December 30, 2019

To: Dr. James Renwick, CSC SC
Independent National Security Legislation Monitor
3-5 National Cct
BARTON ACT 2600
Australia

Thank you for the opportunity to provide a submission as part of your review of the Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018 (TOLA). This legislation grants sweeping and dangerous new powers to Australian law enforcement and intelligence agencies, and thanks to the foreign assistance provisions, extends these powers to foreign authorities as well. In doing so, this legislation raises grave concerns for the privacy and security of internet users and infrastructure in Australia and abroad. In this regard, your review is critical to highlighting and ameliorating the harms of this legislation.

Mozilla's mission is to ensure the internet is a global public resource, open and accessible to all. Our flagship product is Firefox, which is an openly developed and open source web browser used by hundreds of millions of people worldwide. The Firefox code base is also used for the Tor browser, which allows anonymous browsing. In addition to protecting the security of our products, Mozilla has influenced core security protocols used in the internet and backed the adoption of HTTPS, which encrypts website connections to enable more private and secure browsing. In addition, we have advocated to judges and policy makers in many countries on the importance of transparent and robust government processes to handle security vulnerabilities and surveillance requests.

As we noted in our submission to the Parliamentary Joint Committee on Intelligence and Security when this legislation was initially under consideration: "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."

To further your review of TOLA, we are pleased to attach the following submissions and comments we have made about this legislation as a series of addenda:

1. Our first submission to the Parliamentary Joint Committee on Intelligence and Security before the law's passage.
2. Our second submission to the Parliamentary Joint Committee on Intelligence and Security after the law's passage.
3. An opinion piece published in *The Australian* by Martin Thomson, a Distinguished Engineer at Mozilla and the Co-Lead of the Internet Architecture Board's Privacy and Security Program.
4. Our recent submission to the Ministry of Communications, Cyber Safety, and the Arts on their draft guidance on factors the Minister should consider when reviewing Technical Capability Notices.

We thank the INSLM for your thoughtful and thorough review of TOLA. This law represents an unprecedented and unchecked threat to the privacy and security of users in Australia and abroad, and we urge you to make recommendations to mitigate the egregious harms of this legislation as part of your review. Ultimately, we do not believe that this law should have been passed in the first place, and we believe the best possible path is to repeal this legislation in its entirety and begin afresh with a proper, public consultation. If you have any questions about our submissions or if we can provide additional information that would be helpful to your review, please do not hesitate to contact me.

Respectfully yours,
Jochai Ben-Avie
Head of International Public Policy
Mozilla Corporation
[redacted]

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.

February 22, 2019

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) Act of 2018

To the honorable members of the Committee,

Thank you for the opportunity to provide comment as part of your review of Telecommunication & Other Legislation Amendment (Assistance & Access) Act of 2018 (TOLA). This legislation grants sweeping and dangerous new powers to Australian law enforcement and intelligence agencies, and thanks to the foreign assistance provisions, extends these powers to foreign authorities as well. In doing so, this legislation raises grave concerns for the security of internet users and infrastructure in Australia and abroad, and fails to place appropriate limits on government surveillance. Given the serious threats to security and privacy posed by this Act, we welcome the Committee's review of this legislation and urge you to move swiftly to ameliorate its harms.

Mozilla's mission is to ensure the internet is a global public resource, open and accessible to all. Our flagship product is Firefox, which is an openly developed and open source web browser used by hundreds of millions of people worldwide. The Firefox code base is also used for the Tor browser, which allows anonymous browsing. In addition to protecting the security of our products, Mozilla has influenced core security protocols used in the internet and backed the adoption of HTTPS, which encrypts website connections to enable more private and secure browsing. In addition, we have advocated to judges and policy makers in many countries on the importance of transparent and robust government processes to handle security vulnerabilities and surveillance requests.

As we noted in our submission to this Committee when this legislation was initially under consideration: "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."

We do not believe that this law should have been passed in the first place, and we believe the best possible path is to repeal this legislation in its entirety and begin afresh with a proper, public consultation.

While it is our absolute preference that this legislation be abandoned and annulled, we recognize that the political will may not exist to take this action to protect the security of all Australians. To that end, in the remainder of our submission, we focus on a series of amendments that could be offered to avoid some of the most dangerous consequences of this law on the security of the internet.

In order of priority, we urge the Committee and the Australian Parliament to, at a minimum, make the following changes:

1. **Clarify that Australian authorities cannot target an employee of a Designated Communications Provider.**
2. **Remove restrictions on disclosure of Technical Assistance Requests, Technical Assistance Notices, and Technical Capability Notices.**
3. **Require judicial approval of Technical Assistance Notices and Technical Capability Notices.**
4. **Modify the assessments mechanism to ensure an impartial review which considers all rights and interests.**
5. **Require all requests not to disproportionately harm the rights and interests of users not under suspicion.**
6. **Clarify that "systemic weakness" includes any weakness in an individual communications system available to more than one person.**
7. **Limit the delegation of powers in TOLA.**
8. **Impose critically missing limitations on providing assistance to foreign authorities and extraterritorial use of these powers.**

We provide additional detail and recommendations on each of these points below. We look forward to engaging with the Committee as you conduct this critical review of TOLA. If you have any questions about our submission or if we can provide other information that would be helpful to the Committee as part of your review, please contact Mozilla Senior Global Policy Manager Jochai Ben-Avie at [redacted]

