REQUEST FOR COMMENT RESPONSE

AUSTRALIA PRIVACY ACT REVIEW REPORT 2022

March 31, 2023

I. INTRODUCTION

In response to the Australian Government Attorney-General Department's request for feedback on the Privacy Act Review Report, CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

The Attorney-General's ("AG") Department has conducted a thorough Privacy Act Review that takes into consideration the broad variety of viewpoints it received from previous consultations. With each iteration, the Government is making significant progress towards achieving its goals of better empowering consumers, protecting their data and better serving the economy of Australia.

CrowdStrike provided feedback in 2020 and 2022 in response to the AG's Department's earlier requests on the Privacy Act. We are happy to see many previous comments incorporated into the next iteration of the Privacy Act.[1] While we do not have feedback on every aspect of this Privacy Act Review, we do want to offer several points that may be of value to the AG's Department as it continues developing the Privacy Act. We acknowledge this effort is being conducted in

[1] *See* Commonwealth of Australia, Privacy Act Review Report 2022 at footnotes 331-32, 352-53, 362, 379, 1642, 1986.

parallel with the 2023-2030 Australia Cyber Security Strategy Discussion Paper, which we will comment on separately.

Section 6. Small Business Exemption

Proposal 6.1 calls for removing the small business exemption, but only after a number of analyses and consultations with small businesses are completed. These analyses and consultations will take time. Therefore, CrowdStrike reiterates the feedback it provided to the Attorney General in 2020, that today, the failure of a business of any size, from a startup to a tech giant, to meet data protection obligations may pose a risk to the privacy of individuals. Consequently, it is paramount that a business is given the tools it needs to protect the data of its customers without overburdening owners and operators. The Australian Privacy Principles (APPs) are a tool to help a business protect data. With the right incentive structure and harmonized guidelines, certain APP provisions, such as those related to the security of data, may help improve data protection at small entities for the benefit of both the business and their stakeholders.. One data breach can often have a devastating impact on a small business and be difficult to recover from.

Updated APP requirements should focus on incentivizing the adoption of cybersecurity best practices to achieve data protection objectives--for small businesses and large organizations alike. This means ensuring that regulations permit and promote the adoption of affordable, effective, and scalable cybersecurity protections. Today, even small entities can achieve sophisticated cybersecurity protection by leveraging managed service providers.[2] This can be a gamechanger for entities without security programs and/or the resources to adequately equip them.

Section 19. Automated Decision Making (ADM)

The Act calls for a number of proposals regarding Automated Decision Making (ADM), which would be implemented as part of the broader work to regulate AI and ADM. CrowdStrike was pleased to see its feedback from 2022 called out in the body

[2] *See Drew Bagley, Testimony on CISA 2025: The State of American Cybersecurity from a Stakeholder Perspective,* House Homeland Security Committee Subcommittee on Cybersecurity and Infrastructure Protection (March 23, 2023) (How small and medium sized businesses use managed security service providers), https://www.congress.gov/118/meeting/house/115516/witnesses/HHRG-118-HM08-Wstate-BagleyD-20230323.pdf.

of the report, noting that AI has the opportunity to drive positive social outcomes and create the opportunity for innovation in a variety of industries including medicine and education. However, in light of Proposals 19.1, 19.2, and 19.3, which suggest policies that focus on protecting individual rights by giving them the right to object to how a particular technology (AI) uses their information, we would like to reiterate some of the points we previously made in 2022.

We understand from the Privacy Act Review that the concern with AI is the possible harm to Australians, but for AI, like for any other technology, the context in which it is used, rather than the mere fact that it is incorporated, is material. Consequently, relying upon a right to object to a particular technology or data processing methodology is not the best approach to protect rights in an ever-evolving technological landscape. Instead, we recommend protecting the rights of Australians through a technology-neutral approach. When creating regulations on the safe use of AI, Australia should consider adopting language similar to the General Data Protection Regulation's ("GDPR") requirement that organizations implement safeguards "appropriate" to the risk to protect personal information. This approach incentivizes organizations to take into account modern, rapidly-evolving data breach risks posed by cybersecurity threats from e-crime, 'hacktivist', and nation state actors using tactics such as ransomware, supply chain attacks, or malware-less intrusions.

