Oct. 12, 2018

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600
Australia

Re: Comments for Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunication & Other Legislation Amendment (Assistance & Access) Bill 2018

To whom it may concern,

We welcome the opportunity to provide input on the proposed Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018. We recognize the important role of government in the protection of citizens and their lawful activity on the internet, and appreciate the intentions underlying the step taken by the government to propose new powers for agencies to request and compel assistance in investigation of crime. However, we are concerned that the breadth and lack of clarity of the current draft legislation would result in a net loss for security and due process, and would introduce substantial international complexities impacting both developers and users of technology.

Mozilla believes very strongly in the value of the internet as a global, public resource. The value of the internet in stimulating economic activity, eliminating distance, and fostering human communications is immense. Mozilla is an international, mission-driven organization that develops tools that empower individuals on the internet, including the Firefox browser. Our commentary on the proposed bill is based on both our understanding of its potential impact on our mission, and on our analysis of how it would impact our products and technical work in practice.

Our comments concentrate on the three new powers for investigative and intelligence agencies provided by the bill:

1. A Technical Assistance Request (TAR) provides a framework for making requests of communications providers, including provisions that indemnify providers that voluntarily assist agencies.

2. A Technical Assistance Notice (TAN) allows agencies to compel communications providers to provide assistance, if they are able.
3. A Technical Capability Notice (TCN), which can only be exercised by the Attorney-General, compels communications providers to develop new capabilities in anticipation of a future TAR or TAN.

The interaction of the ability to request the development of new capabilities with existing government capabilities has far-reaching implications. These are complex issues that require more consultation and discussion than has been possible in the short time since this bill was first tabled.

While we believe that the challenges presented by the bill will affect many organisations, the long experience Mozilla has with open, community-based software development, together with our unique orientation as a mission-driven producer of technology with hundreds of millions of users, provides a viewpoint that we believe is relevant to the review of the bill.

Any measure that allows a government to dictate the design of internet systems represents a significant risk to the security, stability, and trust of those systems. Mozilla believes that TCNs or any similar device would significantly weaken the security of the Internet. Below, we've highlighted some of the risks that this produces.

Open-ended definitions for potential requests pose challenges for effective security and for technology development processes.

The bill as it stands does not provide sufficient limitations on the scope of potential requests to mitigate the challenges associated with these new powers. For example, with regards to TCNs, Section 317ZAA and similar provide only a loose description of areas that need consideration. We recognise the difficulty that tighter definitions would present, and understand that the bill specifically avoids defining what capabilities might be requested. Instead, the bill relies largely on the judgement of those involved to determine whether a given option is appropriate. In particular, we note that ministries responsible for consumer and business security are not required to be consulted, nor does there appear to be an inter-ministerial process for assessing the risks and interests associated with requests made under these new powers.

The bill is intentionally vague on the form and extent of what might be compelled by a TCN, so it is difficult to say what kinds of capabilities might be requested. We wish to emphasize that an under-specified authority to impose technical capabilities onto a software vendor not only introduces substantive problems through insufficient clarity, but also fails to provide certainty for both users and developers of technology.

Developing new capabilities, particularly those with security implications, is something that Mozilla does very carefully. Mozilla has extensive experience with the deployment and maintenance of security-critical features and systems. The systems we build routinely deal with highly sensitive information, so we take great care in the design of those systems.

In addition to following our principles regarding the use of information, we have learned through experience that successfully building new capabilities requires collaboration with a broad community. Mozilla prides itself in its open collaboration with a broad community on its projects, primarily because we believe that this is how we are most able to meet the high standard for security and privacy that we and our users expect. We also collaborate extensively with partners, competitors, and the research community. For instance, our ongoing response to the emerging class of speculative execution attacks on CPUs (known as Spectre) would not have been possible without extensive collaboration with other companies facing the same problem.

Against this backdrop, any governmental request for a single company to develop a capability - particularly one backed by a requirement of secrecy - runs counter to our established methods of technology development and contravenes the criteria we have established to make our development processes effective. Consequently, this risks making the output of our development less secure, in addition to the security risks that might be created by the capability in and of itself. In other words, complying is not as simple as just writing code - we would need new processes and operating models, and in deploying them would undermine the trust and community that we depend on for our core development.

Shipping compromised software is a risk to all users information.

A TCN is, in effect, an intentional introduction of a security vulnerability. We are concerned both about how such vulnerabilities would introduce significant and potentially widespread user and system insecurity. In addition to the risk to users from the nominally authorized use of the capabilities provided by the TCN, operating such a system in a way that prevents unauthorized use is inherently problematic, and has in the past been seen to lead to real compromises.

Most modern software includes automatic update processes. Automated updates are necessary to ensure that vulnerabilities can be fixed quickly and efficiently. If delivering modified software through update mechanisms is within the intent of the bill, then it creates an incentive for users to disable automated update processes, to preserve their trust and understanding of the software running on their machines. This leaves those systems vulnerable to attack and compromise. This might seem academic, but Mozilla has first-hand experience of how fragile trust can be.