1. Clarify that Australian authorities cannot target an employee of a Designated Communications Provider

Due to ambiguous language in TOLA, one could interpret the law to allow Australian authorities to target employees of a Designated Communications Provider (DCP) rather than serving an order on the DCP itself through its General Counsel or an otherwise designated official for process. It is easy to imagine how Australian authorities could abuse their powers and the penalties of this law to coerce an employee of a DCP to compromise the security of the systems and products they develop or maintain. In order to ensure due process, appropriate diligence, and full compliance where appropriate with orders issued under this legislation, we strongly believe that Australian authorities should only serve an order on the DCP itself. Serving an order on an individual employee rather than a DCP itself would fail to allow a DCP to avail itself fully of the protections afforded under this legislation in regards to consultations, assessments, and legal challenges. Further, this potential would force DCP's to treat Australia-based employees as potential insider threats, introducing another vector for compromise that could undermine trust in critical

products and incentivizing companies to move critical roles to other localities. Parliament recognized the wisdom of this limitation in regards to Contracted Service Providers, but not DCPs.

We recommend the Committee: ADD a clarification in the Section 317B definition of Designated Communications Provider to specify that this term "does not include a person who performs such services in their capacity as an employee, agent, or vendor of the provider."

2. Remove restrictions on disclosure of Technical Assistance Requests, Technical Assistance Notices, and Technical Capability Notices.

As an open source company, we are committed to developing our products and services publicly. More than just a philosophical choice, open source development allows myriad actors outside of Mozilla to identify bugs in our code, and in doing so making our products and services more resilient and secure. This benefits the hundreds of millions of people who use Mozilla products every day. Developing in the open also allows our users to have more trust in the integrity of our code. The restrictions on disclosure in TOLA around building backdoors and other "acts and things" that may be required under the law are not just antithetical to us an open source company but would undermine the security and trust of all of our users.

When the US FBI in 2016 sought to force Apple to develop new software to undermine the security of its systems in order to gain access to an encrypted iPhone, this debate played out in the public eye. This allowed security experts, civil society, other companies, and elected representatives to weigh in on the risks of this order. Yet, if the Australian government were to use their new powers under TOLA today, we wouldn't know about it, because the law contains strict restrictions on disclosing information about any orders that are issued. Moreover, neither the orders issued under TOLA nor the limitations on talking about them have to be approved by a judge. This effectively prohibits the much-needed conversation about the appropriate limits of government surveillance as well as use of exploits that undermine the security of internet users, products, and services.

Secrecy should not be the default. If the government believes that secrecy is required in order to protect the integrity of an investigation or operation, they should have to seek an additional approval from a court of relevant jurisdiction. The Government should have to periodically justify to the court why the continuation of a restriction on disclosure is warranted, and all orders should become public eventually. While we understand that there may be a need for secrecy around the use of TARs and TANs because disclosure may alert the target of an investigation or operation, the same cannot be said of TCNs. Given that TCNs need not be tied to a specific target, operation, or investigation, there is no comparable need for restrictions on disclosure. TCNs designed to ensure that a DCP is capable of giving help could theoretically be used against any user, the vast majority of whom are not and will not ever be under suspicion. While we don't believe Australian authorities should have these powers given the profound security and privacy risks, we believe the government should have to make the case for these capabilities in the public eye. TCNs should never be secret.

We recommend the Committee: DELETE Sections 317ZF (1).

3. Require judicial approval of Technical Assistance Notices and Technical Capability Notices.

Not only does TOLA grant sweeping powers to Australian authorities, the law is made even more dangerous by the lack of judicial review. Around the world, laws authorizing surveillance operations often require an impartial, independent review by a judge. This is an important check on the power of the government to invade the privacy of individuals, ensure policies and procedures are followed, and limit the adverse impacts by government agents. By cutting judges out of the process, this bill is creating dangerous potential for abuse and avoiding a key safeguard found in most democratic countries. Especially considering the severe security risks posed by Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs), it is critical that a truly neutral arbiter review these orders and review challenges from DCPs when they feel an order is unlawful or unconstitutional.

We recommend the Committee: ADD language requiring all TANs and TCNs to be reviewed and approved by a court of relevant jurisdiction. Any variations to a TAN or TCN or limitations on disclosure should similarly be reviewed and approved by a competent judicial authority.

4. Modify the assessments mechanism to ensure an impartial review which considers all rights and interests.

Sections 317WA and 317YA provide DCPs with the ability to request an assessment of whether a proposed TCN should be given or whether a variation of TCN would contravene Section 317ZG respectively. As currently formulated, upon receiving such a request, the Attorney-General must appoint two assessors. However, the Attorney-General in these cases is far from a disinterested party, and this procedure risks allowing the government to appoint biased assessors who will unduly favor the interests of law enforcement and intelligence agencies. Given the significant security risks posed by TCNs and TANs, we strongly believe that assessments should take into consideration all of the relevant risks and interests.

Many countries, notably the US, UK, Germany, and the Netherlands, have established inter-ministerial processes for reviewing vulnerabilities that these governments learn about with the purpose of deciding whether to disclose a vulnerability to the affected vendor immediately or to delay disclosure. These government vulnerability disclosure review groups are composed of representatives from across government, including departments with government security, business security, and human rights missions. Diverse representation from across government, combined with an established set of criteria that must be considered in each case,[1] not only ensures that all rights, risks, and interests will be considered but allows these determinations to be made with the benefit of the full breadth of expertise that exists across government. Given the stakes, this decision should not be made by the Attorney-General alone.

