Google Australia Pty Ltd
Level 5, 48 Pirrama Road
Pyrmont, NSW 2009
Australia

google.com

Friday 27 August 2021

Department of Home Affairs
4 National Circuit
Barton ACT 2600

BY ELECTRONIC SUBMISSION

Thank you for the opportunity to provide feedback in response to the discussion paper titled "Strengthening Australia's cyber-security regulations and incentives ". Google commends the Department and Government for the long standing focus on cyber security and the iteration of the Cyber Security Strategy over time. We were delighted to see the Australian Cyber Security Centre join the UK and US Governments in issuing a joint cybersecurity advisory in July[1] and hope to see further cooperation amongst these allied nations in the future. We welcomed the opportunity to participate in the development of the Code of Practice for Securing the Internet of Things for consumers (launched in September 2020). There remains alot of work to do in this important policy area and we appreciate that this work is a shared responsibility across the Government and the private sector.

Security is a necessity for individual users and businesses, and something that Internet users care about and expect that Google delivers by providing products and services that build security into their design, and through tools that help them easily take control over their online security. Google has a long history in building secure infrastructure and helping to define cybersecurity best practices. We protect our users and enterprise customers by providing industry-leading security.

We recognise our responsibility and are committed to doing our part to keep users, as well as common Internet infrastructure, secure. Effective security requires collaboration. We work with many stakeholder groups to develop and pursue a safe, open, inclusive and global online environment. This includes work with other players in the industry and standard-setting bodies like the International Organisation for Standardisation (ISO), World Wide Web Consortium (W3C), and the Internet Engineering Task Force (IETF) as well as regional standards bodies such

[1] https://www.cisa.gov/news/2021/07/28/us-uk-and-australia-issue-joint-cybersecurity-advisory

as Standards Australia. We also believe in contributing to international best practices, templates, developer tools, and other integrated solutions that make security stronger and easier to implement.

Strong cybersecurity practices start with developing a culture that values security. At Google, we have a central security engineering team with more than 700 dedicated engineers, as well as security engineers embedded in our product teams. We minimise insider risk by mandating employee background checks, having all employees regularly undergo security trainings, and limiting access to sensitive data based on job function and a need to know. Logs access and other access to sensitive information is regularly checked and audited, and we've developed a number of internal tools to ensure compliance with security policies.

Google has many initiatives and tools to support strong cybersecurity and enable/empower users. To highlight a few:

- SafeBrowsing protects more than four billion devices from phishing across the web. Google's SafeBrowsing fulfills Google's mission by making the world's information safely accessible. SafeBrowsing continues to show millions of warnings about websites it considers dangerous or insecure. We build SafeBrowsing into Chrome to keep users from going to unsafe sites, as well as Gmail, to keep users from clicking on unsafe links. We also make it freely available to other browsers -- Apple (Safari) and Mozilla (Firefox) deploy SafeBrowsing to protect their users across the web. Website and application builders can also access SafeBrowsing APIs through our developer tools to help keep their assets secure.
- Password management and alerts: Password Checkup is a feature that enables users to (i) see if their passwords have been compromised when they log into external accounts and (ii) take action to protect themselves if their credentials have been compromised. In 2019, we integrated the Password Checkup feature directly into Chrome. Password Alert is an additional tool that tells users if they may have accidentally entered their Google account password into a non-Google website (oftentimes a dangerous site that is phishing for account credentials).
- Advanced Protection: In 2017, we unveiled the Advanced Protection Program (APP), which provides the strongest account protection that Google offers. APP requires the use of security keys, which are resistant to person-in-the-middle attacks where the use of two-factor authentication codes can be phished. We've helped enroll at-risk users into APP, including human rights activists, journalists, and political campaign staff.
- DNS over HTTPS (DoH): In September 2020, we implemented Secure DNS in Chrome to Android. DoH encrypts DNS communication, thereby helping prevent attackers from observing what sites you visit or sending you to phishing websites.
- Play Protect: Google Play Protect runs on all Android-powered devices and runs a safety check on all apps downloaded on a device. It warns users when they may

unintentionally be attempting to download malware or unwanted software, and also provides alerts when an app is seeking sensitive permissions to personal information, such as the precise location of a device. Play Protect scans more than 100 billion apps daily to make sure users are protected against malicious actors.