Section 23. Overseas data flows

We believe today's economy depends more on cross-border data flows than ever before. This trend will continue, especially in light of the digital transformation accelerated by Covid-19 and the "work from anywhere" movement. The importance of cross-border data flows is far-reaching, from data subjects who benefit from offerings or contribute to the digital workforce all the way to the organizations that manage data flows. Consequently, it is important for any imposition of cross-border data flow requirements to recognize the dependency of Australian innovation, workforce jobs, and effective cybersecurity on cross-border data flows. This means that it is critical to provide organizations with deference to make their own context-informed decisions about cross-border data by adhering to core data protection principles related to the circumstances of specific transfers and weighing risks accordingly.

Data protection is best achieved where intentional transfers of personal data are permitted with practical safeguards, while unintentional transfers of personal data via data breaches are thwarted by protecting against ever-evolving cybersecurity threats with innovative technologies. As a leading cybersecurity provider, it is our view that perhaps the most significant threat to personal data comes from threat actors operating unlawfully. While responsible data controllers and processors adhere to robust compliance programs, cyber adversaries do not play by the rules

In order to remain future-flexible, it is important to prioritize the goal of protecting data regardless of where it is, rather than equating data protection with restrictions on cross-border data transfers. Consequently, providing as many means as possible to lawfully transfer data abroad will continue to afford Australian organizations the ability to create and use innovative technologies on a global scale. This should be the case regardless of whether a certification scheme is introduced, or in the event of the development of standard contractual clauses or a new regional certification scheme that works alongside the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules System (APEC CBPR).

To the extent standard contractual clauses are introduced, it is important to factor-in the practical implications of existing global standards. Whether standard obligations are introduced or APP principles are incorporated into ad hoc agreements, each of the parties in a contract are bound to those with whom there is privity of contract, and the resulting legal protections create a "Chain of Contractual Accountability." Moreover, each party must abide by its own directly applicable legal requirements in a "Chain of Independent Obligations." In other words, data subject rights remain protected by (i) enforceable contractual obligations between respective parties, and (ii) direct application of law, such as the Privacy Act, to any party processing personal data within the law's scope.

Supporting such a written agreement can be done with a strong policy on cybersecurity. Cross-border data flows are necessary for cybersecurity in the private sector, not much unlike how national security depends upon cross-border data flows in the public sector. In fact, many of the most innovative technologies for protecting personal data against data breaches leverage endpoint telemetry data, cloud-native Software-as-a-Service (SaaS) delivery, 24/7 global threat hunting, and

cross correlation of indicators of attack. Moreover, modern IT infrastructure in general often invariably involves cross-border data transfers.

We recommend considering the importance of cybersecurity as a supplemental measure to the written agreements by looking at threats, predominantly in terms of threat actors. Malware, malicious infrastructure, and adversary tactics, techniques, and procedures (TTPs) change over time, but often the groups behind malicious activities are more durable. This means that considering threat actor motivations helps defenders understand everything from their incentives to the risks posed by failing to prevent them from breaching your environment. Threat actors generally fall into the categories of: criminal groups, which largely seek profit; nation state entities, which pursue a variety of geopolitical ends; and 'hacktivists,' which have ideological motives. When crafting guidance, governments must be concerned with each, particularly during a time of unprecedented attacks from specific nation states along with the general trend of increased e-crime.

Specific threats vary across these different types of actors, but a few are especially notable. Criminal groups increasingly target public sector entities with ransomware, which disrupts victim IT environments in order to extort funds. Nation state groups have also used ransomware-like tools and TTPs to cause disruptions for other ends. Additionally, nation states have been observed to hack and leak sensitive communications for political ends, or steal intellectual property or sensitive business information to strengthen domestic commercial actors. Across all types of threat groups, adversaries are leveraging TTPs that enable them to avoid using malware, which complicates detection and prevention for entities using unsophisticated or legacy security solutions.

Further, we advocate the "1-10-60 Rule."[3] This concept holds that security teams should endeavor to reliably detect malicious events within one minute; investigate them within ten minutes; and isolate or remediate affected hosts or resources within one hour. Further, organizational leaders should measure each of these performance indicators over time, and continuously improve them until the goals are met. Organizations that can defend themselves at this velocity will be

[3] A more in-depth explanation of this concept is available here: https://www.crowdstrike.com/resources/crowdcasts/the-1-10-60-minute-challenge-a-framework-for-stopping-breaches-faster/.

well-equipped to outpace the vast majority of threat actors,[4] and prevent minor security events from becoming costly, complex, and sometimes devastating incidents.

