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Thank you for the opportunity to provide comment on your draft guidance on the consideration of requests for Technical Capability Notices (TCN) by the Minister for Communications, Cyber Safety, and the Arts.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 jochai@mozilla.com.

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