In the context of TOLA, we would recommend a two-part process. First, assessments should be conducted by an inter-ministerial review group whose members include departments with government,

[1] See Annex B of the Charter of the Vulnerabilities Equities Policy and Process for the United States Government: https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

business, and consumer security missions. A set of criteria should be articulated by Parliament which establishes the minimal set of criteria for assessing the necessity and proportionality of every TAN and TCN that is issued. The inter-ministerial group should produce an assessment reflecting the views of all members. The inter-ministerial group should further be required to consult the affected DCP as part of conducting this assessment. As is currently required by TOLA, a copy of the assessment should be provided to the DCP.

Second, this assessment should be submitted to a court of relevant jurisdiction for a determination on whether a TAN or TCN should be issued. Given that the assessment will ultimately reflect the views of the government, the affected DCP should also be permitted to present a concurring or dissenting report to the judge who will rule on whether a TAN or TCN should be issued.

We recommend the Committee: AMEND Sections 317WA and 317YA and ADD a new section in regards to assessments of TANs which establishes an inter-ministerial group to assess whether TANs and TCNs should be given or variances approved. This inter-ministerial group should be required by statute to include departments with government security, business security, and human rights missions. A set of criteria which must be considered by the inter-ministerial group in each assessment should be established in statute. As is currently required by TOLA, the DCP should be consulted as part of the assessment, and a copy of the assessment report should be provided to the DCP. The assessment should be submitted to a court of relevant jurisdiction for a final determination, and the DCP should also be allowed to submit a concurring or dissenting report to the judge.

5. Require all requests not to disproportionately harm the rights and interests of users not under suspicion.

TOLA contains many provisions requiring TARs, TANs, TCNs, and variations to these orders to meet certain tests of reasonableness and proportionality (e.g., 317JC, 317RA, 317TAAA, and 317V). However, these tests are woefully insufficient. In particular, these sections call on the relevant Australian authorities to "have regard to… the legitimate expectations of the Australian community relating to privacy and cybersecurity." It is not clear what these expectations are, what expectations the government would consider legitimate and illegitimate, who constitutes the Australian community, or who would make these determinations. Even if all of this information can be ascertained, it is not enough to merely have regard for these expectations, the rights of all users affected by orders issued under TOLA must be considered. The law should require that law enforcement and intelligence agencies authorized under this law to demonstrate that:

- The order does not disproportionately harm the rights and interests of users, especially those individuals who are not under suspicion;
- The order is necessary for the legitimate purposes of a specific investigation or operation, and narrowly tailored to meet this aim;
- There is a high degree of probability that a serious crime has been or will likely be carried out; and
- Information accessed will be confined to that which is relevant and material to the serious crime or specific threat under investigation.

We also note with concern that TOLA requires relevant authorities to consider the "the *legitimate interests* of the designated communications provider to whom the request relates" and the "*legitimate expectations* of the Australian community relating to privacy and cybersecurity" but only requires consideration of the "*interests* of national security" and the "*interests* of law enforcement." While it is unclear what Parliament intended in making this distinction, it certainly appears to set a lower standard for consideration of the interests of the government vis-a-vis the people and companies these orders would affect.

We would also commend for the Committee's attention the International Principles on the Application of Human Rights to Communications Surveillance[2] also known as the Necessary and Proportionate Principles. These Principles have been endorsed by more than 400 international civil society organizations, and Navi Pillay, the former UN High Commissioner for Human Rights has stated in her landmark report *The Right to Privacy in the Digital Age*[3] that they can be considered persuasive interpretive guidance of Article 12 of the International Covenant on Civil and Political Rights (ICCPR) which Australia is a signatory to.

We recommend the Committee: AMEND the tests for reasonableness and proportionality in Sections 317JC, 317RA, 317TAAA, and 317V to require law enforcement and intelligence agencies authorized under this law to demonstrate that:

- ***The order does not disproportionately harm the rights and interests of users, especially those individuals who are not under suspicion;***
- ***The order is necessary for the legitimate purposes of a specific investigation or operation, and narrowly tailored to meet this aim;***
- ***There is a high degree of probability that a serious crime has been or will likely be carried out; and***
- ***Information accessed will be confined to that which is relevant and material to the serious crime or specific threat under investigation.***

We also recommend the DELETION of the word "legitimate" in regards to the interests of the designated communications provider to whom the request relates and the expectations of the Australian community relating to privacy and cybersecurity.

6. Clarify that "systemic weakness" includes any weakness in an individual communications system available to more than one person.

We welcome the amendments made to TOLA when the law passed further limiting Australian authorities from requiring the creation and preventing the patching of systemic weaknesses and vulnerabilities. However, there is substantial and concerning ambiguity around the law's definition that a systemic weakness or vulnerability "affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person." It is entirely unclear what constitutes a "class of technology." Is the Firefox browser a class of technology unto itself? Certainly, it seems contrary to the spirit of this limitation to allow Australian authorities to

[2] https://necessaryandproportionate.org/
[3] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

compromise the security of the hundreds of millions of Firefox users who have never been under suspicion of any wrongdoing. We believe this vital protection could be further strengthened by clarifying that a systemic weakness or vulnerability applies to an exploit that affects any individual product, service, or system available to more than one person.

