Google Cloud cloud.google.com

George Cross
A/g Director - Data Security and Strategy, Technology Policy Branch
Digital and Technology Policy Division
Department of Home Affairs

By email: datasecurityandstrategy@homeaffairs.gov.au

24 June 2022

Dear Mr Cross

National Data Security Action Plan Discussion paper

Google welcomes the Australian government's ambition to develop a National Data Security Strategy and the possibility to share our views in this public consultation. We see tremendous benefit in using data-driven innovation and cloud technologies to boost Australian economic growth and facilitate new market opportunities for Australian businesses, large and small.

Google is committed to the security of the internet

Google Cloud's mission is to accelerate every organisation's ability to digitally transform and reimagine their business through data-powered innovation. We serve customers in over 200+ countries and territories, and have been providing cloud services to customers in Australia for many years. As a global business, we operate across 34 cloud regions, 103 zones and 147 network edge locations to service our customers around the world. This includes a Sydney Cloud Region that was launched in 2017, and the Melbourne Region launched in 2021.

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, and Internet infrastructure more broadly, secure. We do this in part by contributing to international security standards, sharing best practices, templates, developer tools, and providing other integrated solutions that make security stronger and easier to implement. And of course by offering secure services to our customers and users and implementing a shared fate approach to risk management rather than delineate where our responsibility ends.

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 implementing security at scale. By way of example:

- 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, and

- Safe Browsing on Chrome helps keep users secure from bad websites, automatically protecting more than 4 billion devices.
  .

At Google Cloud, our threat intelligence and cybersecurity teams are constantly on alert for potential threats to our customers, our systems, and the integrity of our platforms. Our approach is security that is built-in by default to our platforms through defence in depth layers and zero-trust principles to protect against the impact of malicious cyber activity, and eliminate entire classes of threats. In addition, we ensure the provenance of our software to minimise the risks of compromised supply chains.

We also **provide free versions** of our security protections and services to users and organisations around the world, including:

- **High-risk user protections**: Our Advanced Protection Program protects the accounts of high-risk users, including many journalists and activists. The program is free to enrol for any Google account user. We also provide free Security Checkup services to spot risky passwords and enrol our users in two-factor authentication automatically.
- **Cloud security visibility and controls**: Google Cloud offers a free version of our Security Command Center to help customers strengthen their security posture by evaluating their security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities and threats; and helping mitigate and remediate risks.
- **Open Source security:** Google continues to be one of the largest maintainers, contributors, and users of open source and is deeply involved in helping make the open source software ecosystem more secure through efforts including the Open Source Security Foundation (OpenSSF), Open Source Vulnerabilities (OSV) database, and OSS-Fuzz.
- **Anti-fraud tools**: The free tier of reCAPTCHA helps organisations defend their websites against cyberattacks like credential stuffing, account takeovers and scraping.

Building a common understanding

We share the following observations on the key topic areas raised in pages 18 to 21 of the National Data Security Action Plan discussion paper:

Cross-border data flows

Cross border data flows are important to global commerce. The free flow of information across geographic borders allows organisations to participate in the global economy. In contrast, data localisation requirements complicate or impede operations, could impact security and resilience, and ultimately increase the cost of doing business for organisations that operate across regulatory jurisdictions. The OECD guidelines, which focus on economic benefits derived from a data protection framework, strongly support the free movement of data. The OECD argues that restrictive data localisation requirements “affect firms’ ability to adopt the most efficient technologies, influence investment and employment decisions, increase the cost of innovation and lead to missed business opportunities.” Currently, Australia, Canada, Chile, Colombia, the EU, Japan, Mexico, New Zealand, Singapore, Switzerland, the United Kingdom, and the United States are among the many countries to endorse cross-border data transfers through public statements or international agreements.