In sum, even with a principles-based approach and absent standard contractual clauses, personal information transferred outside of Australia can receive appropriate protection from the Chain of Contractual Accountability, the Chain of Independent Obligations and strong cybersecurity safeguards.

Section 28. Notifiable Data Breaches Scheme

CrowdStrike commends the AG's Department on the Proposals in Section 28, which considers reporting timelines, mitigation measures, information sharing, and harmonization with overlapping schemes. We encourage the AG's Department to consider adding a new Proposal to amend the current definition of an "eligible data breach."

Currently, an eligible data breach is where: Unauthorized access to or unauthorized disclosure of personal information or loss of personal information, that an entity holds, is likely to result in serious harm to one or more individuals, and the entity has not been able to prevent the likely risk of serious harm with remedial action.[5]

Proposal 28.2 calls for entities to notify the Commissioner within 72 hours after becoming aware of "reasonable grounds to believe that there has been an eligible data breach to an entity." In defining what constitutes a notifiable data breach and level of harm, it is critical to focus on internationally-accepted principles-based concepts rather than prescriptive technical requirements. CrowdStrike recommends adopting a risk-based approach and take the following factors into consideration:

- Nature of the data in question: Could the data in question be used by a threat actor to cause significant harm to individuals?

[4] *See* CrowdStrike's 2020 Global Threat Report: https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/.
[5] https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme#identifying-eligible-data-breaches

- Impact of a breach: Was the data successfully exfiltrated and, if so, to whom was the data exfiltrated?
- Mitigations: Did the carrier successfully mitigate impacts?

Therefore, CrowdStrike recommends clarifying what an "eligible breach" is and considering the following distinctions to narrow the scope of the definition of "eligible breach."

Alerts versus Incidents. In cybersecurity, an important distinction exists between alerts and incidents, which should help inform notification scenarios and standards. In most cases, carriers using contemporary cybersecurity solutions should be alerted to malicious activity occurring in their environment. The nature of these alerts may vary, and could cover something like the installation of malicious software on one system, or the compromise of a single account. In most scenarios where defenders see these alerts and address them quickly, an issue does not meet any reasonable standard of a cybersecurity "incident" because the threat actor has not meaningfully achieved their objective or accessed sensitive information. With this in mind, an alert should not be included in the definition of "breach."

Impact versus Serious Impact. Another important distinction that merits discussion is that of impacts versus serious impacts. Not all breaches have the same level of severity. For example, an incident where a threat actor sees a list of user names might have a small or negligible impact on affected parties. Whereas, another incident in which a threat actor exfiltrates complete financial or medical records may have a severe impact. Consideration of the impact and severity of a breach is important not only when initially assessing evidence of an intrusion but also in discerning the efficacy of mitigation measures.

Mitigated Attacks. Threat actors may choose to target an organization in a series of steps, rather than in a single attack. In fact, an initial intrusion into an enterprise is often not a threat actor's end goal. Instead, threat actors may first deploy a backdoor, harvest credentials, or use other methods in order to move laterally throughout a network and to their ultimate objective. A threat actor may be stopped at any of the steps in the killchain, and this raises important questions that impact the breach notification process - namely, if a breach is mitigated, does the obligation to notify still exist? For example, if a threat actor enters an enterprise

with the goal of exfiltrating data but is stopped before the infiltration occurs, the possible resulting impact of the incident has been mitigated. In such an example, it is a breach when the threat actor enters the network but it could have been a substantial breach if the goal of data exfiltration was reached. Ultimately, this means that a data breach in and of itself may not pose a risk of harm to consumers where successful steps have been taken to mitigate the breach and prevent exfiltration. Mitigated breaches should not be included in the reporting scope.

Reporting Timeline. The Privacy Act Review calls for reporting an "eligible breach" within 72 We recommend that any reporting timeline requirements be considered in context. As discussed above, not all cyber incidents have the same level of severity and rise to a level of individual harm that necessitates reporting.

III. CONCLUSION

The Privacy Act Review provides a thoughtful response to a complex legal and policy area. As updates to the law and administrative rulemaking moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any legislative updates and proposed rulemaking focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Fabio Fratucello
Field CTO, International

Email: policy@crowdstrike.com

***