We recommend the Committee: AMEND the definitions of "systemic weakness" and "systemic vulnerability" in Section 317B to say: "systemic vulnerability/weakness means a vulnerability/weakness that affects the product, service, or system used by more than one individual, but does not include a vulnerability that is selectively introduced to one or more target technologies specific to a particular person."

7. Limit the delegation of powers in TOLA.

TOLA provides Australian authorities with serious and unprecedented powers to undermine the privacy and security of users all over the world. We do not believe these powers should have been authorized in the first place, but certainly they should not be treated lightly. The more people who have the power to issue TARs, TANs, and TCNs, the greater the chance there is that these powers will be abused. Providing these powers to any police officer in Australia is irresponsible, risks the dangerous overuse of TOLA's powers, and in doing so demonstrates a cavalier attitude toward the privacy and security of users in Australia and abroad. The Australian Parliament could substantially reduce the potential for abuse of TOLA by requiring the approval of a senior official in order to issue a TAR, TAN, or TCN.

We recommend the Committee: AMEND Sections 317ZN, 317ZP, 317ZQ, and 317ZR to require the approval of the Director General of Security, the Director General of the Australian Secret Intelligence Service, the Director General of the Australian Signals Directorate, or the chief officer of an interception agency. Further delegation of powers should explicitly not be permitted.

8. Impose critically missing limitations on providing assistance to foreign authorities and extraterritorial use of these powers.

While the new powers that TOLA grants to Australian authorities would be deeply damaging to user security even if they were limited to Australia, TOLA dangerously extends the use of these powers to foreign governments with utterly insufficient safeguards. In particular, TOLA fails to require that requests by foreign countries to Australian authorities to use the powers granted by TOLA are:

- Not disproportionately harmful to the rights and interests of users, especially those individuals who are not under suspicion;
- Necessary for the legitimate purposes of a specific investigation or operation, and narrowly tailored to meet this aim;
- Only issued when there is a high degree of probability that a serious crime has been or will likely be carried out;
- From countries that have strong human rights and due process protections enshrined in law;
- Not used to evade the legal protections of the target as well as those not under suspicion in the requesting country; and
- Related only to an offence that is considered a serious crime in both Australia and the requesting country.

Furthermore, there are no limitations on which countries may request the assistance of Australian authorities. This leaves far too much discretion to the government. Again, we do not believe that Australian authorities should have these powers, and we certainly do not believe that foreign governments should effectively be granted these powers just by asking their Australian counterparts. Parliament and the public should have a say in determining which countries may make use of TOLA's powers. Given the grave potential for abuse with these foreign assistance requests, TOLA must also be amended to bring more transparency to how foreign governments are using these powers.

At the same time, TOLA currently allows Australian authorities to indiscriminately use their powers anywhere in the world. This not only exponentially increases the security and privacy risks posed by this legislation but also violates the sovereignty and legal protections of other countries. The extraterritorial reach of TOLA could also set a dangerous international precedent, and could in turn be used to justify operations by a foreign government seeking to engage in extraterritorial operations that would violate the rights of Australians.

We recommend the Committee: AMEND TOLA to require that requests by foreign countries to Australian authorities to use the powers granted by TOLA are:

- ***Not disproportionately harmful to the [privacy and security] rights and interests of users, especially those individuals who are not under suspicion;***
- ***Necessary for the legitimate purposes of a specific investigation or operation, and narrowly tailored to meet this aim;***
- ***Only issued when there is a high degree of probability that a serious crime has been or will likely be carried out;***
- ***From countries that have strong human rights and due process protections enshrined in law;***
- ***Not used to evade the legal protections of the target as well as those not under suspicion in the requesting country; and***
- ***Related only to an offence that is considered a serious crime in both Australia and the requesting country.***

We recommend the ADDITION of a provision which would require a public consultation and the explicit approval of Parliament before any country is allowed to request assistance from Australian law enforcement and intelligence agencies.

We recommend the ADDITION of a provision requiring the Attorney-General to publish a transparency report at least once every six months which provides aggregate statistics on:

- ***How many times assistance was requested under TOLA;***
- ***The nature of the crimes alleged in the requests;***
- ***The proportion of requests where Australian authorities actually provided help;***
- ***The nature of the acts or things that a DCP was ordered to do; and***
- ***The usage of different legal instruments (e.g., TARs, TANs, TCNs, computer access warrants, etc).***

These statistics should be broken down by country and the requesting agency within each country.

Finally, we recommend the ADDITION of a provision in TOLA prohibiting the use of these powers outside the territorial borders of Australia.

We thank the Committee for your diligent review of TOLA. This law represents an unprecedented and unchecked threat to the privacy and security of users in Australia and abroad. We urge the Committee and the Australian Parliament to move swiftly to remedy the significant harms posed by this legislation. Ultimately, the best course of action is to repeal this law and start afresh with a proper, public consultation. We remain at your disposal if there's other information that we can provide that would assist in your review of this dangerous law.

Respectfully submitted by:

Alan Davidson
Vice President of Global Policy, Trust, and Security
Mozilla Corporation

Jochai Ben-Avie
Senior Global Policy Manager
Mozilla Corporation

THE AUSTRALIAN

Access act robs users of privacy, security

By **MARTIN THOMSON**
12:00AM FEBRUARY 19, 2019 • 2 COMMENTS

At the end of last year, Australia's parliament hurriedly passed a law that will make us all less secure.

The Access and Assistance Act, now under review by parliament, gives the government new powers to weaken the encryption systems that keep our online communications, banking and browsing secure.

