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