Cyber Security Legislative Package 2024

25 October 2024

Recommendations

This submission recommends that:

> The Joint Committee revise the requirement that enforcement notices for connected device security standards be sent in a sequential order to allow the Secretary to send stop and recall notices in the first instance.

> The Cyber Security Bill 2024 be amended to require the Department of Home Affairs establish a public register of compliance notices, stop notices and recall notices to improve transparency and consumer visibility of relevant connected devices.

About this submission

The Australian Communications Consumer Action Network (**ACCAN**) thanks the Parliamentary Joint Committee on Intelligence and Security (**the Joint Committee**) for the opportunity to comment on the Cyber Security Legislative Package 2024 (**the Legislative Package**). ACCAN's comments on the Legislative Package are restricted to the Cyber Security Bill 2024 (**The Bill**).

The Cyber Security Legislative Package 2024 intends to implement seven initiatives under the 2023-2030 *Australian Cyber Security Strategy*. The initiatives aim to address legislative gaps to bring Australia in line with international best practice and help ensure Australia is on track to become a global leader in cyber security. In this submission, ACCAN provides the Joint Committee with recommendations to improve the cybersecurity of consumers using connected devices, including Internet of Things (**IoT**) devices by improving the enforcement structures established under the Bill related to non-compliance with security standards for connected devices.

ACCAN's submission is endorsed by the Women's Services Network (**WESNET**).

Contents

Australian Communications Consumer Action Network

ACCAN is the peak body that represents consumers on communications issues including telecommunications, broadband, and emerging new services.

ACCAN provides a strong unified voice to industry and government as we work towards communications services that are trusted, inclusive and available for all.

Introduction

Ensuring a fit-for-purpose regulatory framework for the enforcement of cybersecurity standards is critical to improving consumer confidence in relevant connectable products, including IoT devices.

According to the .au Domain Administration (**auDA**)'s recent *Digital Lives of Australians* report:

- 64% of consumers and 55% of small businesses avoid online activity due to concerns about data security.[1]
- 81% of consumers and 74% of small businesses believe companies should do more to protect the personal information of customers from cyber-attacks.[2]
- 83% of consumers and 79% of small businesses feel failure to protect the personal information of customers should result in penalties.[3]
- 13% of consumers and 24% of small businesses feel they have high capability with cyber security skills.[4]

ACCAN supports the government measures to establish the most practical and comprehensive secure-by-design principles to protect consumers as the 'complexity of security configuration should not be a customer problem', as consumers are time-poor and there is limited digital literacy in the community.[5] Consumers who are not confident in their digital skills and/or have limited digital ability should be assured that the devices they purchase have sufficient cyber security protections. Better minimum standards combined with responsive enforcement capabilities would facilitate a more competitive and effective connected device market. Consumers can place greater trust in devices they purchase, with the knowledge they are covered by mandatory, minimum regulations.[6]

Risks to vulnerable consumers

Standards and protections are essential to support the safety of consumers, particularly given the prevalence of technology-facilitated abuse in the community. 'Technology-facilitated abuse is estimated to involve 8% to 48% of all Domestic and Family Violence (DFV) cases, with 27% of children in Australia experiencing technology-facilitated DFV.'[7] A survey conducted by WESNET noted that the use of technology to monitor and track victim-survivors showed increases across all areas between 2015 and 2020.[8] Additionally, 99% of Australian domestic abuse support workers report they have clients who have experienced technology-facilitated abuse and stalking. [9]

[1] auDA, Digital Lives of Australians 2024 (Report, 2024) 6. Available at: https://www.auda.org.au/news-events-insights/reporting/research-reports/digital-lives-australians-2024.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] ACCAN, 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (Submission, 2024) 4. Available at: https://accan.org.au/accans-work/submissions/2278-cyber-security-strategy-23-30.
[6] Ibid.
[7] ACCAN. Domestic and Family Violence Policy Position (Policy Position, 2023) 1. Available at: https://accan.org.au/accans-work/policy-positions/2253-domestic-and-family-violence.
[8] Ibid p.3.
[9] Woodlock, D., Bentley, K., Schulze, D., Mahoney, N., Chung, D., and Pracilio, A., (2020). Second National Survey of Technology Abuse and Domestic Violence in Australia. 2. WESNET.

WESNET's survey noted the increasing risk of Technology Facilitated Coercive Control (**TFCC**) to vulnerable consumers.

