www.accan.org.au
info@accan.org.au
02 9288 4000

Submission

21 June 2022

National Security Action Plan Discussion Paper

Submission by the Australian Communications Consumer Action Network (ACCAN) to The Department of Home Affairs

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards communications services that are trusted, inclusive and available for all.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will represent the views of its broad and diverse membership base to policy makers, government and industry to get better outcomes for all communications consumers.

Contact

Samuel Kininmonth
Policy Officer

PO Box A1158
Sydney South NSW 1235
Email: info@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
Contact us through the National Relay Service

Contents

Introduction

The Australian Communications Consumer Action Network (ACCAN) welcomes the opportunity to respond to the Department of Home Affairs *National Security Action Plan Discussion Paper* (the Discussion Paper). As the leading voice for communications consumers in Australia, ACCAN has engaged with the ongoing Privacy Act Review,[1] [2] the introduction of the Consumer Data Right (CDR)[3] and the Digital Platforms Services Inquiry.[4] Our response to this consultation, along with the others, is informed by our research and consultation with the community.

Consumer confidence will be crucial to building Australia's digital economy. Data security and privacy are fundamental parts of building public trust. According to research, 94% of Australian consumers are concerned about data security, with "data breaches or hacks" topping the list for what worries people about their online safety.[5] While the Discussion Paper is more broadly concerned with data security and protecting information stored on digital systems and networks, this submission focuses more on personal data and privacy as the most pressing issue of concern for consumers and a crucial part of data security. While data security more broadly is important for businesses and governments to protect information such as strategic assets and commercial secrets, from a consumer perspective, the greatest risks concern protecting personal information from both external unauthorised access and misuse from data holders. As this submission explains, to foster public trust in data security regimes and support the emerging digital economy, the Federal Government must ensure that it provides adequate data protections for all consumers. Regulators must hold businesses and governments to account for those protections through compliance and penalty regimes. There needs to be a centralised resource that provides effective and accessible educational materials for consumers. These materials should outline steps that consumers can take to protect themselves as well as the expectations they should have from the entities that handle their data.

[1] ACCAN (2020) *Privacy Act Review Issues Paper consultation*. Available at: https://accan.org.au/accans-work/submissions/1827-privacy-act-review-issues-paper-consultation
[2] ACCAN (2022) *Privacy Act Review Issues Paper*. Available at: https://accan.org.au/accans-work/submissions/1969-privacy-act-review-issues-paper
[3] ACCAN (2022) *CDR Rules and Standards Design Paper*. Available at: https://accan.org.au/accans-work/submissions/1978-cdr-rules-and-standards-design-paper
[4] ACCAN (2022) *ACCC DPSI September Interim Report*. Available at: https://accan.org.au/accans-work/submissions/1977-accc-dpsi-september-interim-report
[5] CPRC (2020) *CPRC 2020 Data and Technology Consumer Survey*. Available at: https://cprc.org.au/cprc-2020-data-and-technology-consumer-survey/

ACCAN makes four key recommendations to empower and educate consumers about data security:

Recommendation 1: The Federal Government should further invest in the creation of high quality, accessible resources to provide consumers with personal data security skills and house those resources in a single location accompanied by a public awareness campaign.

Recommendation 2: The Federal Government should implement pro-consumer defaults regarding data collection and privacy by design to minimise the data at risk in the event of data breaches.

Recommendation 3: The Federal Government should introduce strong accountability measures such as those under consideration in the Privacy Act Review including higher penalties for breaching the Privacy Act, a Direct Right to Action and a Statutory Tort for Invasions of Privacy.

Recommendation 4: The Federal Government should run targeted public awareness campaigns that explain what security and privacy obligations apply to businesses and governments when they collect, store and use data. It should publicise the penalties for data security and privacy breaches and publicly report examples of the Government holding organisations to account over data breaches that have impacted consumers.

Responses to National Security Action Plan Discussion Paper

Given our expertise, ACCAN limits our response to the consultation questions regarding empowering and educating consumers and the broader community about data security.

14. Does the Australian Government currently have sufficient public information for consumers and citizens on data security best practice? How can we make that information more easily accessible, usable and understandable?

Question 14 in the Discussion Paper asks how data security best practice can be made more easily accessible, usable and understandable to consumers.

This question can be split into two important parts: consumer education to foster personal security habits, and public information around organisations' data security obligations and penalties for failing to protect data. Both elements are crucial to informing consumers about data security.

Regarding consumer education to foster personal security habits, the Discussion Paper lists four sources of existing published guidance for data security related issues:

- Australian Cyber Security Centre (ACSC).
- e-Safety Commissioner.
- Office of the Australian Information Commissioner.
- Office of the National Data Commissioner.

