SalingerPrivacy

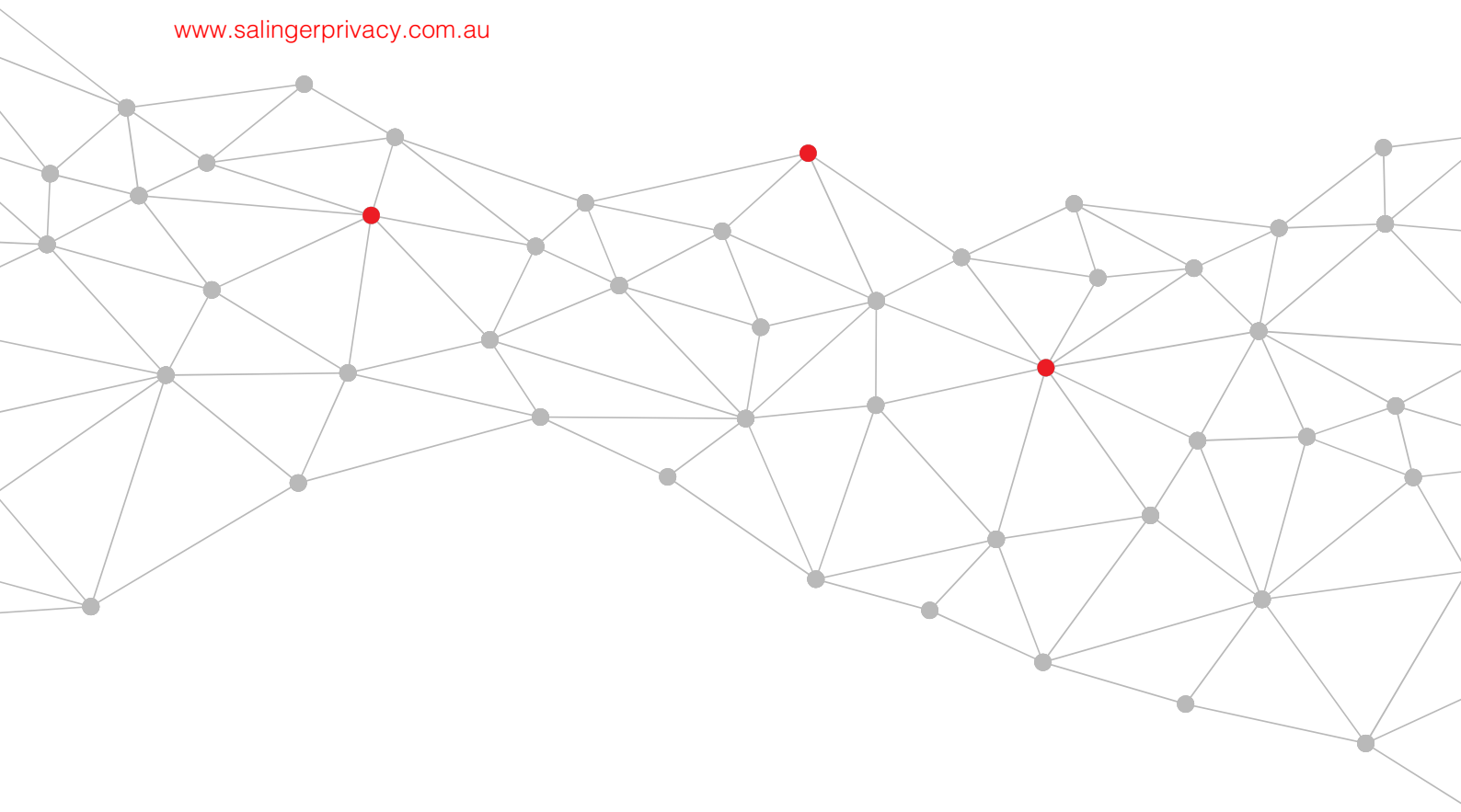
We know privacy inside and out.

