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

google.com

By email: pjcis@aph.gov.au

We welcome the opportunity to provide this statement and to meet with the members of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) to discuss the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*.

Google is committed to the security of the internet

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 are committed to doing our part to keep users and customers, as well as Internet infrastructure more broadly, secure. We do this in part by contributing to international security standards, best practices, templates, developer tools, and other integrated solutions that make security stronger and easier to implement. And of course by offering secure services to our customers and users.

Protecting Google's users, and customers

Security is a cornerstone of our product strategy. We've spent the last decade building infrastructure and products that are secure by design and implement security at scale:

- Every day Gmail blocks more than 100 million phishing attempts and 15 billion spam messages that never reach our users and customers
- Gmail blocks more than 99.9% of spam, phishing attempts, and malware from reaching users
- Google Play Protect scans over 100 billion apps for malware and other issues.
- Every year we block billions of bad ads - on average 100 per second - through a combination of live reviewers and sophisticated software
- Safe Browsing on Chrome helps keep users secure from bad websites, automatically protecting more than 4 billion devices
- Our Threat Analysis Group identifies bad actors, warns our users about them, and shares intelligence with other companies and law enforcement officials

Strong cybersecurity practices start with developing a culture that values security. Starting in 2011, Google was one of the earliest adopters of enterprise-wide zero trust. Google's global implementation of zero trust for its entire workforce resulted in greater security and improved collaboration, productivity and innovation. We took the lessons learned, and many of the technical innovations that came from our own zero trust journey, and embedded them into the solutions we now make available to customers, e.g. BeyondCorp Enterprise.

Google employs a dedicated team of full-time security and privacy professionals as part of our software engineering and operations division. This team includes some of the world's foremost experts in information, application, and network security. Tasked with maintaining our defence systems, developing security review processes, building security infrastructure, and implementing the company's security policies, the team actively scans for security threats using commercial and custom tools, penetration tests, quality assurance (QA) measures and software security reviews.

Delivering security in the cloud

As a cloud pioneer, Google fully understands the security implications of the cloud model. Our cloud services are designed to deliver better security than traditional on-premises solutions and we are committed to delivering the most trusted cloud in the industry.

From custom-designed data centres to private undersea cables that transfer data between continents, we operate one of the world's most secure and reliable cloud infrastructures. This infrastructure is continuously monitored to protect customer data and keep it available. In the event of a disruption, platform services can be automatically and instantly shifted from one facility to another so that they can continue without interruption.

Google Cloud runs on a technology platform that is conceived, designed, and built to operate securely. Google is an innovator in hardware, software, network, and system management technologies. We custom-designed our servers, proprietary operating system, and geographically distributed data centres. Using the principles of "defense in depth," we've created an IT infrastructure that is more secure and easier to manage than more traditional technologies.[1]

We believe it is fundamentally important that the Bill recognise the shared responsibility model that exists between cloud service providers and their customers, and provide a framework of responsibility for 'security of the cloud' (the infrastructure, by the cloud provider) and 'security in the cloud' (of the workload or the data, by the customer).

We support the Government's overarching objectives in the Bill and believe that those objectives could be better met with amendments relating to the 'data storage or processing' sector

Amending the definitions for the 'data storage or processing' sector

We want to take the opportunity to reiterate the importance of ensuring the definitions for the sector are appropriate. Google considers the Bill should be amended to define the terms 'data processing' and 'data processing service', and define 'wholly or primarily' in the context of when an asset may be used with a data storage or processing service. These definitions should take into account the differences between the operation of physical infrastructure versus cloud services.

Enabling industry to respond to cybersecurity incidents as a priority

Threat analysis and incident response is a key component of Google's overall security and privacy program. We have a rigorous process for managing data incidents. This process specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of customer data.

Google's incident response program is managed by teams of expert incident responders across many specialised functions to ensure each response is well-tailored to the challenges presented by each incident.

We remain concerned with the proposed notification of cyber incidents provisions in the Bill because: (a) they focus on reporting of incidents rather than on containment and remediation; (b) requirements to report on vulnerabilities that have not yet been addressed can seriously undermine a system's security, and (c) the short time frame will require companies to sacrifice quality to achieve speed, resulting in premature, ill-informed, and faulty incident notifications that ultimately erode the value of all notifications.