While the government acknowledges that breaking encryption is dangerous, this legislation provides law enforcement the means to weaken security measures that keep information safe. There is an observation that breaking encryption is much harder than the Five Bs: burglary, bribery, bludgeoning, blackmail, and bugs. The - Access and Assistance Act adds a sixth B: backdoors.

This law gives Australian law enforcement and intelligence agencies the powers to:

Force the maker of a phone to install devices or software that record private text messages, photos and voicemails, then have that data sent to the agency;

Force a messaging app to secretly add law enforcement agents to your private chats without your knowledge; and

Force a company to turn on the microphone and camera on your laptop or log all of your keystrokes.

As a principal engineer at Mozilla, I work on a team that develops and maintains network security software that protects the online activity of hundreds of millions of people around the world. Securing that code requires vigilance and constant effort.

In software, every line of code is a potential bug, and every bug is a vulnerability the bad guys could exploit.

It is impossible to avoid bugs in software, and we constantly find and fix new security vulnerabilities.

It's hard enough to do this when the government isn't trying to build backdoors, and security experts widely agree that ensuring a backdoor is accessed only by the right people under the right circumstances is impossible.

But I have a more selfish concern about bugs in backdoors. A system with a backdoor is more complex than one without. Adding code for a backdoor means more opportunities for complicated bugs.

In addition to the risks associated with controlling access to the backdoor itself, new code interacts with existing code in ways that might produce other, unintended vulnerabilities.

Industry wide, there are multiple major security incidents reported almost daily.

What is most sobering is that as a result of these incidents, people lose money, their jobs and their identities. I work hard every day to ensure that it's not my code, my bug, which is the cause of that sort of trouble.

In my role as lead for the Internet Architecture Board Privacy and Security Program (IAB), I've been involved in efforts to map out longer term improvements to online security.

The introduction of this legislation means we need to more profoundly question the trust infrastructure of the web.

When this legislation was first under review, the IAB's statement to parliament highlighted how trust is a critical component of our system of defences.

Our safety online requires being able to trust that the hardware and software we use is not acting against our interests.

Major software companies consider the security of supply chains and updates very seriously, but it is difficult to ensure that the processes they follow effectively prevent backdoors or malware from being added.

This is exactly the situation that this legislation exploits.

Securing software updates is another hard problem that the technical community is only just starting to come to terms with. Right now, the industry relies on people trusting that updates provide only new features and security fixes.

Having governments legislate means of undermining or circumventing safeguards undermines that trust and makes an already difficult job harder.

When the FBI in sought to force Apple to help break into an iPhone, this debate played out in public. If the Australian government were to make the same request of Apple today, we wouldn't know about it because the law contains strict limitations on disclosing information about these orders.

The law also allows foreign law enforcement and intelligence agencies to request help from the Australian authorities.

The gag orders apply to foreign requests as well, so we wouldn't know if the FBI in the US or GCHQ in Britain had asked their Australian counterparts to use these new powers.

What is most disappointing is that our politicians have chosen to give law enforcement and intelligence agencies offensive capabilities, when a paltry effort has been put into strengthening defences.

Proactive prevention of crime and ensuring the safety of all Australians is important, but the government seems determined to instead concentrate on granting agencies reactive and destructive capabilities.

This legislation makes the internet and all Australians who rely on it less secure.

Fortunately, this legislation is currently under review, a condition of it passing without adequate public consultation.

Even though the law has passed and is already being used, amendments are still possible as this stage.

As they return to work, MPs should consider how they might legislate to improve the security of all Australians.

Martin Thomson is principal engineer at Mozilla and program lead of the Internet Architecture Board Privacy and Security Program.

December 23 2019

To the Honourable Minister for Communications, Cyber Safety and the Arts Paul Fletcher
Department of Communications and the Arts
GPO Box 2154
Canberra ACT 2601
Australia

Thank you for the opportunity to provide comment on your draft guidance on the consideration of requests for Technical Capability Notices (TCN) by the Minister for Communications, Cyber Safety, and the Arts. This guidance is an important and useful starting point for placing appropriate limits on perhaps the most significant and even potentially harmful new power under the Telecommunication & Other Legislation Amendment (Assistance & Access) Act of 2018 (TOLA). This legislation grants sweeping and dangerous new powers to Australian law enforcement and intelligence agencies, and thanks to the foreign assistance provisions, extends these powers to foreign authorities as well. In doing so, this legislation raises grave concerns for the security of internet users and infrastructure in Australia and abroad. In this regard, thoughtful and thorough review of TCNs by the Minister for Communications, Cyber Safety, and the Arts is critical.

Mozilla's mission is to ensure the internet is a global public resource, open and accessible to all. Our flagship product is Firefox, which is an openly developed and open source web browser used by hundreds of millions of people worldwide. The Firefox code base is also used for the Tor browser, which allows anonymous browsing. In addition to protecting the security of our products, Mozilla has influenced core security protocols used in the internet and backed the adoption of HTTPS, which encrypts website connections to enable more private and secure browsing. We have also advocated to judges and policy makers in many countries on the importance of transparent and robust government processes to handle security vulnerabilities and surveillance requests.

As we noted in our submission to the Parliamentary Joint Committee on Intelligence and Security when this legislation was initially under consideration: "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."