Submission in relation to the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

Senate Legal and Constitutional Affairs Committee

7 November 2022

Salinger Consulting Pty Ltd
ABN 84 110 386 537
PO Box 1250, Manly NSW 1655
www.salingerprivacy.com.au



Covering letter

7 November 2022

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

By email: legcon.sen@aph.gov.au

Dear Senators,

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

Thank you for the opportunity to make submissions in relation to the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022.

Please find our submission attached.

We have no objection to the publication of this submission, and no redactions are required prior to publication.

Please do not hesitate to contact me if you would like clarification of any of the comments made in this submission.

Yours sincerely,

Anna Johnston
Principal | Salinger Privacy

Submission

This submission is made in relation to the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (the Bill).

The Bill would amend three Commonwealth Acts, including the *Privacy Act 1988* (Cth) (the Privacy Act), to increase penalties for serious or repeated interferences with privacy, enhance the Australian Information Commissioner's enforcement powers, and provide the Commissioner (the OAIC) and the Australian Communications and Media Authority with greater information sharing powers.

In particular, the maximum civil penalty for a serious or repeated breach by a body corporate will increase from the current maximum of $2.22M to whichever is the greater out of:

- $50 million,
- 30% of turnover,
- or three times the benefit obtained from the breach.

For individuals (e.g. sole traders), partnerships and other unincorporated entities, the penalty will increase from the current maximum of $440,000 to $2.5 million.

I write in support of the Bill, but also to make suggestions for improvement.

No reason not to proceed

Although I make suggestions for improvements to the penalties regime below, I wish to stress that even if none of the suggestions below are adopted, the Bill should be passed as soon as possible.

As recent data breach events have demonstrated, Australians' privacy is not being appropriately respected or protected by corporations, which leaves individuals at risk of various types of harm. It is essential that the regulatory regime in Australia makes the cost of non-compliance with the Privacy Act more expensive than the cost of compliance. Fines under the Privacy Act should not be seen as simply a cost of doing business.

Increasing the penalties available under the Privacy Act will send a strong signal to businesses and other entities around Australia that they must take their legal obligation seriously. I therefore support the Bill.

The penalty regime needs to be pragmatic and fair, to be effective

I do however caution that as the Bill stands, it will not impact on non-compliant conduct by the vast majority of organisations.

The Bill does not fix two of the significant problems with the current enforcement regime:

- Fines are only for 'serious' or 'repeat' conduct, and
- The OAIC cannot levy fines directly.

(There is a third significant problem with the current regime, which is the chronic under-funding of the OAIC, but this is not a problem which can be solved through legislation.)

Business from banks to dentists, from real estate agents to app developers, should be motivated to implement good practices due to concern about the likely consequences of not complying with the Privacy Act. So long as the enforcement regime is only for 'serious' or 'repeat' conduct, and fines can only be levied by the Federal Court, many organisations will continue to ignore their obligations in the hope that the regulator is too overwhelmed to bother taking them to court, and that they could easily defend most conduct as either not serious or not repeat anyway.

We suggest that the perceived *likelihood* of being penalised is a more powerful motivator than simply the amount of the maximum penalty.

Until this limitation is addressed, it will not matter that the top fine is $50M or more; most organisations will not imagine themselves ever being subject to such a penalty, and thus will continue their information handling practices without improvement.

Across all sectors of the economy, all sizes of organisations, and throughout the information life cycle, privacy obligations are currently being ignored. From giving patients access to their medical records, to implementing appropriate data security for tenancy information, to designing apps to avoid over-collection of personal information, there is much room for improvement.

The prospect of facing smaller but directly levied fines from the OAIC, quickly and without the OAIC being tied in knots before it could levy such fines, would provide an incentive for organisations of all sizes to ensure that they comply with their privacy obligations.

We suggest that a much more effective, fair and scalable penalty regime would be a tiered approach, such as:

- The OAIC should be able to levy fixed fines directly for *any* interference with privacy:
    - Individuals and unincorporated entities: $25,000
    - Incorporated entities with an annual turnover of less than $3M: $50,000
    - Incorporated entities with an annual turnover of $3M+: $100,000; *and*

- The above fines could be doubled if any aggravating factors are present, such as if:
    - The entity failed to take its privacy obligations seriously
    - The entity demonstrated a blatant disregard for its privacy obligations (i.e. either deliberate or reckless conduct)[1]
    - The interference with privacy did, or is likely to, result in serious harm to one or more individuals; *and*
- The OAIC to be able to approach the Federal Court in cases of 'serious' or 'repeat' interferences with privacy, with maximum penalties as per those proposed in the Bill.

More significant reform work remains

I also caution that tinkering with penalties and enforcement powers alone will not improve the overall level of privacy protection for Australians.

The successful passing of this Bill should not provide an excuse for the Government to lose momentum in terms of the wider review of the Privacy Act. Our previous submissions on the review of the Privacy Act demonstrate the many areas in which reform is urgently needed.[2]

Bigger fines for breaching the rules will be an improvement. However we also need to strengthen and clarify the rules themselves, and empower and appropriately resource the umpire.

[1] For example, this could be if an entity proceeded with the conduct, which constituted the interference with privacy, after advice not to; or the entity failed to take reasonable steps to correct and improve its privacy practices following earlier findings, determinations, advice or warnings from the OAIC, internal or external auditors

[2] Please see https://www.salingerprivacy.com.au/privacy-reforms/ for links to our previous submissions and summaries of our views.

About the author

This submission was prepared by Anna Johnston, Principal, Salinger Privacy.

Anna has served as:

- Deputy Privacy Commissioner of NSW
- Chair of the Australian Privacy Foundation, and member of its International Committee
- a founding member and Board Member of the International Association of Privacy Professionals (IAPP), Australia & New Zealand
- a member of the Advisory Board for the EU's STAR project to develop training on behalf of European Data Protection Authorities
- a Visiting Scholar at the Research Group on Law, Science, Technology and Society of the Faculty of Law and Criminology of the Vrije Universiteit Brussel
- a Member of the Asian Privacy Scholars Network
- a member of the Australian Law Reform Commission's Advisory Committee for the Inquiry into Serious Invasions of Privacy, and expert advisory group on health privacy, and
- an editorial board member of both the Privacy Law Bulletin and the Privacy Law & Policy Reporter.

Anna has been called upon to provide expert testimony to the European Commission as well as various Parliamentary inquiries and the Productivity Commission, spoken at numerous conferences, and is regularly asked to comment on privacy issues in the media. In 2018 she was recognised as an industry leader by the IAPP with the global designation of Fellow of Information Privacy (FIP).

In 2022, Anna was honoured for her 'exceptional leadership, knowledge and creativity in privacy' with the IAPP Vanguard Award, one of five privacy professionals recognised globally whose pioneering work is helping to shape the future of privacy and data protection. In particular, the award recognised Anna's passionate pursuit of law reform to improve protection against digital harms.

Anna holds a first class honours degree in Law, a Masters of Public Policy with honours, a Graduate Certificate in Management, a Graduate Diploma of Legal Practice, and a Bachelor of Arts. She was admitted as a Solicitor of the Supreme Court of NSW in 1996. She is a Certified Information Privacy Professional, Europe (CIPP/E), and a Certified Information Privacy Manager (CIPM).

About Salinger Privacy

Established in 2004, Salinger Privacy offers privacy consulting services, specialist resources and training.

Our clients come from government, the non-profit sector and businesses across Australia. No matter what sector you are in, we believe that privacy protection is essential for your reputation. In everything we do, we aim to demystify privacy law, and offer pragmatic solutions – to help you ensure regulatory compliance, and maintain the trust of your customers.

Salinger Privacy offers specialist consulting services on privacy and data governance matters, including Privacy Impact Assessments and privacy audits, and the development of privacy-related policies and procedures. Salinger Privacy also offers a range of privacy guidance publications, eLearning and face-to-face compliance training options, and Privacy Tools such as templates and checklists.

Qualifications

The comments in this submission do not constitute legal advice, and should not be construed or relied upon as legal advice by any party. Legal professional privilege does not apply to this submission.

SalingerPrivacy

We know privacy inside and out.

Salinger Consulting Pty Ltd

ABN 84 110 386 537

PO Box 1250, Manly NSW 1655

www.salingerprivacy.com.au