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

www.fastmail.com | @FastMail

21 February 2019

ATTN: Parliamentary Joint Committee on Intelligence and Security

Dear committee,

Thank you for the opportunity to provide feedback on the "*Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018"* (TOLA), particularly regarding the impact it has had on our business, staff and customers since being passed.

Summary of key points in this submission:

- Many of the problems caused by this bill resolve around perception and trust. Australia's reputation as a country which respects the right to privacy has been damaged.
- Staff – both those developing software, and those responding to access requests – need clear guidance on what their legal responsibilities are and the scope of what they could be lawfully asked to do.
- The existence of capabilities in a system which are not documented, designed, and tested along with the rest of the system adds systemic weakness by definition – especially when those capabilities involve security and access control.
- It is not possible to reliably keep technical capabilities secret, and when they are inevitably exposed, it destroys trust and damages Australian firms.
- We don't have the expertise or authority to determine whether all requests are proportional or justified, which is why we strongly support judicial oversight.

About FastMail

We are an Australian company, employing staff in Australia and overseas. We provide hosted email services to a worldwide customer base, and are a net exporter with over 90% of our customers living outside Australia.

FastMail have always spoken proudly and clearly about how being an Australian company gives our customers world-class privacy protection. In a world in which many online companies sell insights into their customer base to subsidise services, we instead charge our customers money, and are their trusted partner.

Global trust in the quality of Australian Privacy Protection

The general public has a growing awareness of privacy issues in online platforms. Events over the past few years have made it to regular media: from coverage of the Facebook/Cambridge Analytica situation, wholesale data leaks (PageUp), the forced password reset on the federal government's own computer systems, or the way every service emailed updated privacy policies triggered by the EU's GDPR.

In this landscape, the way in which TOLA was introduced, debated, and ultimately passed into law creates a perception that Australia has changed — that we are no longer a country which respects the right to privacy.

Our customers are deeply concerned that they cannot trust the Australian government to properly manage, monitor and control the flow of access requests. They don't trust the government's technical capabilities (activities around the MyHealthRecord and Robodebt are sources for justification for this view.)

We have already seen an impact on our business caused by this perception. Our particular service is not materially affected as we already respond to warrants under the Telecommunications Act. Still, we have seen existing customers leave, and potential customers go elsewhere, citing this bill as the reason for their choice.

Developing software without introducing systemic weakness

Regarding TCNs, we are happy to add capabilities to provide data in a more usable format, or capture more useful data, to assist police in their work. However, we do not believe that it is technically possible to keep those capabilities themselves secret.

The downsides of attempting to do so can be seen clearly with the case of Yahoo, where a backdoor was discovered by their security team, only it turned out that a secret backdoor had been installed by management in response to a government request. This destroyed trust internally within Yahoo as well as among their customers, and key security staff left the company.

Our staff are curious and capable – if our system is behaving unexpectedly, they will attempt to understand why. This is a key part of bug discovery and keeping our systems secure.

Technology is a tinkerer's arena. Tools exist to monitor network data, system calls, and give computer users more observability than ever before. Secret data ex-filtration code may be discovered by tinkerers or even anti-virus firms looking at unexpected behaviour.

TOLA's requirements for secrecy put all companies which are built on a trusted relationship with their customers at risk. To conclude that additional capabilities built under TCN can be kept a secret, whether from staff or customers, is naive at best. When the capability is discovered, TOLA threatens criminal penalties for acknowledging that the capability even exists. This is incompatible with best practices for computer security.

- Just on a practical matter: distinguishing "work that's for a TCN" from "regular security and logging capability" changes is impossible. Particularly as code is refactored and products change over time, ensuring that a technical capability isn't lost means that everybody working on the design and implementation needs to know that the technical capability exists and take it into account.
- Any source code leak, or reverse engineering, could find the technical capability. Short of installing deliberately undocumented security holes (which the legislation claims to explicitly avoid), technical capabilities need to be documented, tested and maintained. This requirement particularly applies when those capabilities are part of the security perimeter of products.
- **The mere existence of capabilities which are not documented or tested along with the rest of the system is a systemic weakness.**

Thus, the existence of capabilities within the system can not be kept secret. If a technical capability is built, it is not feasible to guarantee that customers don't know that we have the capability, and a discovery in future that we had the capability would destroy all trust our customers have in us.