We do not believe that this law should have been passed in the first place, and we believe the best possible path is to repeal this legislation in its entirety and begin afresh with a proper, public consultation. Acknowledging that the political will may not exist to do this, this draft guidance on the factors that the Minister should consider when reviewing a TCN order is still a useful check on the powers of Australia's law enforcement and intelligence services.

In many respects, the draft guidance offers a strong foundation. We commend you and your staff for including a number of valuable factors, in particular, your articulation of the legitimate interests of the designated communication provider (DCP) and the impact on the efficiency of business. However, we believe there are several additional considerations as well as

clarifications on the Minister's interpretation of TOLA which could further strengthen this guidance and position the Minister's review as a more substantive check on the harms TCNs may pose.

In this submission, we provide comments and recommendations on the following topics:

- Consideration of privacy, civil rights, reasonableness, and proportionality;
- Consideration of the harm TCNs pose to Designated Communications Providers' reputations and user trust;
- Consideration of whether a TCN is the least intrusive means possible for achieving Australian authorities' objectives and whether other investigative means have been exhausted;
- Consideration of the terms and conditions for giving help;
- The definition of a Designated Communications Provider;
- The imposition of limits on disclosure of TCNs;
- The definition of Systemic Weakness; and
- Limitations on providing assistance to foreign authorities and extraterritorial use of these powers.

The inclusion of these recommendations in the final iteration of the guidance that will be relied on by the Minister when assessing TCNs would go a long way to preventing the gravest dangers posed by TCNs. Moreover, the overbreadth of the law, particularly the disproportionate impact on innocent individuals, will in part materialize as harm to the reputations, efficiency, and competitiveness of individual communications providers, motivating inclusion of these factors in your analysis. We look forward to engaging with your office as you finalize this guidance. If you have any questions about our submission or if we can provide additional information that would be helpful to your office, please contact Mozilla's Head of International Public Policy Jochai Ben-Avie at [redacted]

Consideration of privacy, civil rights, reasonableness, and proportionality

We note with concern that the draft guidance abdicates responsibility for assessing the privacy, civil rights, reasonableness, and proportionality to the Attorney-General. Endangering the privacy and civil rights of users, especially the countless millions of people who have not and will never be suspected of a crime, by the disproportionate and unnecessary use of a TCN are some of the gravest threats posed by this provision. For example, a TCN requiring Mozilla to modify components of Firefox would undermine the privacy and security of hundreds of millions of innocent users of our software.

Moreover, the Attorney-General is far from an impartial or disinterested party when considering the use of TCNs. The Minister of Communications, Cyber Safety, and the Arts was specifically empowered by Parliament in TOLA to act as an additional check on TCNs approved by the Attorney-General. As your ministry offers a unique and valuable perspective on these issues, it would be a serious omission for the Minister not to consider these harms in his review.

TOLA contains many provisions requiring TCNs, and variations to these orders, to meet certain tests of reasonableness and proportionality (e.g., 317TAAA and 317V). While we believe that these tests should have been more carefully articulated in legislation, it is clear that the intent of that legislation is to offer the minister discretion in their implementation. The role of guidelines in this therefore becomes critical. In particular, these sections call on the relevant Australian authorities to "have regard to… the legitimate expectations of the Australian community relating to privacy and cybersecurity." It is not clear what these expectations are, what expectations the government would consider legitimate and illegitimate, who constitutes the Australian community, or who would make these determinations. Even if all of this information can be ascertained, it is not enough to merely have regard for these expectations, the rights of all users affected by orders issued under TOLA must be protected.

WE RECOMMEND the Minister only approve TCNs if* inter alia *all of the following conditions are met:

- ***The TCN does not disproportionately harm the privacy, security, and civil rights of users, especially those individuals who are not under suspicion;***
- ***The TCN is necessary for the legitimate purposes of a specific investigation or operation, and narrowly tailored to meet this aim;***
- ***There is a high degree of probability that a serious crime has been or will likely be carried out;* and**
- ***Where information accessed will be confined to that which is relevant and material to the serious crime or specific threat under investigation.***

Consideration of the harm TCNs pose to Designated Communications Providers' reputations and user trust

Distinct from the privacy and security impacts that could occur from a TCN, forcing a DCP to modify its products or services also risks a loss of user trust and potentially irrevocable damage to a DCP's reputation. Many companies, Mozilla in particular, rely on consumer trust; trust is the lifeblood of commerce. It is one of the single most important factors of whether a company can effectively compete in the market.

Put another way, one negative news cycle can forever damage a company's reputation and their relationship with their users. Research shows that consumers are already leaving brands that suffer a data breach.[1] People are unlikely to use products and services they know are vulnerable. Additionally, people are likely to feel betrayed if they find out that a company that they entrusted their data to has secretly worked with the government to undermine their privacy and security. The Australian Home Affairs Department has dismissed the concerns of companies opposed to TOLA by saying that the legislation provides that they'll be compensated for any costs incurred.[2] No amount of money can compensate for the loss of trust of our users.

[1] https://www.securitymagazine.com/articles/89777-shows-consumers-are-abandoning-brands-after-data-breaches

[2] https://www.theguardian.com/australia-news/2019/jan/21/home-affairs-plays-down-encryption-law-fears-and-promises-to-help-industry-cover-costs

This potential reputational harm could impact not just companies such as Mozilla but also technology companies that Mozilla may consider using as vendors. To put it plainly, as a result of this law, Mozilla must take a more guarded approach to whether to use technology vendors based out of Australia. Use of TCNs, without robust considerations of the factors we identify here, will make that problem worse.

