kaspersky

Proven.
Transparent.
Independent.

11 June 2019

Submission to the Parliamentary Joint Committee on Intelligence and Security:

Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Kaspersky, a global cybersecurity company, is grateful to the Parliamentary Joint Committee on Intelligence and Security (further, 'Committee') for the opportunity to provide additional comments on the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA). We also thank the Parliament of the Commonwealth of Australia for publishing the amendments to be moved on behalf of the Government.

Our company remains supportive of the intention of the Australian Government to ensure the safety and security of its citizens, and here we are pleased to offer recommendations for the Committee's review of the TOLA, and further improvement of the Act.

Recommendation 1 - Introduction of strong legal safeguards for protecting companies' security information, including source code

We at Kaspersky provide access for government stakeholders and enterprise partners (both existing and prospective ones) to review our source code, software updates, and threat detection rules, along with other technical and organisational processes[1]. We provide such access at a dedicated secure environment – our Transparency Centres in Zurich and Madrid. The source codes of our cybersecurity products are the intellectual property of Kaspersky.

In this regard, the compelled and non-transparent disclosure, under technical assistance notice (TAN) or technical capability notice (TCN), of our most critical and sensitive security infrastructure, including source code[2], may pose a serious threat to keeping our products' integrity and trustworthiness.

We urge to introduce strong protections of sensitive security information of companies (DSPs) and their intellectual property through:

- Developing mechanisms for a process, negotiated and approved by both sides, for disclosure of companies' intellectual property;
- Adding reasonable timeframes for companies (DSPs) to get prepared for such disclosure of their sensitive security information, including source code;

---

[1] https://www.kaspersky.com/transparency-center-offices

[2] As stated in the Explanatory memorandum to Section 317E https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr6195_ems_1139bfde-17f3-4538-b2b2-5875f5881239%22;rec=0

- Introducing a legal mechanism for companies (DSPs) to challenge requests for disclosing their sensitive security information, including source code;
- Adding mandatory independent oversight of such a process by the Commonwealth Ombudsman or the Office of the Australian Information Commissioner (OAIC);
- Allowing transparent, publicly available reporting by companies with a specification of the information that has been disclosed.

Recommendation 2 - Introduction of limitations for actions under section 317E 'Listed acts or things' and independent oversight for execution of such limitations

Under section 317E, a company (or DSP) can be asked to do a number of 'listed acts or things, including 'installing, maintaining, testing or using software or equipment'; however, the TOLA does not have reasonable and clear limitations on such actions.

Clear limitations are extremely important as the software or equipment deployed within a company's system upon the request of an agency might give the agency direct access to the sensitive information or traffic data, metadata or to the functionality of such software or equipment a non-limited period and beyond the immediate needs of a specific TAN or TCN.

We recommend introducing a transparent procedure of invoking such abilities with independent oversight by the Commonwealth Ombudsman or the Office of the Australian Information Commissioner (OAIC) to ensure compliance with the Australian Privacy Principles (APPs) and establishing a mechanism of reporting APPs violations.

In addition, we recommend introducing a legal prohibition on disclosure of data to investigating authorities that are not associated with a specific TAN or TCN with clear rules developed for the transfer of data between the participating agencies.

Recommendation 3 - The consultation notice mechanism should be improved in terms of inclusion of greater independent oversight, and real participation of companies in the consultation process.

We very much welcome amendments of introducing sections 317WA to establish a consultation notice mechanism – a framework that requires the decision maker to consult with the provider to the issuing of a TCN. The sections also allow companies to highlight the requirements that will undermine those systems that protect the security of personal information.

These amendments state that the Attorney General (AG) must appoint two persons, called assessors, to carry out an assessment of whether the proposed TCN should be given. We also welcome here the amendment to strengthen independent oversight by requiring that the assessors must provide a copy of the final report to the Inspector General of Intelligence and Security, if there are acts or things that relate to ASIO, and to the Commonwealth Ombudsman, if there are acts or things that relate to an interception agency.

However, there are limitations that could potentially undermine the independence of the consultation notice mechanism:

kaspersky

Proven.
Transparent.
Independent.

- Companies (or DSPs) cannot appoint assessors; only the Attorney General is capable of doing so, and this fact raises questions over assessors' true independence;
- Assessors, in the new subsection 317WA (7), must only 'consider' whether TCNs are reasonable and proportionate as well as whether compliance with the TCN is practicable and technically feasible, but assessors do not have the right either to approve or disapprove TCNs. This questions the real role of assessors and their opinions' value in the consultation process.The TOLA provides ambiguous wording as to whether the assessment carried out under the consultation notice is binding or not – 'if a copy of the assessment report has been given to the Attorney General, the Attorney General must have report considering whether to proceed in giving the notice' (new subsection 317WA (11)).

Recommendation 4 - Introduction of clear thresholds for 'urgent' cases with reasonable and appropriate timeframes to comply with TANs and TCNs.

