INSLM TOLA Report Analysis - Mozilla Asks & INSLM Answers

What we asked for	What the INSLM said
Clarify that Australian authorities cannot target an employee of a Designated Communications Providers We recommended that the Section 317B definition of Designated Communications Provider be clarified 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."	INSLM clarified that a natural person should only be considered to be a DCP where that natural person is a sole trader (i.e., an order served on a DCP which is a company must be served on the company, not an employee of that company). The Department of Home Affairs also stated on record that this was their interpretation. An individual employee could still receive a voluntary request to provide assistance to ASIO under Schedule 5, and currently that request can come from any ASIO "senior position holder". The INSLM has recommended that TOLA be amended to make clear that nothing in s 21A authorises the Director-General to make a request of a person that is properly the subject of a TAR and that this power now be exercised by an officer not lower than a Deputy Director-General.
Remove restrictions on disclosure of Technical Assistance Requests, Technical Assistance Notices, & Technical Capability Notices We recommended that section 317ZF be deleted. The restrictions on disclosure in TOLA around building backdoors and other "acts and things" that may be required under the law would undermine the security and trust of all of our users.	Unfortunately, it looks like disclosure by a DCP is still prohibited. However, the INSLM did recommend that Commonwealth officials be authorized to disclose TAR/TAN/TCN info to the public and to government officials when disclosure is in the national or public interest. The decision to disclose may be made by the relevant agency or departmental head or the relevant minister.
Require judicial approval of Technical Assistance Notices and Technical Capability Notices We recommended that language be added 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.	The need for independent review by a competent legal authority is the strongest recommendation in the report, reiterated multiple times. The INSLM recommends TANs and TCNs be reviewed and approved by the Administrative Appeals Tribunal (AAT) – an impartial, independent body – to be overseen by a proposed Investigatory Powers Commissioner. INSLM suggests that the IPC be a retired high ranking judge, appointed by the Governor-General, on the advice of the Attorney-General, following consultation with the

	Leader of the Opposition. The INSLM would also "expect" but "would not mandate" consultation with industry. Australia is currently seeking acceptance/status under the US CLOUD Act, and the Attorney-General has tabled the International Production Order (IPO) Bill which would require AAT authorization for TANs and TCNs (amongst other types of surveillance orders), giving effect to this recommendation.
Modify the assessments mechanism to ensure an impartial review which considers all rights and interests We recommended that sections 317WA and 317YA be amended and a new section added 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 group should be required by statute to include departments with government security, business security, and human rights missions.	While the assessment process still exists and the INSLM didn't propose any changes directly, the proposed introduction of review of TOLA orders by the AAT with access to its own technical experts adds an adversarial process that makes this ask of ours a moot point.
Require all requests not to disproportionately harm the rights and interests of users not under suspicion. We recommended that the tests for reasonableness and proportionality in sections 317JC, 317RA, 317TAAA, and 317V be amended to require law enforcement and intelligence agencies authorized under this law to demonstrate that the order doesn't disproportionately harm the rights and interests of users, among other requirements. We also recommend the deletion of the word "legitimate" in regards to the interests of the designated communications provider.	The proposed amendment to the systemic weakness definition is definitely an improvement in this regard. See the section on systemic weakness definition for more detail. Disappointingly, while the INSLM recognizes that determining what "the legitimate expectations of the Australian community relating to privacy and cybersecurity" are "hard to enunciate," he doesn't recommend any real changes. The INSLM also recommends reducing the scope of offences for which a TAR, TAN, or TCN can be sought from the current (crimes punishable by at least 3 years in prison) to the more restrictive list of serious offences included in the Telecommunications Interception Act (generally a minimum of 7 years plus other offences like murder).

Clarify that "systemic weakness" includes any weakness in an individual communications system available to more than one person. We recommended that the definitions of "systemic weakness" and "systemic vulnerability" in Section 317B be amended 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."	INSLM recommended some very helpful amendments to the definition of systemic weakness (and recommends the removal of the term "systemic vulnerability"). Some relevant passages: I recommend that s 317ZG(4A) state prohibited effects as follows: (4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness into a form of electronic protection means a reference to any act or thing that creates a material risk that otherwise secure information will be accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party. I further recommend the introduction of the following definitions: a. 'Otherwise secure information' means 'information of, any person who is not the subject, or is not communicating with the subject of, an investigation'. b. 'Unauthorised third party' means 'anyone other than a party to the communication, the agency requesting the relevant TAR, TAN or TCN and/or integrity agencies'. I recommend clarification of definitions through the use of non-exhaustive statutory examples: a. Clarify that 'target technology' in s 317B refers to the specific instance used by the intended target. b. Include non-exhaustive examples of what is excluded from the meaning of 'electronic protection' in s 317B. 'Class of technology' can then be defined through examples of services used by a group of users broader than the intended target – for example, all Telstra mobile phone subscribers or all subscribers in a particular location.
Limit the delegation of power in TOLA	Under the new system proposed by the INSLM,

We recommended that sections 317ZN, 317ZP, 317ZQ, and 317ZR be amended 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.	TANs and TCNs will first need to be approved by the head of an agency before being submitted to the AAT for review. However, Commonwealth, State, and Territory law enforcement officers can still obtain computer access warrants,[1] and any law enforcement officer can still apply to an eligible judge or nominated AAT member for an assistance order that compels a person to provide certain assistance in respect of a computer that is the subject of a computer access warrant. As discussed above, the INSLM also recommended that voluntary requests made by ASIO under Schedule 5 be authorized by an officer not lower than a Deputy Director-General.
Impose critically missing limitations on providing assistance to foreign authorities and extraterritorial use of these powers. We recommended that TOLA be amended to place requirements on the requests by foreign countries to Australian authorities to use the powers granted by TOLA, and add 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 services. We also recommended the addition of a provision requiring the Attorney-General to publish a transparency report at least once every six months and the addition of a provision prohibiting the use of these powers outside the territorial borders of Australia.	The INSLM noted that there is a significant overhaul of the procedural safeguards around mutual legal assistance in criminal matters coming in the forthcoming International Production Orders (IPO) Bill which Australia is likely to enact later this year in order to get access/status under the CLOUD Act. The INSLM also recommended that statistics on use of TOLA powers be made public annually by the IPC, save for the revealing of any operationally sensitive or classified info. ASIO's exercise of powers under Schedule 5 should, according to INSLM, also be detailed in its annual report provided to the PJCIS, the Leader of the Opposition, the Inspector General of Intelligence and Security, the INSLM, the Attorney-General and the Minister for Home Affairs.

Information in this table is pulled from:

- *Our latest filing to the PJCIS*
- *The INSLM's report*

[1] Subject to some procedural requirements, computer access warrants allow a law enforcement officer to access, copy, add, alter, and/or delete data on a target computer or computer system. These are different from TARs, TANs, and TCNs.