- 'Respondents noted they were seeing GPS tracking apps used 'all the time' (16.2%) and 'often' (45.6%). This is a 131% and 75% increase respectively from 2015'.[10]
- 'The use of technology to monitor and track victim-survivors showed increases across all areas between 2015 and 2020'.[11]
- 'The developments in accessible digital technologies such as GPS enable the quick uptake by large numbers of perpetrators using the technologies to control and monitor women victim-survivors'.[12]

If not securely protected, the granular data collected by connected devices, including location data, can be used by abusers to perpetrate TFCC. It is critical that 'the risk of tech abuse be incorporated into risk assessments and safety planning processes' of IoT device manufacturers.[13] Requiring connected device manufacturers to consider the consumer harm facilitated through their devices would help limit consumer vulnerabilities and improve consumer confidence in the IoT market.[14]

IoT devices are 'inherently designed based on the assumptions that all of their users trust each other' which may leave consumers vulnerable to avenues of abuse if device manufacturers do not account for the possibility of TFCC in the design and manufacture of their products.[15]

Statement of Compliance obligation

Section 16 (3) of the Bill should be amended to require that entities that supply relevant connectable products in Australia must ensure that the statement of compliance with the security standard for a class of relevant connectable product is clearly provided to the customer upon purchase.

This may be achieved through accessible electronic or physical means and should prompt consumers to the relevant and appropriate reporting pathways, should they suspect that their relevant connectable product is non-compliant. This change will contribute to the 'light touch' regulatory system proposed by the Legislative package and improve consumer visibility and awareness of the security standard framework.[16]

[10] Woodlock, D., Bentley, K., Schulze, D., Mahoney, N., Chung, D., and Pracilio, A., (2020). Second National Survey of Technology Abuse and Domestic Violence in Australia. 19. WESNET.
[11] Ibid p.24.
[12] Ibid p.24.
[13] Tanczer, L, Lopez Neira, I, Parkin, S, Patel, T, Danezis . 2018. Gender and IoT Research Report (Report, 2018) 6. Available at: https://www.ucl.ac.uk/computer-science/research/research-groups/gender-and-tech/gender-and-iot#Research.
[14] ACCAN, 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (Submission, 2024) 4. Available at: https://accan.org.au/accans-work/submissions/2278-cyber-security-strategy-23-30.
[15] Tanczer, L, Lopez Neira, I, Parkin, S, Patel, T, Danezis . 2018. Gender and IoT Research Report (Report, 2018) 4. Available at: https://www.ucl.ac.uk/computer-science/research/research-groups/gender-and-tech/gender-and-iot#Research.
[16] Explanatory Memorandum, Cyber Security Bill 2024 (Cth) 124. Available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/CyberSecurityPackage.

Recommendations - Enforcement

Section 17 – Compliance Notice

Section 17(3) of the Bill should be amended to better facilitate effective enforcement outcomes in response to non-compliance with security standards.

ACCAN considers that Section 17(3) should be amended to (**changes in bold**):

> (3) Before giving the notice to the entity, the Secretary must:
>
> (a) notify the entity that the Secretary intends to give the notice to the entity; and
>
> (b) give the entity a specified period (which must not be shorter than **5 business** days) to make representations about the giving of the notice.

Section 18 – Stop Notice

Section 18 of the Bill should be amended to facilitate timelier responses to consumer harm as a result of non-compliance with connected device standards. Requiring enforcement notices to be sent in sequential order risks allowing consumer harm to continue before a recall notice is eventually issued.

In response to identified instances of consumer harm caused by non-compliance with mandatory security standards, ACCAN recommends that the Secretary should be given the authority to be able to issue stop notices and recall notices without first issuing the prior notices required under the Bill. This would improve the Secretary's ability to effectively respond to currently unforeseen instances of significant consumer harm.

ACCAN considers that section 18 (1) of the Bill should be amended to (**changes in bold**):

> (1) The Secretary may give an entity that must comply with an obligation under section 15 or 16 a stop notice if:
>
> **(a) the Secretary is reasonably satisfied that the entity is not complying with the obligation; or**
>
> **(b) is aware of information that suggests that the entity may not be complying with the obligation; or**
>
> **(c) the Secretary is reasonably satisfied that actions taken by the entity to rectify non-compliance with the obligation (whether in accordance with the compliance notice or otherwise) are inadequate to rectify the non-compliance.**

ACCAN considers that Section 18(3) should be amended to (**changes in bold**):

> (3) Before giving the notice to the entity, the Secretary must:
>
> (a) notify the entity that the Secretary intends to give the notice to the entity; and

(b) give the entity a specified period (which must not be shorter than **5 business** days) to make representations about the giving of the notice.

Section 19 – Recall Notice

In accordance with the above recommendation, ACCAN considers that Section 19(3) should be amended to (**changes in bold**):

(2) The Secretary may give an entity that must comply with an obligation under section 15 or 16 a recall notice if:

(a) the Secretary is reasonably satisfied that the entity is not complying with the obligation; or

(b) is aware of information that suggests that the entity may not be complying with the obligation; or

(c) the Secretary is reasonably satisfied that actions taken by the entity to rectify non-compliance with the obligation (whether in accordance with the compliance notice, stop notice or otherwise) are inadequate to rectify the non-compliance.