- We have a number of other security products and services not mentioned here, including Project Shield (a free service that protects critical organisations, like news agencies, from DDos attacks), titan security keys (our strongest protection against account hijacking and phishing), and Chronicle.

Turning to the some of the questions posed by the discussion paper;

1. What are the factors preventing the adoption of cyber security best practice in Australia?

   [No response]

2. Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

   [No response]

3. What are the strengths and limitations of Australia's current regulatory framework for cyber security?

   [No response]

4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

   Google would welcome consolidation of the multiple statutes that address cyber security that are overseen by a number of different portfolios. Multiple legislative frameworks managed by different agencies creates confusion and risks alienating businesses from engaging with these frameworks.

5. What is the best approach to strengthening corporate governance of cyber security risk? Why?

   Start with voluntary standards to underpin a security environment that is well situated to address emerging threats; proceed from the assumption that lack of awareness can be remedied through guidance and further education. Has the Department considered working with the Australian Institute of Company Directors (AICD) to include cyber

security training within their coursework (targeting aspiring company directors) and refresher training modules (for more established company directors).

6. What cyber security support, if any, should be provided to directors of small and medium companies?

   Google sees tremendous benefit in targeted strategies to improve understanding of cyber security by directors of small to medium sized businesses. Such strategies could include developing a list of the five protections that every small to medium sized business should invest in, equipping small business advocacy groups with practical guidance that they can share with members, establishing a directory of cyber security related services that are available to small to medium businesses.

7. Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

   It would be helpful to develop a directory of courses for senior business leaders; perhaps the Government could work with the ANU National Security College and / or AustCyber to develop such a directory?

8. Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

   It is important to note that the Privacy Act currently regulates businesses generating more than $3m in annual revenue. Therefore, a key target audience for promoting the uptake of cyber security standards in Australia - businesses earning less than $3m in annual revenue - would be precluded from complying with an enforceable cyber security code under the Act. Furthermore, Australian Privacy Principle 11 already requires that entities regulated by the Privacy Act take steps to secure personal information. Therefore, Google is not persuaded that a code under the Privacy Act would bring about any significant change from the status quo.

9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

   See response to question 8.

10. What technologies, sectors or types of data should be covered by a code under the Privacy to achieve the best cyber security outcomes?

See response to question 8.

11. What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

    Consumers and hardware manufacturers benefit when security is easy, simple, and clear. Whether it's because they expect that their information is protected, aren't willing to take extra steps to secure it, or aren't aware of those steps at all, consumers shouldn't be expected to have to protect their information themselves. They are safest when security protections are automatic and built-in to a device.

    Consumers would benefit from more transparency about a device's protections as well. If there are standardised criteria that are presented clearly and simply, security labels would be helpful as more consumers would invest in devices with stronger security protections and manufacturers would compete on this point.

    We should note that any labeling / rating scheme has to negotiate the ever-evolving nature of security. Issues will always arise that would have affected a device's original security review. We are supportive of a 'live label'; for example, this could be a scannable QR code on a device's packaging that shows users up-to-date evaluation of that device's security protections.

    Device manufacturers face two challenges when it comes to making security simple: lack of clarity around standards and difficulty testing their devices to make sure they're compliant. Harmonising IoT security standards worldwide, and providing resources for testing will dramatically improve security of smart devices.

12. Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices? a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate? b. If not, what standard should be considered?

    Google does not have a preferred standard. Rather we submit that it is more important to work towards harmonising existing standards in order that compliance and labelling obligations are clear and easy to understand.

13. [For online marketplaces] Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?