The draft guidance on TCNs indirectly acknowledges these considerations in a few places. For example, under the section on "The legitimate interests of the designated communications provider": "the goodwill of the business", "market share and competitive advantage", and "the ability of the provider to maintain continuity of services to its customers and the reputational impact of disruption of services or service quality". It's not clear, for example, whether "goodwill of the business" refers to the goodwill of the company toward the Australian government or the goodwill of users toward the company. It's similarly unclear whether the totality of actions a DCP could be forced to do under a TCN and the corresponding reputational harm is covered by "disruption of services of services or service quality." We believe substantial harm would be averted if loss of user trust and reputation for the business were included as factors explicitly.

WE RECOMMEND the Minister consider "loss of user trust" and "reputational harm to the DCP" as additional legitimate interests of a DCP which should preclude the issuing of a TCN.

The consideration of whether a TCN is the least intrusive means possible for achieving Australian authorities' objective and whether other investigative means have been exhausted

Ordering a DCP to modify its software to undermine user privacy and security via a TCN is one of the most dangerous and invasive powers available to Australian authorities. Before signing off on such deeply harmful tactics, we would strongly recommend the Minister verify whether this is the least intrusive means of acquiring the sought information and whether the requesting agency and the Attorney-General have exhausted all other investigative means before issuing a TCN.

In the *Apple v FBI* case in the United States, the FBI sued Apple in an attempt to force the company to develop software which would degrade the iPhone's encryption. Ultimately, the FBI abandoned their case against Apple because they found another way to access the San Bernardino attacker's phone, making clear that forcing Apple to undermine their encryption wasn't the only way. As noted above, the Minister of Communications, Cyber Safety and the Arts was specifically empowered by Parliament in TOLA to act as an additional check on TCNs approved by the Attorney-General. We believe it is critical that the Minister exercise this authority to reject any TCN where the Attorney-General and the requesting agency have not demonstrated that a TCN is the least intrusive means necessary to acquire sought information and that all other investigative tools have been exhausted.

WE RECOMMEND the Minister reject any TCN where the Attorney-General and the requesting agency have not demonstrated that a TCN is the least intrusive means necessary to acquire sought information and that all other investigative tools have been exhausted.

Consideration of the terms and conditions for giving help

We were surprised to see the draft guidance state that "The Minister will not consider how any terms and conditions for giving help should be agreed between the provider and an interception agency or ASIO under this provision." While we recognize that terms of cost recovery are specified elsewhere in statute, the terms and conditions for giving help may be far more expansive than just compensation. Indeed, the ability to specify *how* an interception agency or ASIO is requesting a compromise to a DCP's products or services can be just as important as *what* they want to compromise. We recommend that the Minister also review any terms and conditions for providing help notwithstanding any limitations existing in Australian law.

WE RECOMMEND the Minister consider the nature and impact of the terms and conditions for providing help as part of their review.

The definition of a Designated Communications Provider

Due to ambiguous language in TOLA, one could interpret the law to allow Australian authorities to target employees of a Designated Communications Provider (DCP) rather than serving an order on the DCP itself through its General Counsel or an otherwise designated official for process. It is easy to imagine how Australian authorities could abuse their powers and the penalties of this law to coerce an employee of a DCP to compromise the security of the systems and products they develop or maintain. In order to ensure due process, appropriate diligence, and full compliance where appropriate with orders issued under this legislation, we strongly believe that Australian authorities should only serve an order on the DCP itself. Serving an order on an individual employee rather than a DCP itself would fail to allow a DCP to avail itself fully of the protections afforded under this legislation in regards to consultations, assessments, and legal challenges. Further, this potentially would force DCP's to treat Australia-based employees as potential insider threats, introducing another vector for compromise that could undermine trust in critical products and incentivizing companies to move critical roles to other localities. Parliament recognized the wisdom of this limitation in regards to Contracted Service Providers, but not DCPs.

WE RECOMMEND the Minister not approve any TCN which is imposed on an employee, agent, or vendor of a DCP, rather than to the DCP itself.

The imposition of limits on disclosure of TCNs

As an open source company, we are committed to developing our products and services publicly. More than just a philosophical choice, open source development allows myriad actors outside of Mozilla to identify bugs in our code, and in doing so making our products and services more resilient and secure. This benefits the hundreds of millions of people who use

Mozilla products every day. Developing in the open also allows our users to have more trust in the integrity of our code. The restrictions on disclosure in TOLA around building backdoors and other "acts and things" that may be required under the law are not just antithetical to us an open source company but would undermine the security and trust of our users.

Any requirement that Mozilla change its code in ways that are not public in our code base would directly contradict our mission and our brand promise. Thus, the secrecy of TCNs can have serious implications, not just for individuals, but for the interests of Designated Communications Providers and trust in the internet more generally. These secrecy provisions can impact the competitiveness of the Australian telecommunications industry, its ability to attract a skilled workforce, and companies' willingness to conduct their operations in Australia. These implications must be part of the Ministry's analysis.

Moreover, disclosure limits on TCNs are directly at odds with current industry initiatives[3] to give people more fidelity and a baseline level of security for the software they use. Today, people may unknowingly use versions of software that have somehow been modified by malicious attackers and that are being represented as coming from authoritative sources. Work on initiatives such as *binary transparency* and *reproducible builds* is intended to address this problem by providing stronger guarantees that the software running on people's machines has the same security properties as those found in public code repositories. This work has the potential to create a more secure software ecosystem for everyone. Secret TCNs are incompatible with the intent of these technologies because they would require software makers to include surveillance capabilities in their products that are inconsistent with public representations of those products. Were secret TCNs to be used broadly, they would threaten to forestall these important initiatives.