At a very high level, any company that is able to run software on a computer is a potential threat to the integrity of any information that computer has access to. While steps have been made to isolate software from the actions of other software on the same computer, such protections are currently neither perfect nor uniformly implemented. As a result, the ability to run software without fear of unintended effects on the system as a whole depends greatly on trust in the provider of that software.

In this context, the list of possible targets in 317E is very broad. For example, under 317E(1)(e)(iii), a TCN could be used to cause the vendor of a traffic or weather information application to extract information from a messaging application.

The definitions of what can be requested dangerously lacks clarity. The assessment that might be conducted under 317W(7) is likely to be important in determining the answers to questions like this. However, we don't believe this to be an adequate safeguard.

Process limitations compound the practical negative consequences likely to arise.

Adding further to the practical uncertainty faced by technology companies from uncertain and unspecified potential requests, the lack of opportunities to challenge requests and to seek judicial review make cost and risk mitigation hard in practice. Under the bill as it stands, while providers must be consulted before being served a TAN or TCN, there is no avenue for them to object or an appeal an order. They’re also not permitted to disclose that they’ve received such an order, and they can be compelled to take steps to conceal any weaknesses that are introduced.

For an open source organization, which would need to close portions of its source code and/or release builds that are not made from its publicly released code bases, this is at odds with the core principles of open source, user expectations, and potentially contractual license obligations.

The breadth of scope introduces substantial international tensions.

We appreciate that the bill recognises that where activity occurs and where data is stored do not always follow jurisdictional boundaries. Yet, extraterritoriality provisions in law increase the cost and complexity of compliance across the entire industry, and put user expectations and trust at risk. And the broad definition of communications provider means that the bill grants Australian agencies the ability to make requests of software vendors anywhere on the planet, even if those vendors don't conduct business in Australia. If these provisions are enacted into law, they will not only pose problems in themselves, but will also set a concerning precedent for other countries who may demand similar exceptional access powers and assistance from companies, including those in Australia.

The limitation on systemic vulnerabilities is inadequate.

The key provision seeking to limit the widespread security risks of this bill is a prohibition on forcing companies to build a "systemic vulnerability" into their systems or to prevent them from rectifying a systemic vulnerability. However, the term "systemic" is not defined in the bill, leaving dangerous ambiguity that could be exploited by the government. The accompanying Explanatory Document provides some additional clarity but not confidence in stating that systemic vulnerabilities exclude "actions that weaken methods of encryption or authentication on a particular device."

The Government goes on to say that this legislation would permit "requir[ing] a provider to enable access to a particular service, particular device or particular item of software." For a company to enable this capability would effectively be to create a systemic vulnerability, whether the capability is provided by "one-off" upgrades sent to specific devices or by inserting a remote access capability to all versions of their products. In either case, the company will be left with a fast-path method to compromising their user's data, thus creating a high risk of compromise by malicious actors.

Other matters worth further consideration have been raised.

Others have noted factors that we believe require more consideration; We offer this nonexhaustive list of elements that we believe are worthy of further consideration:

- The interaction between new and existing capabilities with respect to Intercept Related Information (that is, metadata) requires more analysis. The accepted understanding of what IRI and content of communications is with respect to telephony might be well-understood, but the extent and complexity of the information exchanged over the Internet is not as easily subjected to classification of this sort.

- The effect of the bill on individuals and businesses outside of Australia is not sufficiently well-defined. For Australian businesses with foreign customers, this presents a risk to their operations.
- The civil liability protections associated with a voluntary Technical Access Request are not subject to the same limitations as other provisions.
- The definition of communications provider in 317C is too broad. We agree with other submissions that request making this definition clearer and more narrowly targeted.
- The list of acts in 317E is too broad. We agree with other submissions that request narrowing the acts that might be requested.
- The set of exclusions for "systemic weakness or systemic vulnerability" is too vague. We agree with submissions that request greater clarity about the intent and implementation of 317ZG.

Conclusion

A rush to enact legislation in the proposed form could do significant harm to the Internet. TCNs in particular present the government with capabilities that we don't believe are appropriate, as well as being a significant risk to the security of the Internet. The bill as proposed represents a one-sided view, without adequate consideration for the broader and longer-term costs and repercussions of its implementation.

Critical in evaluating risks and costs is the process by which the powers the bill grant agencies are safeguarded. The purposefully unclear definition of what can be requested, the secrecy provisions, and the lack of process and oversight are significant problems.

Mozilla believes that this bill will harm the ability of Australians and Australian companies to be competitive in the global industry created by the Internet. We recognise that information exchanged using Internet-based services can be critical to investigation and prosecution of crime, and the role that this plays in protecting society. Yet, as proposed, the bill provides powers that represent a real risk of harm to the Internet and additionally does not provide proper safeguards around the new powers it defines.

We ask Australia to join us in strengthening the security of the Internet, not weaken it.