Sections 317PA and 317W state that before giving a TAN or TCN, the Director General (DG) of Security or the chief officer of an interception agency, and the Attorney General (AG) must not give a TAN or TCN to a designated communications provider (DSP), respectively, unless they have first given the provider a consultation notice. However, further in both sections the TOLA states that such a rule *does not apply [...] if such authorities are satisfied that either TAN or TCN should be given as a matter of urgency.*

Such limitations 'as a matter of urgency' are provided in the TOLA without clear thresholds for what such 'urgency' might imply and under what criteria. Therefore, it appears that the consultation notice mechanism can be bypassed by the requesting authority simply saying that either TAN or TCN is urgent.

Companies (or DSPs) might be put at risk of an unforeseen burden to comply with 'urgent' TAN or TCN (preparation of technical information requires manpower and timing resources), etc.

Recommendation 5 – Introduction of precise definitions for the terms 'systemic weakness' and 'systemic vulnerability' in close consultation with relevant industry, academia and human rights experts.

We appreciate the amendments made to the sections 317ZG, and attempts to define 'systemic weakness' and 'systemic vulnerability'.

However, there are a number of ambiguities that remain open that may cause issues from a technical and practical point of view:

- It is not clear what a 'whole class of technology'[3] implies (in case of cybersecurity solutions, would a 'class' imply all such cybersecurity solutions, or only some selective detection and performance technologies?). Industry and technology

[3] As stated in the Amendments made by the House of Representatives https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fsched%2Fr6195_sched_d701fa80-e013-4a9e-b3e2-4e52b8b2facf%22

literature have no terms or analogues of such a definition. None of the mechanisms (technical assistance request TAR; technical assistance notice TAN or technical capability notice TCN) could ever be issued to a single individual or company that has control over the 'whole class of technology', hence, it is difficult to imagine that TAR, TAN or TCN could cover such a 'whole class of technology'. If such an individual or company does exist, TAR, TAN or TCN – even for a selective target technology – might weaken or even disrupt one vendor's entire service or network.

- Both definitions are identical, and they do not provide differentiation between 'weakness' or 'vulnerability'. It may be reasonable to avoid duplication and leave one term. Both definitions also contradict the definition of a 'target technology'. The latter definition implies targeting a particular person: 'for the purposes of this Part, a particular carriage service, so far as the service is used, or is likely to be used (whether directly or indirectly) by a particular person, is a target technology that is connected with that person'. However, the Act adds that 'for the purposes of paragraphs (a), (b), (c), (d), (e) and (f), it is immaterial whether the person can be identified (italic - Kaspersky)'. If it is immaterial that the target person can be identified, the provision means that the TOLA would permit bulk interception/surveillance. If the person cannot be identified, he or she shall not be targeted in the first place.

Recommendation 6 – Mitigation of punishment for disclosure about requests under the TOLA

Under section 317ZF, companies (or DSPs), for unauthorised disclosure of information under TAR, TAN or TCN might face harsh penalties – imprisonment for up to five years.

We believe that such penalties are too grave for companies, since practice shows that in case of requests and for preparation of technically accurate information for the disclosure, several departments within companies might be involved – information security, legal, RnD, IT, and other teams. Companies might also consult external experts and lawyers for ensuring full compliance with legal frameworks under which such requests are made. For such cases it is difficult to avoid disclosure about requests under the TOLA.

Recommendation 7 – Unification of a legal procedure for issuing TANs, and introduction of additional approval by the respective body and consultation notice mechanism

Under section 317L, the Director General of Security or the chief of an interception agency (*meaning there can be several at once, bold – Kaspersky)* may issue a company (DSP) a technical assistance notice. We welcome the amendments regarding the Committee imposing time-limits of 12 months for TANs and introducing consultation notices prior to the issuing of a TAN (new section 317PA).

We also support the amendment under the new subsection 317MAA (3) (4) to provide the right to the company (DSP) to make a complaint about the TAN to the IGIS under the IGIS Act, to the Commonwealth Ombudsman or an authority that is the State or Territory inspecting agency in relation to the interception agency.

However, TANs

kaspersky

Proven.
Transparent.
Independent.

- Do not still require a binding confirmation or approval by the independent bodies (e.g., the Commonwealth Ombudsman) or other parties engaged for the consultations if the TAN/TCN is proportionate, technically feasible, and complies with the TOLA; and
- Can be issued by various delegated officers of interception agencies, and companies (DCPs) may receive multiple requests for similar information and assistance from different agencies. We suggest further reducing the number agencies with powers to issue TANs or TCNs while introducing a 'request escalation' mechanism that would allow other agencies to request assistance from the agencies with those powers.

Conclusion

We would like to reiterate that Kaspersky remains a strong advocate of cooperation between the government and industry to ensure that cyberspace is there for good. We hope that the Law would be corrected to reach the goal of ensuring the security and wellbeing of the citizens in Australia, while taking into account legitimate interests of users and businesses.

We also hope to see more actions for engaging the private sector in reaching optimal effectiveness of the measures and principles which the Law stipulates for in transparent and collaborative manner. Should you require any information, we are at your disposal for inquiries at any time.

About Kaspersky

Kaspersky is a global cybersecurity company which has been operating in the market for over 20 years. Kaspersky The company's comprehensive security portfolio includes leading endpoint protection and a number of specialised security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters most to them; our office for Australia and New Zealand is located in Melbourne, Victoria. Learn more at www.kaspersky.com

[redacted]