In light of the above factors, it is imperative that secrecy not be the default. If the government believes that secrecy is required in order to protect the integrity of an investigation or operation, they should have to seek an additional approval from a court of relevant jurisdiction. The Government should have to periodically justify to the court why the continuation of a restriction on disclosure is warranted, and all orders should become public eventually. While we understand that there may be a need for secrecy around the use of TARs and TANs because disclosure may alert the target of an investigation or operation, the same cannot be said of TCNs. Given that TCNs need not be tied to a specific target, operation, or investigation, there is no comparable need for restrictions on disclosure. TCNs designed to ensure that a DCP is capable of giving help could theoretically be used against any user, the vast majority of whom are not and will not ever be under suspicion.

While we don't believe Australian authorities should have these powers given their profound threat to security and privacy, we recognize that TOLA does allow for TCNs to be kept secret. However, given the risks here, we believe the Minister should use his considerable authority to ensure that secrecy is not the default, and to push the Attorney-General and the interception agencies which seek to use TCNs to justify why disclosure should be restricted.

[3] https://internetpolicy.mit.edu/pjcis-2018/

WE RECOMMEND the Minister assess the necessity of any limitations on disclosure for every TCN and require removal of any unnecessary limitations on disclosure in order to obtain their approval.

The definition of Systemic Weakness

We welcome the amendments made to TOLA when the law passed further limiting Australian authorities from requiring the creation or preventing the patching of systemic weaknesses and vulnerabilities. However, there is substantial and concerning ambiguity around the law's definition that a systemic weakness or vulnerability "affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person". It is entirely unclear what constitutes a "class of technology." Is the Firefox browser a class of technology unto itself? Certainly, it seems contrary to the spirit of this limitation to allow Australian authorities to compromise the security of the hundreds of millions of Firefox users who have never been under suspicion of any wrongdoing. We believe this vital protection could be further strengthened by clarifying that the standard for a "systemic weakness or vulnerability" applies to a weakness or vulnerability that affects any individual product, service, or system available to more than one person.

This limitation should be further clarified to prohibit a DCP being forced to weaken the security of its products or services in ways that would damage the trust and integrity of a DCP's upgrade channels. Updates are the means by which users receive the latest features as well as critical security updates, and so delivering a flawed update (one containing a vulnerability) could lead people to stop updating their software. This would likely have systemic impacts, resulting in a larger number of insecure products and devices, even if the vulnerability itself was targeted to a specific user.

WE RECOMMEND the Minister interpret the definitions of "systemic weakness" and "systemic vulnerability" in Section 317B to mean: "a vulnerability/weakness that affects the product, service, update channels, or system used by more than one individual, but does not include a vulnerability that is selectively introduced to one or more target technologies specific to a particular person."

Limitations on providing assistance to foreign authorities and extraterritorial use of these powers

While the powers granted in TOLA, especially TCNs, would still be quite dangerous even if limited to the territorial boundaries of Australia and Australian authorities, this legislation extends these powers to foreign governments with utterly insufficient safeguards. The potential for harm generally scales with the number of actors who can use investigative powers, so allowing foreign governments to request a TCN dramatically expands the scope of the threats to users and industry posed by this law.

As the number of entities requesting TCNs grows, so too does the potential for unintended consequences. It may be challenging, for example, to understand how the changes companies

would be forced to make to their products and services from multiple TCNs will interact. Given that all actors rely on commercially available technologies, this could have significant implications for national security, supply chain risks, availability and integrity of services, company reputations, as well as user privacy, security, and trust. To the extent that changes required by TCNs may have impacts in other jurisdictions, the use of such powers may also violate the sovereignty and legal protections of other countries.

Finally, allowing the use of TCNs by foreign governments would further erode Australia's reputation, and by extension the reputation and competitiveness of Australian industry. Given the risks posed by TOLA, many companies may choose to limit their investment in the Australian market as well as engagement of Australian vendors. These dangerous powers may also set a dangerous international precedent, which could be leveraged by other governments to justify their government hacking efforts in ways that would harm users and businesses in Australia and abroad.

While TOLA does not contain safeguards against these and other harms, the Minister could impose checks as part of his review which would usefully reduce the scope of these threats.

WE RECOMMEND the Minister require that requests by foreign countries to Australian authorities to use TCNs are:

- ***From countries that have strong human rights and due process protections enshrined in law;***
- ***Not used to evade the legal protections of the target as well as those not under suspicion in the requesting country;***
- ***Related only to an offence that is considered a serious crime in both Australia and the requesting country; and***
- ***Authorized at the highest levels of government by foreign nations.***

We thank the Minister and your staff for your diligent review of and public engagement around how the Minister will consider TCNs. TCNs, and TOLA more generally, represent an unprecedented and unchecked threat to the privacy and security of users in Australia and abroad. We urge the Minister to exercise his considerable authority to act as a bulwark against the dangers of TCNs. We remain at your disposal if there is other information that we can provide that would assist in your development of this critical guidance around the approval of TCNs.

Respectfully submitted by:

Jochai Ben-Avie
Head of International Public Policy
Mozilla Corporation