Countries following the OECD approach have realised the economic benefit of cross border data flows. For example, a 2016 report by McKinsey Global Institute estimated that cross border data flows contributed $2.8 trillion to the global economy in 2014, and this figure is estimated to reach $11 trillion by 2025. On the contrary, data localisation laws can also negatively impact a country's gross domestic product (GDP). According to the Brookings Institution, a study by Bauer et al, the cost of proposed and enacted data localization measures in India, Indonesia, and Vietnam would reduce GDP in India (-0.1 percent), Indonesia (-0.5 percent), and Vietnam (-1.7 percent).

The ability to transfer data across borders also directly contributes to important policy objectives relating to the protection of privacy, security, and regulatory compliance. For example, in the context of financial services, the ability to transfer and analyse data in real-time across borders is critical to efforts to combat financial fraud, money laundering or other illicit financial transactions. Many cybersecurity tools that monitor traffic patterns, identify anomalies, and divert potential threats depend on global access to real-time data. Restricting the ability to monitor and analyse data in real-time can reduce an organisations' ability to speedily identify and respond to vulnerabilities and threats.

Digital trade rules

Australia has been a global leader in forging new digital trade rules, standards and norms that facilitate the growth of digital trade, including on cross-border data flows. The digital policy landscape is becoming increasingly fragmented — the Digital Policy Alert, for instance, has recorded over 1700 digital policy or regulatory changes across G20 and EU economies from 1 January 2020 to June 2022, with data governance-related policies as one of the most active areas of regulatory activity. Such fragmentation adds unnecessary friction and compliance costs, and disproportionately affects small businesses who are trying to scale globally through the use of digital technologies. Google therefore supports Australia's efforts to foster greater digital regulatory alignment and certainty through digital trade rules in bilateral agreements such as the Australia-Singapore Digital Economy Agreement, and via Australia's role as a co-convenor of the digital trade negotiations at the World Trade Organisation.

Data localisation

The Data Security Action Plan discussion paper expressly seeks input on whether Australia needs an explicit approach to data localisation. We respectfully submit that the desire to improve data security cannot be achieved by data localisation requirements: Google supports a free and open Internet that allows for frictionless cross-border data transfers while preserving privacy by encrypting data in transit and at rest by default across Google services and systems.

Security and privacy can be optimised when cloud-based services are free to leverage distributed network infrastructure without geographic restrictions. The physical location of data does not make it secure: what matters most are technological controls to ensure security and privacy, along with policies that ensure best practices are adopted.

Data localisation primarily refers to laws or policies, which are intended to keep data in-country. 'Data localisation' is the opposite of 'free flow of data across borders' which forms part of many free trade agreements, including agreements that Australia is a signatory to. Even where data localisation controls are applied, they have little effect over the privacy and security of data, which is ensured through controls applied to the data. In particular, data residency controls do not provide customers with control independence vis-à-vis the Cloud Service Provider (CSP). While data sovereignty controls allow the customer to be the arbiter of access to their data, data location simply assumes trust based upon the physical geo-location of the data or nationality of CSP employees.

Networks like Google's are global by nature, and imposing data localisation requirements could negatively impact resilience by reducing the availability of backups in disaster recovery scenarios. Furthermore, by particularising the provision of services from customer to customer and reducing the available workforce, these approaches are also likely to reduce the overall interoperability of services and portability of customer data, both of which help to ensure survivability and continuity of operations in exigent circumstances.

Availability, disaster recovery, and business continuity are an essential part of running a business or providing government services in today's digital economy. Unfortunately, earthquakes, hurricanes, floods, and other natural or human-made disasters are also an inevitable occurrence. Organisations will not survive if they do not have the ability to withstand and quickly recover from such events. Leveraging a globally distributed network like Google Cloud, which intelligently distributes data and applications through a geographically diverse network, enables businesses to confidently backup critical data and quickly recover and respond when disaster strikes. Laws, regulations or policies that require an organisation's data or applications to remain in one physical location dramatically increase the likelihood that a single catastrophic event will be insurmountable.