ACCAN considers that Section 19(3) should be amended to (**changes in bold**):

(3) Before giving the notice to the entity, the Secretary must:

(a) notify the entity that the Secretary intends to give the notice to the entity; and

(b) give the entity a specified period (which must not be shorter than **5 business** days) to make representations about the giving of the notice.

These amendments should not prohibit an accelerated enforcement process in response to egregious harm as a result of non-compliance with security standards for relevant connected devices.

Section 20 - Public notification of failure to comply with recall notice

ACCAN recommends the Department of Home Affairs (**DoHA**) establish a public register of compliance notices, stop notices and recall notices to improve transparency and consumer visibility of relevant connected devices. ACCAN would support the establishment of a public register of compliance notices, stop notices and recall notices to improve transparency and consumer visibility over the IoT device market.

Under the existing Legislative Package, only recall notices may be published by the relevant Minister's website. Providing consumers with information on the compliance of entities with security standards can facilitate consumers making educated purchasing decisions and avoiding entities who have demonstrated non-compliance with security standards. This would assist in facilitating a market in which manufacturers are more likely to comply with security standards.

Section 21 - Revocation and variation of notices given under this Part

ACCAN considers that section 21(2) be amended to (**changes in bold**):

> (2) Before giving the notice to the entity under subsection (1), the Secretary must:
>
> (a) notify the entity that the Secretary intends to give the notice to the entity; and
>
> (b) give the entity a specified period (which must not be shorter than **5 business** days) to make representations about the giving of the notice.

The existing staged enforcement structure facilitates delayed responses to consumer harm

To provide further context for ACCAN's recommendations, we have set out the steps required under the current framework to recall a relevant connected device that exposes consumers to significant harm. These steps include:

1. Examination and testing of the relevant security standards by the Secretary or consumer reporting of cybersecurity vulnerabilities leads to the Secretary being reasonably satisfied that an entity is not complying with the obligations in relation to a relevant connected products' security standards.
2. The Secretary intends to give a compliance notice to the entity and must wait a *minimum* of 10 days to allow the entity to make representations about the giving of the notice.
3. Following the issuing of a compliance notice, the entity may present false compliance with the previous issued compliance notice, requiring the Secretary to examine the entity's compliance with the notice or consumer reporting to indicate non-compliance.
4. Once the Secretary is reasonably satisfied that an entity is not complying with the obligations of the compliance notice, the Secretary must wait a *minimum* of 10 days to allow the entity to make representations before issuing the stop notice.
5. Following the issuing of a stop notice, the entity may present false compliance with the stop notice, requiring the Secretary to examine the entity's compliance with the notice.
6. Following the Secretary being reasonably satisfied that an entity is not complying with the obligations of the stop notice, the Secretary must wait a *minimum* of 10 days to allow the entity to make representations before issuing the recall notice.
7. If an entity fails to comply with a recall notice, the Minister may publish information on the identity of the entity, details of the product and the risks posed by the product relating to the non-compliance on the Department's website.

In ACCAN's view, it is only at point seven that consumers may have any visibility that the devices used in their homes may be insecure and a threat to their wellbeing. The proposed framework's process is time consuming, administratively intensive and unnecessarily delays responses to possibly egregious consumer harm.

Amending the Bill to facilitate accelerated issuing of stop and recall notices can more effectively facilitate appropriate responses to instances of significant consumer harm. ACCAN's experience with respect to consumer protections in the telecommunications sector has demonstrated that a staged enforcement approach produces ineffective, delayed responses to significant consumer harm, and risks ongoing harms to consumer wellbeing.

Conclusion

ACCAN supports amending the Bill to improve the responsiveness of the enforcement structure proposed by the Joint Committee. However, ACCAN's longstanding experience in supporting consumer protections in the telecommunications sector suggests that the current approach, without significant revisions, will only provide superficial protections for consumers, while potentially allowing consumer harms, including TFCC, to continue.

Therefore, ACCAN urges the Joint Committee to:

- Revise the requirement that enforcement notices for connected device security standards be sent in a sequential order to allow the Secretary to send stop and recall notices in the first instance.
- Establish a public register of compliance notices, stop notices and recall notices to improve transparency and consumer visibility of relevant connected devices.

Adopting these measures will ensure the Bill provides much greater protections to consumers, especially those in vulnerable circumstances, while also adopting best practice regulation and helping to ensure Australia becomes a global leader in cyber security.

We thank the Committee for the opportunity to comment on the Legislative Package. Should you wish to discuss any of the issues raised in this submission further, please do not hesitate to contact Con Gouskos, Policy Adviser, at con.gouskos@accan.org.au.