---

[1] Defense in depth describes the multiple layers of defense that protect Google's network from external attacks. Only authorised services and protocols that meet our security requirements are allowed to traverse it; anything else is automatically dropped.

Google is concerned that the current thresholds would result in the initial reporting of events that are otherwise quickly proven to not be a threat or attack, and as such may divert scarce resources within the ACSC to review reports that may be something unrelated to a threat or vulnerability. Those in the government charged with reviewing the notifications may become overwhelmed with all this noise and not be able to readily distinguish between those that matter and those that are simply premature.

Google remains of the view that amendments should be made to the Bill as outlined in our initial submission.

Amending the application of the government assistance measures

Despite some limited safeguards in the Bill, we remain concerned that the powers contained in the government assistance provisions have the potential to significantly adversely affect providers that operate in multiple markets across the world, with globally planned, interconnected and operated infrastructure.

We outlined a number of concerns in our initial submission and make the following additional observations.

In nearly every situation, it will be better for government agencies to seek information from the customer of a cloud service provider, rather than going to the provider. The customer will likely have much better insight into and understanding of the significance and potential sensitivities of the information. Google provides its customers with access and tools to investigate incidents and report to government agencies. In rare situations where important customer data exists but is not available to the customer, Google can work with, and at the direction of, the customer in an attempt to recover the data so that the customer can share information with the government.

In the rare situations where the government has knowledge that a customer of Google has been targeted or victimised but doesn't know the identity of the customer, Google may be able to provide identifying information and a point of contact at the customer's business. This will allow the government to approach the customer directly. We consider the Bill should be amended to require this as a necessary process to be undertaken.

Other than identifying information, Google may have little insight into the customer's data, how it is structured, what it means or how it can be analysed. For example, an organisation may have multiple cloud service providers, custom software and on-premise services. A cloud service provider is not going to be aware of all of these other components of the customer's system. Knowledgeable personnel within the customer's business are needed for that. The government assistance powers that would enable ASD to effectively 'run' a cloud provider's system would simply not provide an adequate level of access to customer data. Rather, such powers would be best reserved for ASD to downstream cloud customers, as opposed to being directed to the cloud service provider.

In most other cases, each of the other CI verticals primarily cater to Australian entities (e.g. ports, water, retail, logistics) while 'data storage or processing' is both horizontal and inherently global. We strongly recommend that the PJCIS amend the Bill to restrict the use of these powers on those other critical infrastructure sectors that operate in a vertical, as opposed to horizontal, manner as outlined in our initial submission.

Similarly to the reasons outlined above, we strongly oppose the ability for the Australian Government to compel the installation of software on networks, systems, or assets. The ability to undertake such an action, particularly in the data storage and data processing sector, could have unintended consequences to customer privacy and security (business and citizens) in Australia, and around the world.

Such measures are likely to increase security and operational risks. The software that runs the cloud environment is highly sophisticated. Any third-party software has the distinct possibility of hindering the performance of the cloud environment and threatens the overall security and stability of the environment. For example, enabling ASD to install software on a provider's network, or within a customer's projects without an intimate understanding of the project itself (an understanding that only the customer would have) could be disastrous and would require testing and verification to avoid unintended consequences or negative impacts, including introducing vulnerabilities into a cloud provider's network.

For these reasons, we recommend that the Bill be amended to specify the system information software notice requirement does not apply to the data storage or processing sector.

The importance of collaboration to address cybersecurity risks

We welcome growing efforts by governments around the world to address cybersecurity challenges. Meaningful improvement in cybersecurity will require the public and private sectors to work together in areas like sharing information on cyber threats; developing a comprehensive, defensive security posture to protect against ransomware; and coordinating how they identify and invest in next-generation security tools.

Google works 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 Organization for Standardization (ISO), World Wide Web Consortium (W3C), and the Internet Engineering Task Force (IETF) as well as regional standards bodies.

We also maintain relationships with law enforcement agencies around the world and, when merited, share pertinent threat data. For example, Google's Threat Analysis Group, which works to counter targeted and government-backed hacking against Google and our users, regularly shares relevant threat information on government-backed campaigns with law enforcement and other tech companies with the goal of preventing and mitigating the damage of cyberattacks.

We welcome the opportunity to discuss our experience and our concerns with respect to the Bill with the members of the PJCIS.

Google Australia