commissioner should be an alternative complaint body about privacy complaints. It is unclear how the eSafety

Commissioner would have assisted with any of the recent data breaches. It is also unclear how the eSafety Commissioner was prevented from assisting by virtue of not being listed as an alternative complaint body.

Recommendation: The eSafety Commissioner should not be made an alternative complaint body.

Australian Link Loophole

EFA welcomes the closure of the 'Australian Link' loophole in existing legislation proposed by the Bill that permits organisations to avoid Australian privacy law by collecting data on Australians from sources not based in Australia. It is right and proper that Australians should expect data about them to be kept safe no matter how it came to be in the possession of an organisation.

Recommendation: Close the Australian Link loophole as proposed in the Bill.