Google operates an online store that sells Google manufactured devices. All of the products sold within the Google store have been reviewed and certified by ioxt[2], a public/private organisation dedicated to security standards and compliance.

14. What would the costs of a mandatory standard for smart devices be for consumers, manufacturers, retailers, wholesalers and online marketplaces? Are they different from the international data presented in this paper?

    The cost of mandatory standards differs among consumers, manufacturers, retailers, and wholesalers. However, at a high level, we are supportive of a set of mandatory, baseline standards that are harmonised across different markets. Beyond this baseline, the ecosystem could voluntarily demonstrate security protections that they've implemented beyond the baseline.

    A mandatory standard would be least costly for consumers, as they'd benefit from safer devices, overall. However, there could be concerns about previously owned devices that don't meet the standard, or difficulty understanding the standard itself leading to its irrelevance. It would be more costly for manufacturers, as they may need to make changes to their product development. However, in the long run, compliance with a standard could serve as a positive product differentiator.

    Retailers / wholesalers / online marketplaces are similarly positioned. Given the proliferation of smart devices, some devices won't meet standards and might not be able to be sold. Given the massive size of the IoT market — nearly 30 billion are expected to be available by 2025[3] — this would have a significant adverse financial impact for these businesses. This could be offset by increased sales of devices that do meet the standard and eventually devices that have implemented new protections to meet it.

15. Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in this paper?

    The proliferation of many different security standards for smart devices around the world is a substantial risk to securing this market. Google is strongly supportive of solutions — a common, baseline security standard for example — that help to harmonise these standards.

---

[2] https://www.ioxtalliance.org/

[3] https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

IoT security standards are currently being developed in the US, Singapore, Finland, EU, and Australia. We are fully supportive of prioritising security, especially at this early juncture when the IoT space is still evolving. However, a laundry-list of different standards is not scalable for hardware manufacturers and will be detrimental to the overall safety of the ecosystem. Relatedly, this could be damaging for particular countries with standards that are perceived to be weaker than others. Not only would they be perceived as more lax on security, but they could create a market for less secure devices.

16. What is the best approach to encouraging consumers to purchase secure smart devices? Why?

    [No response]

17. Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

    Assuming the labelling is also standardised across the industry, this combination could be effective because it would set expectations for both consumers and hardware manufacturers about a device's protections. OEMs would have to consider these specs as they manufacture a device, and consumers would understand the types of protections they'd be receiving.

18. Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not? a. If so, which existing labelling scheme should Australia seek to follow (Singapore, Finland, UK, US)?

    There will be challenges to voluntary uptake of labelling for smart devices. For example, hardware manufacturers — particularly at the lower end — operate on razor-thin margins and often can't afford to prioritise security. Furthermore, many retailers do not provide incentives for hardware manufacturers to develop these types of transparency tools.

    Notwithstanding, Google is firmly of the view that the security benefits of labelling outweigh these hurdles. The combination of mandatory labelling based on a consistent, baseline standard with potential incentives for manufacturers—particularly those building lower-cost devices—could prove to be a winning approach.

    Finally, Google suggests that it would be beneficial for manufacturers to label smart devices both digitally and physically; with the caveat that manufacturers / retailers would have to develop these labels carefully to avoid confusing consumers. For

example, the digital rating might differ from the physical one because it has been updated based on issues that were unknown when the device was first examined and a physical label affixed to it.

19. Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?

    If a mandatory labelling scheme were established, an expiration date is a good option. However, given the multitude of different security protections, defining precisely what is 'expiring' would be critical in order for the labels to be meaningful. For instance, an expiration date could mean that a device will no longer receive security updates.

    An alternative would be a 'live label' that reflects the nature of security issues which are constantly evolving. For example, this could be a QR code that users scan to see the most up-to-date evaluation of a device's security protections.

20. Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

    If a mandatory labelling scheme were established, it should cover mobile phones for a few different reasons:

    - *Phones are increasingly the hub that controls other connected devices that people use in their everyday lives: speakers, TVs, watches, cars, appliances. The lines dividing phones from IoT are increasingly blurry and a labelling scheme should be developed with this trend in mind.*
    - *While there is likely a better understanding of smartphone vs IoT security among consumers, a labelling scheme doesn't exist for phones at the moment. This is arguably more urgent than a labelling scheme for smart devices. Consumers would benefit from these for the reasons outlined above.*
    - *It would make the connected device ecosystem significantly safer without the challenge of developing new security standards from scratch. The work wouldn't be trivial for smartphone OEMs, but they would have clear and concrete targets based on established standards and would likely be working from a base of existing security protections.*

21. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

    The main concern faced by any business when considering disclosing a vulnerability is a loss of reputation and standing in their industry. Encouraging a behavioural shift

whereby companies feel more comfortable with making such disclosures will take time and will improve as we see more and more businesses leading by example. Guidance that sets out different ways of approaching vulnerability disclosure could be helpful; for instance, vulnerability rewards programs (like those run by Google[4]) can encourage a more public posture on vulnerability reporting.

22. Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

    To be valuable and useful to small businesses, any health check program developed by the Government would need to be accessible and simple.

    As an alternative, the Government could choose to partner with one or more private sector companies like Google to develop a health check program. Like many organisations, Google regularly shares information and updates on security practices. Earlier in 2021, we shared how we're helping to reshape the software supply chain ecosystem securely in the wake of the Solar Winds attack[5]. Beyond this specific attack, we outlined how we remain focused on defending against all forms of supply chain risk and feel a deep responsibility to collaborate on solutions that benefit our customers and the common good of the industry. Google has also recently announced a significant five year commitment to advancing cybersecurity, including helping to secure the software supply chain[6].

    Utilising existing (or new) international standards would enable Australian companies to benefit from improved supply chain management when it comes to the software supply chain. We've long advocated for securing the software supply chain[7] both through our internal best practices[8] and industry efforts that enhance the integrity and security of software. Google is currently collaborating with the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) to support and develop a new

---

[4] https://www.google.com/about/appsecurity/reward-program/

[5] https://cloud.google.com/blog/products/identity-security/how-were-helping-reshape-software-supply-chain-ecosystem-securely

[6] https://blog.google/technology/safety-security/why-were-committing-10-billion-to-advance-cybersecurity/amp/?utm_campaign=603f4a6c48788b0001538f13&utm_content=6126d344b15b0f00015e9462&utm_medium=smarpshare&utm_source=linkedin

[7] https://cloud.google.com/blog/products/identity-security/how-were-helping-reshape-software-supply-chain-ecosystem-securely

[8] https://cloud.google.com/blog/products/identity-security/applying-zero-trust-to-user-access-and-production-services

framework that will help to improve the security and integrity of the technology supply chain[9].

23. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

    Google is driven by a vision of invisible security - where security is engineered into products, making security controls easy to use. Enabling businesses to utilise security controls without needing special configurations or IT support teams can make it easier for small businesses to improve their cyber security posture and of course saves these businesses money.

    A health check, or similar mechanism, may be helpful to small businesses. Google Workspace customers have access to a checklist maintained by Google that assists small (1-100 employees) and medium (100+ employees) businesses in taking simple steps to protect accounts, file storage or other collaboration tools where they may not have existing IT support structures[10].

24. Is there anything else we should consider in the design of a health check program?

    As noted above, a simple, easy to use health check will be imperative for the adoption of a health check program for small businesses. Where and how the information is maintained will be important for small businesses, to ensure any information or materials remain current.

25. What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?

    None.

26. Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

    The review of the Privacy Act 1988 is underway however it would be premature to comment on the outcomes of this review.

---

9 https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/

10 https://support.google.com/a/answer/9211704?hl=en and https://support.google.com/a/answer/7587183?hl=en&ref_topic=7559287

27. What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights of consumers?

    [No response]

Yours sincerely,

Samantha Yorke
Government Affairs and Public Policy