Similarly, data location does not ensure the privacy and security of customer data, and may actually work against these objectives. There are four critical ways in which forced data localisation requirements can undermine security of data in the cloud:

1. Location-based requirements are separate and distinct from efforts to implement stronger data security - data localisation in a single location does not inherently make the data more secure
2. Data localisation can make data more susceptible to attack - requiring data to be stored or processed in one location can make a specific data centre an attractive target for bad actors, and increase vulnerability to targeted cyber attacks
3. Data localisation laws may prevent some cloud customers from leveraging the benefit of cutting-edge security tools that rely on cross border data flows, and
4. Customers subject to data localisation requirements at an operational disadvantage because they cannot fully leverage tools to detect and prevent fraud, spam and other vulnerabilities.

Data localisation does not offer a solution against the application of foreign laws to the products and operations of service providers established in foreign jurisdictions. Foreign providers continue to be subject to their domestic laws relating to data disclosure and content removals no matter where they store the data. The CLOUD Act and U.S. surveillance laws apply to all providers established in the U.S. wherever they store the data.

The important role that cloud technology plays in today's economies, societies and governments has led to the development of advanced privacy and security solutions and policy proposals in Europe and elsewhere for providers to enable greater customer control over public cloud environments. Many policymakers want to empower the public and private sectors to take advantage of the expanded capabilities offered by the public cloud, while safeguarding privacy and data protection, among other priorities. They seek solutions that allow the customer to exercise greater control over data in public cloud environments and, thereby, engender greater trust in CSPs. They also emphasise the value of interoperability, including through open source and multi-cloud offerings, that enable domestic entities to simultaneously take advantage of foreign and local cloud offerings and ensure that the economic benefits of moving to the cloud are shared. For further information, see Google's white paper on Digital Sovereignty in the Cloud, and additional information on Google customer controls and open cloud solutions.

In developing a data security strategy, we strongly recommend that Home Affairs have regard to the utilisation of technical controls to uplift the security of data, rather than imposing data localisation policies which may have significant negative impacts on the adoption of technology in the Australian economy and otherwise undermine data security.

Government's role - federal, state and territory and municipal government uplift

Protecting the world's largest network against persistent and constantly evolving cyber threats is a preoccupation at Google Cloud. Our commitment to security underpins everything we do - from our platform, infrastructure, software solutions and purpose built hardware - including how we keep our customer data private - to how we enforce global standards that support compliance with internal policies and external regulations.

Alignment with international standards ensures best practices are utilised, promotes interoperability, and avoids introducing unnecessary and burdensome complexity. Wherever possible, any frameworks attached to a future data security strategy should be aligned to international standards and best practices. This avoids conflicting standards and reduces complexity for customers of technology services and for companies providing products or services to the Australian market. Importantly, it would also help Australian companies seeking to enter export markets to minimise development costs.

Clarity and empowerment for business

Empowering and educating citizens and consumers, and the community

We welcome growing efforts by governments around the world to address data security challenges. Meaningful improvement in cybersecurity will require the public and private sectors to work together in areas like sharing information on cyber threats: building a more integrated ecosystem to keep enterprises secure, developing a comprehensive defensive security posture to protect against ransomware and other cyber-enabled crime, and coordinating how they identify and invest in next-generation security tools. We run programs, like Safer with Google, and provide various additional resources.

We also work directly with business - our Google Cybersecurity Action Team has been working with a range of enterprise and public-sector customers, and partners around the world, to help advise on cybersecurity defences and operational preparedness. We will continue to provide these strategic advisory services and resources for security best practices to partners in government, critical infrastructure, and businesses of all sizes. This includes a security and resiliency framework to help customers protect themselves against adverse cyber events by using our comprehensive suite of security and resilience solutions.

Google also 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, other technology companies and are publicly available for anyone in the cyber security community, or elsewhere, to access with the goal of preventing and mitigating the damage of cyberattacks.

We welcome the opportunity to discuss our experience and to engage with Home Affairs as it considers the development of a data security strategy.

Yours sincerely

Stefanee Lovett
Government Affairs and Public Policy