A brief inspection of the homepages of these four suggested sources of information shows that while the ACSC, e-Safety Commissioner and Office of the Australian Information Commissioner do provide tips for personal security habits, only the ACSC provides dedicated security education to the public. The e-Safety Commissioner's homepage is largely concerned with online abuse and the data security information is located deeper into the website. The Office of the Australian Information Commissioner has information about the Privacy Act and the Consumer Data Right but fewer resources on data security. The Office of the National Data Commissioner is largely concerned with public sector data and the prominent information on its homepage does not seem applicable to individual consumers.

The resources provided across these websites consist largely of tip sheets encouraging consumers to use stronger passwords, enable two-factor authentication, review privacy policies and settings and to avoid interacting with suspicious messages. There were some interactive resources worth noting

such as the ACSC's tips on how to spot a phishing email.[6] The e-Safety Commission also provided lesson plans for educators to teach children about security.[7] Explainer videos were also provided across some webpages. While the resources were often of sufficient quality it is not ideal that they are spread across multiple websites and not housed prominently in a central location. It would be favourable to invest in the creation of more data security education resources co-designed with the community, housed in a single location, and meaningfully communicated to the community. These resources should meet current accessibility guidelines and be available in a range of languages including plain English and Auslan. The ACSC or the e-Safety Commissioner could be well placed to provide this prominent, centralised resource.

> **Recommendation 1:** The Federal Government should further invest in the creation of high quality, accessible resources to provide consumers with personal data security skills and house those resources in a single location accompanied by a public awareness campaign.

It is also important to recognise that consumer education to encourage better security practices is only part of the required public information. While personal data security precautions are important, they do require consumers' time, effort and expertise. They rely on user judgement. As research has found, around nine in 10 security breaches can be attributable to human error.[8] Furthermore, there is usually a trade-off to enabling privacy settings, from limiting functionality to being excluded from a service altogether. For example, some government resources recommend consumers carefully read the terms and conditions and privacy policies for digital services, but research consistently shows that around 94% of Australian consumers report that they have not read "all of the privacy policies or T&Cs that applied to them in the past 12 months".[9] In another example, some websites recommend consumers consider blocking location services where possible.[10] However, this can limit the functionality of services including navigation services and recommendation systems. Instead, the government should heed research findings that when it comes to security and privacy "Australian consumers believe that government has an important responsibility to ensure that consumers are protected".[11] As we discuss in relation to question 15, a key part of informing the public of best practice is to ensure adequate security protections by default, hold organisations accountable and communicate that accountability to the public.

---

[6] Available at: https://www.cyber.gov.au/acsc/view-all-content/campaign/know-how-spot-phishing-scam-messages/scam-messages

[7] For example: https://www.esafety.gov.au/educators/classroom-resources/be-secure

[8] For more information: https://cisomag.eccouncil.org/psychology-of-human-error-could-help-businesses-prevent-security-breaches/

[9] CPRC (2020) *CPRC 2020 Data and Technology Consumer Survey*. Available at: https://cprc.org.au/cprc-2020-data-and-technology-consumer-survey/

[10] For example: https://www.esafety.gov.au/women/using-your-device-safely/phones-tablets

[11] CPRC (2020) *CPRC 2020 Data and Technology Consumer Survey*. Available at: https://cprc.org.au/cprc-2020-data-and-technology-consumer-survey/

15. Should there be enhanced accountability mechanisms for government agencies and industry in the event of data breaches? How else could governments and industry improve public trust?

This question asks how the government can better foster public trust with how data is handled. Although the previous question inquired about public information regarding best practice in data security, it is worth noting that public information on accountability is also an important factor in improving public trust. The government should prioritise introducing stringent consumer protections and communicate the obligations of organisations to consumers, as well as enforcement information to ensure that consumers know that organisations with insufficient security are caught and penalised.

When it comes to privacy and data security, consumers expect there to be safeguards. As a recent Consumer Policy Research Centre (CPRC) submission concerning the Consumer Data Right argues, "[s]afety and fairness should not be left to consumer choice – these are things which consumers expect the law to ensure regardless of choice".[12] As ACCAN has recommended to the recent Privacy Act Review, the current legislation favours business and places consumers at risk. Privacy is fundamental to data security. It can limit how entities misuse personal data as well as minimise the amount of available personal data in the event of a data breach. In our previous privacy submissions, ACCAN has suggested that there needs to be pro-consumer defaults regarding data collection and privacy by design.[13]

> **Recommendation 2:** The Federal Government should implement pro-consumer defaults regarding data collection and privacy by design to minimise the data at risk in the event of data breaches.

To foster public trust in how organisations handle data, the public needs to be reassured that there are sufficient penalties for organisations that fail to adequately protect their data. As the current system stands, research has found that security may not be a priority for some businesses. For example, a security expert told researchers at Deakin University that for Internet of Things manufacturers "Security is something that's kind of annoying for these companies … 'just put it out and if there's an issue we will just patch it up later, let's just get it out as soon as possible'".[14] Clearly greater consumer protections are needed.