We strongly request that companies not be forced to keep technical capability requests secret. Keep the specific use of capabilities secret, but not the existence.

Impacts on Australian companies who export IT services

We anticipate a reduction in foreign investment for startups, as people refuse to put their money into a product that could be compromised without warning. We also anticipate that other Australian companies will find it more difficult to export their products or services to other countries.

We are regularly being asked by customers if we plan to move. In addition to affecting current businesses, this bill has a chilling effect on anyone who might be considering starting a business. Technology companies have a choice of location that bricks-and-mortar companies do not.

If Australians with great ideas choose to take their intellectual property to another country, it has a negative impact both by reducing future tax revenue and by depriving the technology community in Australia of another entrant.

Impacts on staff morale and employability of Australians

Our staff have expressed concerns that they may be forced to attempt to secretly add back doors or security holes in our service - actions that would be just cause for dismissal - and be unable to tell us why they have made these changes. We believe that practically speaking, no individual would be subject to a Notice; that the organisation would instead be targeted. But if this is the case, the law should be written to this exact intent rather than leave it to hoping that it will be handled reasonably when put into practice.

This is not just a matter of looking after our own staff's mental health, it also makes it harder for Australians looking to work for overseas companies if there is any risk that they will be compelled to act against their employer's interests.

By far the biggest concern for our staff is that they would inadvertently leak information about a capability that we had built in response to a TCN, possibly not even knowing that it was built for a TCN.

By not trying to keep the capabilities secret, the only thing staff would need to worry about is whether they mention specific warrants for specific users, and everybody is happy that they can avoid that.

Further, if the system's capabilities (TCN) are well documented, then activating those capabilities (TAN) can be restricted to a few key staff, and the process for using those capabilities can be handed over to new people as staffing changes over time.

Any secret capability (TCN) only known to some people causes "bus factor" headaches for management and is more likely to lead to process breakdowns and a lack of trust within teams.

Customer trust and statistics

There's really only one thing we would ask for here. The ability to publish overall metrics on how often capabilities had been activated, on something like a 6 month schedule and rounded to broad numbers, like:

"In the past 6 months we responded to [fewer than 50 / 50 - 200 / 200 - 500 / 500 - 2000 / over 2000] legitimate requests for access to data about our customers". Customers will otherwise assume the high end of this range, when the low end is in fact the truth.

At a larger scope, to retain Australia's position as a country that people trust on the topic of privacy, a higher level report should be produced about total usage of these capabilities. The AFP claim in (Sub 21 - TOLA Act.pdf) that it would require an unreasonable amount of manual labour. This act creates work for everybody. Perhaps the AFP could file a TCN on themselves to build out a technical capability to track the number of warrants they request.

Supporting law enforcement while remaining trusted

FastMail publish our values online for our customers: that we are loyal to our customers, that they own their data, that we are good custodians of their data, and that we are good internet citizens.

We believe in the rule of law, and part of being good citizens is assisting the police in their inquiries once they have provided due cause. We don't consider ourselves qualified to evaluate due cause, and support the concept of judicial oversight of police requests, and hence a process for verifying requests from our end being "is a valid warrant produced? If yes, respond - if no, request a warrant". That is a practical and implementable process.

We appreciate that sometimes the police need to find out information about a suspect without tipping that suspect off about the investigation. We are happy to provide data without informing the customer upon receipt of a duly authorised warrant to do so. Being requested to activate existing capabilities is a key part of assisting the police. We appreciate that sometimes the data needs to be captured in a hurry and are happy to expedite requests, so long as they are still receiving appropriate levels of judicial oversight.

We are happy to clarify anything in our submission which is unclear, and to assist you in formulating an improved bill to keep Australia safe, while keeping the law-abiding among our customers private, and our staff protected.

Sincerely,

Bron Gondwana
CEO, FastMail Pty Ltd
[redacted]