Fastmail Pty Ltd
PO Box 234, Collins Street West 8007
Victoria, Australia

www.fastmail.com | @Fastmail

January 12, 2021

Fastmail welcomes the opportunity to participate in the review of the legislation governing the powers our law enforcement entities can use to identify and stop criminal activity.

Much of Australia's privacy legislation lags behind the pace of change of a globally connected society. We recognize the use of digital platforms to promote and coordinate crimes in progress, and the need for legislation to address that reality.

To prevent overreach, law enforcement seeking access to digital platforms should scale with the severity of the crime under investigation and have clear judicial review. Specific language will clarify use, and take steps towards improving Australia's reputation around digital rights.

About Fastmail

Fastmail is the world's oldest, independent email provider. Established in Melbourne, Victoria, in 1999, we are a privacy-focused email provider. Customers choose us over larger name services in part because of our values including our stance on treating customer data as private data that they own: we don't use it for direct or indirect commercial gain.

We process approximately three requests a month from law enforcement, of which 90% originate with foreign agencies, made through mutual assistance treaty via the Australian Federal Police. Just 10% are from Australian state and federal law enforcement.

Australia's position on the global stage

- Australia's global reputation for moving away from individual rights and more towards state level surveillance is increasing, thanks to TOLA and other bills like Surveillance (Identify and Disrupt).
- Currently, data surveillance laws are not really given effective oversight or public accountability. The Commonwealth Ombudsman’s report in 2019 on warrantless access to retained telecommunication data showed large scale inappropriate access, with an average of 1000 accesses to Australians’ data each day. This shows that Australia must increase our capacity for oversight and accountability, with sufficient rigor applied to seeking access: as the range and depth of these powers increases, the capacity for harm if used inappropriately also increases.
- We are concerned these changes will continue to damage Australia's reputation on the global stage. Australia already doesn't meet the criteria for adequacy under GDPR; legislation like the Identify and Disrupt Act, and the Attorney General's Privacy Act review make it harder for us to achieve adequacy, particularly in the wake of the Schrems II decision. Even as more countries are taking on GDPR-style protections, we are moving further away from global norms, and from the expectations of privacy protection that consumers are now demanding.

Reasonable and proportionate

- These changes deserve more rigorous protections to ensure that they are given oversight and targeted sufficiently. They grant immense power but are issued primarily under subjective discretion.
- This law rests on the use of "proportionate" and "reasonable" measures. These terms lack adequate definition and are deeply subjective. The same criticism levelled against the use of these terms for TOLA also applies here: any judge issuing warrants will err on the side of greater powers for police in the absence of any objective measures to define the degree of intrusion that might be appropriate for a given crime.
- Specifying a severity by length of penalty is in keeping with past acts and creates clarity for law enforcement and the judicial system. Companies, organisations, and citizens alike deserve certainty that private data is being accessed under consistent consideration, that the severity of the privacy intrusion matches the severity of the crime under investigation and that it has met with suitable review.
- When setting some guidelines of what is proportionate and reasonable, we'd encourage alignment between similar acts. To obtain data under the Surveillance Devices Act, the offense needs to be indictable, which carries a minimum penalty of 2-3 years. Under the Telecommunications (Interception and Access Act), the penalty minimum is 7 years of the suspected offense before interception of content is considered justifiable. The Identity and Disrupt powers are no less intrusive than the TIA: the criteria for the application of their powers should be similar. Better alignment between the various instruments helps everyone understand under what circumstances these intrusions are appropriate, reasonable, and proportionate.

Consultation process

- Where the target computer is not owned by the person suspected of the offense, we'd like to see a consultation process introduced. This gives the organisation providing the data the ability to advise about the consequential damages that might result from the warrant and give some guidance on more appropriate mechanisms to meet law enforcement's needs. Without this, there's nothing preventing law enforcement from compelling us to shut down our servers when they only need to target a single account, resulting in an immense compliance cost. Where urgency could be an issue, provide emergency clauses with clear guidelines to fast track this process for judicial approval.
- When considering consequential damages, we'd like to see built into the law, a requirement that incidental harm or loss be avoided or fully compensated, and/or an express right of compensation for all losses (not just property and personal injury) from all three kinds of warrants. This provides accountability and safeguards to proportionality that help protect law enforcement from accusations of overreach, while ensuring that businesses know that the impact of their compliance can be recognised.
- This bill as it stands, could have unforeseen flow-on effects further down the supply chain. For instance, if the popular accounting platform Xero (headquartered in NZ, but with offices in Australia) were to be disrupted, taken over, or shut down, then thousands of Australian businesses would have their operations interrupted. Consumer confidence would be shaken, with reputation damage far extending beyond the original suspect's operation. Providers of electronic services rarely operate in a vacuum.

Clarity over foreign usage

- We would like some consideration given to the capacity of these new powers to be used by foreign law enforcement entities. The Mutual Assistance of Criminal Matters Act and the Telecommunications Legislation Amendment (International Production Orders) Bill don't - and couldn't possibly, as they precede this bill - permit or deny the use of these new powers, but there's nothing in them that would obviously preclude the usage of these warrants on behalf of a participating foreign country.
- Could these new access powers be used by foreign powers to circumvent stronger data privacy protections in their own country?

Summary

We believe that building a set of specific guidelines about when these warrants are appropriate to use and aligning them with existing acts helps reduce confusion for both the law enforcement officials using these powers, and organisations beholden to comply.

The bill is not business-neutral. It produces a set of powers that have the capability to disrupt an organisation's operations with no consultation or recourse. While we believe there would not be any intention to cause such a disruption, building in a consultation process or incidental harm measures into the bill helps ensure that consumers and businesses across a supply chain are also considered.

Our laws do not operate in a vacuum: we have mutual assistance treaties in place around the world, with a streamlined version coming soon through the International Production Orders platform. An understanding of when these new disruption powers might be invoked by foreign agencies and how we ask them to demonstrate their request is reasonable and proportionate is also appropriate.

We look forward to the review taking into account concerns from industry and the wider community to keep our country safe, while recognising that this legislation can't come at the cost of compromising Australians' digital privacy, and Australian companies' ability to serve customers in jurisdictions with strong digital privacy rights.