---

[12] CPRC 2022, *Submission to Ms Elizabeth Kelly PSM on the Statutory Review of the Consumer Data Right – Issues Paper*, p.2.
[13] ACCAN (2020,) *Privacy Act Review Issues Paper consultation*. Available at: https://accan.org.au/accans-work/submissions/1827-privacy-act-review-issues-paper-consultation
[14] Warren, I. Mann, M. & Harkin, D. 2021, (p.48) *Enhancing Consumer Awareness of Privacy and the Internet of Things*, Australian Communications Consumer Action Network, Sydney. Available at: https://accan.org.au/grants/current-grants/1611-regulating-the-internet-of-things-to-protect-consumer

ACCAN has recommended a range of accountability measures to previous consultations, many of which are relevant for consideration in the National Data Security Action Plan. These include:

Higher penalties for breaching The Privacy Act:[15]

> ACCAN supports the introduction of a privacy regulatory framework equivalent to the CDR scheme in its current form. The Act should replicate the much higher penalties imposed by the CDR scheme to remedy a breach of a Privacy Safeguard – i.e. whichever is highest out of $10M, 10% of domestic turnover pa, or three times the value of benefits obtained from the breach. The civil penalties under the Privacy Act, to be levied by the OAIC, should be increased to mirror the CDR scheme.

A Direct Right to Action:[16]

> ACCAN is in favour of the introduction of a direct right of action to more sufficiently provide consumers with access to justice. The penalties and procedures in Australia's privacy regulatory regime need to be genuinely prohibitive to deter organisations who breach privacy laws. A direct right of action, via a straightforward, easy to access and cheap tribunal, is essential to deliver meaningful privacy protections to everyday Australians.

A Statutory Tort for Invasions of Privacy:[17]

> ACCAN agrees with the ACCC that, although "there is overlap" between the introduction of a direct right of action and a statutory tort for invasion of privacy, a Federal statutory tort would address gaps in the existing privacy framework which is comprised of both Federal and State and Territory legislation. ACCAN is in favour of the introduction of the recommended statutory tort to allow individuals to bring actions for serious invasions of their privacy.

Amendments to the Notifiable Data Breaches Scheme

ACCAN strongly supports the amendment of subsections 26WK(3) and 26WR(4) of the Notifiable Data Breaches Scheme "to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates".[18]

These accountability measures, in addition to other pro-consumer defaults mentioned, should provide a starting point for improving the accountability framework.

---

[15] ACCAN (2020, p.17*) Privacy Act Review Issues Paper consultation*. Available at: https://accan.org.au/accans-work/submissions/1827-privacy-act-review-issues-paper-consultation

[16] ACCAN (2020, p.17) *Privacy Act Review Issues Paper consultation*. Available at: https://accan.org.au/accans-work/submissions/1827-privacy-act-review-issues-paper-consultation

[17] ACCAN (2020, p.18) *Privacy Act Review Issues Paper consultation*. Available at: https://accan.org.au/accans-work/submissions/1827-privacy-act-review-issues-paper-consultation

[18] Attorney General's Department (2022, p.17) *Privacy Act Review Discussion Paper* https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/

Recommendation 3: The Federal Government should introduce strong accountability measures such as those under consideration in the Privacy Act Review including higher penalties for breaching the Privacy Act, a Direct Right to Action and a Statutory Tort for Invasions of Privacy.

Following the implementation of enhanced consumer protections and accountability measures such as those above, the government should conduct targeted consultations with the community to ensure that there is adequate public understanding of the security and privacy obligations and penalties that apply to businesses and governments. This information about data security obligations and penalties should be housed in a single location with the public education materials discussed regarding question 14. This information must meet current accessibility guidelines and be available in a range of languages, including plain English and Auslan.

Recommendation 4: The Federal Government should run targeted public awareness campaigns that explain what security and privacy obligations apply to businesses and governments when they collect, store and use data. It should publicise the penalties for data security and privacy breaches and publicly report examples of the Government holding organisations to account over data breaches that have impacted consumers.

Conclusion

This submission responds to the question of consumer safety and trust in data security regimes. For the digital economy to flourish, it will require consumers to trust businesses and governments with their data. The three data security pillars listed in the Discussion Paper state that data should be secure, accountable and controlled. In the same order these could be interpreted from a consumer perspective to ensure that there are clear security and privacy obligations, effective compliance and enforcement and educational materials about personal data habits and public information on investigation and penalties of breaches. Security systems need to account for variable security knowledge to and provide greater security and privacy protections by default. Australia's digital economy can only thrive when consumers can be confident that data is being stored securely and used only in their interest.

The Australian Communications Consumer Action Network (ACCAN) is Australia's peak communication consumer organisation. The operation of ACCAN is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers.