Australian Computer Society Inc. (ACT)
ARBN 160 325 931

National Secretariat
Tower One, 100 Barangaroo Avenue, Sydney NSW 2000
PO Box Q534, Queen Victoria Building, Sydney NSW 1230
T +61 2 9299 3666 | F +61 2 9299 3997
E info@acs.org.au | W www.acs.org.au

To the Senate Legal and Constitutional Affairs Committee

ACS response

Privacy Legislation Amendment (ENFORCEMENT and Other Measures) Bill 2022

1 November 2022

Dear Sir or Madam

Thank you for the opportunity to contribute to this critical discussion.

The Australian Computer Society (ACS) is the peak professional association for Australia's information and communications technology sector. We represent over 35,000 members working in all sectors and across the nation. Our members work in industry, education, government and the community, delivering the digital services that drive the nation and provide the high-skilled jobs of today and tomorrow. ACS works to grow the technology sector while making sure IT professionals act ethically, responsibly, and in keeping with the best interests of not only their employers, but the wider community.

In response to the proposed Bill, ACS is broadly in support of increased penalties for companies that fail to comply with the Privacy Act. These changes will serve to highlight the importance of cyber security and hopefully reduce the number of cyber incidents that have impacted millions of people in the last few months.

We are also strongly in support of increased transparency and the increased ability of the OAIC to investigate breaches and communicate the results of those breaches to relevant enforcement agencies.

We would urge that this be backed up with increased public funding of the OAIC to ensure that proper investigation and enforcement is practically feasible.

Our support for the Bill does have some caveats. In order to protect Australians, there should be formal privacy frameworks for businesses of every size.

Instead of enforcing minimum requirements (which would be burden for both government and business), we would suggest investigating a voluntary certification scheme that offers limited safe

harbour under the Privacy Act as well as a standardised model of assurance for partners, insurers, procurement officers and customers.

The case for business cyber security trust marks

We agree that penalties for privacy failures should be higher, but suggest that courts should be allowed to consider mitigating factors such as the level and extent of preventative action that an organisation's governing body has put in place to prevent cyber security failures.

Such action might include the use of standards-based trust marks based on recognised cybersecurity frameworks. ACS would be happy to help with the development and implementation of such trust marks.

These would be analogous, for example, to vehicle roadworthiness checks ('pink slips'), where a registered and recognised assessor evaluates a company's systems against a framework and provides certification that the company is undertaking reasonable steps to secure customer data.

Security incidents may occur even in well-prepared organisations

In 2016, the United States National Security Agency was hacked.

A group called The Shadow Brokers managed to infiltrate the organisation and steal some of the NSA's most advanced electronic spying tools and zero-day exploits. That malware was quickly turned to criminal purposes, and some of that criminal malware still plagues the internet today.

The fact that even the NSA was breached is evidence of a simple fact: there is no system in the world that is 100% secure. Humans are fallible, and a malicious insider or simple human error can bring down the most stringent of cyber security regimes.

As noted in Australian Securities and Investments Commission v RI Advice Group Pty, "It is not possible to reduce cybersecurity risk to zero, but it is possible to materially reduce cybersecurity risk through adequate cybersecurity documentation and controls to an acceptable level."[1]

[1] https://download.asic.gov.au/media/zhodijpp/22-104mr-2022-fca-496.pdf

Australia has, in recent months, seen a number of enormous data breaches, with the identities of millions of Australian citizens now for sale in the dark reaches of the internet. Some of the notable breaches include Optus[2], Medibank[3], Vinomofo[4] and Australian Clinical Labs[5].

In response to those breaches there have been calls for harsh punitive penalties for companies that fail in their duty of care to their customers[6], and the Privacy Legislation Amendment (ENFORCEMENT and Other Measures) Bill 2022 is a clear manifestation of that.

As noted above, in principle ACS has no objection to harsh penalties for organisations that fail to do everything they can to protect their customers' data – especially for those companies that make the cynical calculation that the cost of compliance with cyber security principles exceeds the risk-adjusted liability of a breach.

However, there is a danger that companies that are doing all the right things still get compromised. We do not believe equal penalties should apply to those organisations.

Instead, we would argue for the development of a government-endorsed voluntary certification scheme that would provide assurances to courts, insurers, customers and partners that a company had undertaken reasonable steps to protect customer data and prevent breaches.

The cyber security pink slip

The specifics of any trust mark would likely require a negotiation between government and business (and, likely, providers of cyber security insurance services) to find the right balance between assessment costs and effectiveness.

There are many existing frameworks that could be applied: NIST[7], ISO 27001/27002[8], SOC 2[9], GDPR[10], the FAIR Cyber Risk Framework[11] and of course Australia's own Essential 8[12] and ACSC Top 35[13] among many others.

[2] https://ia.acs.org.au/article/2022/optus-confirms-2-1m-customer-id-numbers-stolen.html
[3] https://ia.acs.org.au/article/2022/medibank-concedes-all-customers-affected-by-breach.html
[4] https://ia.acs.org.au/article/2022/vinomofo-customer-details-for-sale-following-breach.html
[5] https://www.abc.net.au/news/2022-10-27/acl-cyber-attack-pathology-lab-health-data/101584072
[6] https://ia.acs.org.au/article/2022/government-proposes--50m-data-breach-fines.html
[7] https://www.nist.gov/cyberframework
[8] https://www.iso.org/isoiec-27001-information-security.html
[9] https://www.imperva.com/learn/data-security/soc-2-compliance/
[10] https://gdpr-info.eu/
[11] https://www.fairinstitute.org/
[12] https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
[13] https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents

While it would be easy to just pick one (Essential 8, for example), we do believe that it is worth consulting with businesses and cyber security experts to determine their suitability. Essential 8, for instance, is a relatively low bar, even at maturity level 3 – it only covers the *essentials*, as the name implies.

ACS would be happy to engage with industry and government on the creation of an effective trust mark. We believe that a final security audit should include elements such as:

- penetration testing outcomes
- certification of the cyber security professionals working in the organisation
- process audits
- data requirements and governance analysis
- governance models.

Once again, the burden of compliance should not be so great at to discourage companies from even trying, but not so minimal as to be a box-ticking formality with no real value.

However, with a balanced approach we believe that the Australian government can help Australian businesses achieve far better cyber security outcomes, leading to a safer environment for all Australian citizens.

Other legislative considerations

A tiered penalty regime and clear modelling of penalties

There is a strong consensus among industry groups – and ACS joins in this as well – that there needs to be a tiered penalty regime and much clearer (and explicit) models for calculating penalties.

Tiering (based on revenue, staff and/or criticality of the business, for example) will provide better incentives for all businesses to implement cyber security. The current one-size-fits-all legislation over-punishes small companies and under-punishes large, distorting incentives for companies of all size.

Large companies will potentially see that the cost of compliance with cyber principles is greater than the liabilities of a breach, and decide that budget is better reserved for dealing with the fallout rather than ensuring no breach occurs. Small companies, the least able to afford complex cyber security, are conversely potentially completely destroyed by a breach.

Alongside tiering, we would also recommend significantly improving clarity about how penalties are modelled. The legislation currently leaves a great deal of leeway for interpretation, creating uncertainty about potential penalties for both enforcement agencies and organisations.

Modelling might be based on company revenue, number of breached personal information records, 'gap' analysis of cyber security spend or some combination of the above. Most importantly, it is made clear to businesses what their liabilities might be.

Strengthening Notifiable Data Breaches

The Privacy Amendment (Notifiable Data Breaches) Act 2017 was a positive move to ensure companies didn't just 'bury' cyber breaches and hope customers and government agencies would never find out.

However, the implementation of the scheme has been mixed. We have seen companies play fast and loose with the rules, stretching out "investigation" periods or using wilful interpretation of some of the unclear language to avoid acting in the spirit of the law (a recent example is Medlabs Pathology breach, which was not revealed until eight months after the event[14]). We recommend:

- reducing the Notifiable Data Breaches 'window' from 30 days to 15 days
- fiercely enforcing it, with additional penalties for companies that do not comply
- providing additional clarity on what "serious harm" is with respect to breaches
- likewise providing clarity on what constitutes a "suspected" breach.

Reviewing data retention laws

One of the key takeaways from the recent reported breaches is that the issue is as much what is kept behind within the organisation's walls as the quality of the wall itself.

Breached businesses have stored unnecessary customer information, including personal authentication data, and this has significantly exacerbated the problem. There is a significant difference in the cost of replacing a stolen credit card compared to the cost of replacing passports/driver's licences.

There is also a burden on the government agencies that issue these documents. Planning to replace stolen identity documents every time there is a breach is not sustainable.

We strongly recommend a major overhaul of current data retention laws, reviewing the collection and retention of personal identity documents by Australian businesses and in particular laws that require identity documents be held for compliance reasons.

The government can also look to token-based authentication models that require no personal data to be stored, and provide guidance on best-practice implementation of such schemes.

[14] https://ia.acs.org.au/article/2022/223-000-australians-in-medlab-pathology-breach.html

Whistleblower protections

Cyber security professionals currently have no clear whistleblower protections, which gives no outlet for reporting corporate malfeasance safely and privately. Existing whistleblower laws and mechanisms could readily be expanded to incorporate cyber security reporting.

Operational considerations

Using procurement to encourage cyber security uplift

In order to provide additional incentives to companies to implement cyber security principles, overall government procurement processes can also be modified to require private companies meet a minimum set of standards and disclose their level of compliance. This could be accomplished through the trust mark model proposed above, or at a minimum requiring that all tenders submit a comprehensive report on their cyber security practices.

Streamlining the reporting process

Current reporting lines for breaches are unclear to many organisations, with a variety of government organisations having partial jurisdiction (for example ASIC, ACSC, OAIC). Clear step-by-step process guidelines for businesses would be very useful to ensure that organisations that are the victims of breaches know exactly what they must report and to whom.

ACS would like to thank you for the opportunity to offer this submission. We would welcome the opportunity to address these and other issues in more detail.

If you would like to discuss any part of this response or simply seek further clarification or input, please feel free to contact myself by email at troy.steer@acs.org.au or by phone on 0417 173 740.

Yours sincerely

Troy Steer
Director of Corporate Affairs and Public Policy
Australian Computer Society