7 July 2022

Department of Home Affairs
Via email: datasecurityandstrategy@homeaffairs.gov.au

RE: **National Data Security Action Plan - Discussion Paper**

I write in regard to the Department of Home Affairs' Discussion Paper on the National Data Security Action Plan.

As Australia's largest consumer advocacy group, CHOICE supports measures that protect the rights of consumers both offline and online. As more people turn to the internet to access essential services and make consumer transactions, it is crucial that regulatory measures are forward-looking and work to correct power imbalances that are prevalent in the digital space.

This is particularly important when it comes to data security, as consumers often have limited oversight, knowledge and control over where their data flows and rests. Instead, consumers place implicit trust in the business that collects or holds their data, expecting that their information is kept securely. However, this trust can cost the consumer. When a data breach occurs, consumers become susceptible to cybercrime, such as identity theft and scams.

The Discussion Paper highlighted that customer personal information is the most common and most expensive type of record lost or stolen in a data breach, costing on average $252 per record.[1] Consumers often have no recourse after such a breach occurs, as seen in the recent National Disability Insurance Scheme third party data breach where a sample of stolen client data was posted on a deep web forum.[2] Such experiences can alter a consumer's life, impacting their financial, emotional and social wellbeing through fraud, scams and erosion of trust. This is why it is crucial that companies understand the importance and take actions to secure data, no matter where they exist in the supply chain.

[1]Department of Home Affairs 2022, *National Data Security Action Plan*, p 11, https://www.homeaffairs.gov.au/reports-and-pubs/files/data-security/nds-action-plan.pdf
[2]Blakkarly, J 2022, 'NDIS recipient information hacked in major data breach', *CHOICE,* 31 May, https://www.choice.com.au/consumers-and-data/protecting-your-data/data-privacy-and-safety/articles/ndis-recipient-information-hacked-in-major-data-breach

CHOICE urges the Australian Government to introduce a best interest duty for businesses that collect, use or disclose data. This would allow for a cultural change in which businesses consider first and foremost the individual whose data they collect and assess potential risks from that perspective.

Responses to questions

9. What steps could your business take to better understand the value of the data they process and store? Do businesses have sufficient awareness of their data security obligations?

Australian consumers expect that the businesses they interact with will process and store our data securely. Consumers often have no other choice than to trust that this is the case as they lack resources, capability and expertise to manage cybersecurity risks.

A recent CHOICE investigation into the use of facial recognition technology in retail settings found that many businesses lacked sufficient awareness of their data collection and security obligations under existing Australian law.[3]

In April 2022, CHOICE commenced an investigation into the use of facial recognition technology in major Australian retail stores. CHOICE requested information from 25 leading Australian retailers on their use of facial recognition technology and analysed their privacy policies, available online.

Based on the responses and analysis, CHOICE identified that Kmart, Bunnings and The Good Guys are collecting and using their customers' sensitive information via the use of facial recognition technology. More specifically, the retailers are collecting sensitive biometric data known as a 'faceprint' through their facial recognition technology systems. Under the *Privacy Act 1988*, the collection of sensitive information, such as biometric data, has stricter requirements in relation to notice and consent. This matter has been referred to the Office of the Australian Information Commissioner for consideration.

The investigation received widespread media coverage indicating that the Australian community was not aware of the retailers' practices in relation to the use of facial recognition technology in store. This was also reflected in CHOICE's nationally representative survey data conducted between March and April 2022, which found 76% of respondents didn't know retailers were using facial recognition in retail settings.[4] Equally, 78% expressed concern about the secure storage of faceprint data.

[3]Blakkarly, J 2022, 'Kmart, Bunnings and The Good Guys using facial recognition technology in store', *CHOICE*, 15 June, www.choice.com.au/facialrecognition

[4] CHOICE Consumer Pulse March 2022 is based on a survey of 1034 Australian households. Quotas were applied for representations in each age group, as well as genders and location, to ensure coverage in each state and territory across metropolitan and regional areas. Fieldwork was done between 22 March and 7 April 2022.

This case demonstrates that businesses in Australia are not sufficiently informing and gaining consent from consumers for the collection and use of their sensitive information, which is an important starting point for data security. Such practices pose significant risks to individuals, including invasion of privacy, misidentification, discrimination, profiling and exclusion, as well as vulnerability to cybercrime through data breaches and identity theft.

12. Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a 'size' threshold?

Big data is big business and the use of consumer data by businesses of all sizes will increasingly have material implications for consumers. Data security should be treated the same regardless of the size, structure or sector of an organisation or business.

Businesses of all sizes should strive to ensure the data they hold is safeguarded. It should not be up to the consumer to determine the level of risk they will accept depending on the size of the business they are interacting with. In line with other consumer protection frameworks including the Australian Consumer Law, people should be able to expect a baseline of protection regardless of the size of business.

The Australian Government should hold businesses to stronger standards of data security. This could be supported by overarching best practice guidance for businesses, including a set of minimum standards and expectations related to data security.

The introduction of a best interest duty for businesses that collect, use or disclose data would benefit consumers and allow for a cultural change in which businesses consider first and foremost the individual whose data they collect and assess potential risks from that perspective.

A consistent and uniform approach to data security across the economy will increase trust and confidence amongst consumers as they can make assumptions that their personal information is being treated in accordance with the law, regardless of the size of the business they interact with.

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?

The onus on ensuring strong data practices should be placed on the businesses who control and store people's data, not on consumers. Businesses should be responsible for ensuring the system is working for consumers.

As identified in the Discussion Paper, many consumers lack the resources, capability and expertise to manage cybersecurity risks, and yet are the most vulnerable to data breaches and associated harms. CHOICE is cautious in suggesting that consumers need more public

information on managing cybersecurity risks, particularly since they are not well-placed to do so in the data ecosystem.

However, the Australian Government should consider working with regulators and consumer advocacy groups to share information that promotes data security best practice and reach the target audiences.

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?

CHOICE supports the introduction of an obligation for government agencies and industry to act in the interests of the people whose data they collect, hold and use. This could take the form of a best interest duty, as is being explored by some jurisdictions in the United States, or a broader obligation to act in the collective interests of a large group, similar to obligations that apply to superannuation fund trustees. This would allow for a norm shift in which organisations and businesses consider the interests of the user of the product and service and assess potential risks that may arise.

CHOICE also supports amendments to the Notifiable Data Breaches scheme. The Australian Government can make improvements in relation to the triggers for reporting a data breach. Specifically, the eligibility criteria of a data breach being 'likely to result in serious harm to one or more individuals' and 'the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action' should be removed.[5] The severity of harm is subjective and may lead to underreporting by an entity to manage reputational risk. This comes at a cost to the consumer. Similarly, consumers have the right to know when their information is involved in a data breach, regardless of whether remedial action has been taken.

For further information, please contact CHOICE on apereira@choice.com.au

Yours sincerely,

Amy Pereira
Senior Campaigns and Policy Advisor

[5] Office of the Australian Information Commissioner 2022, 'When to report a data breach', accessed on 6 July 2022, https://www.oaic.gov.au/privacy/notifiable-data-breaches/when-to-report-a-data-breach