KASPERSKY lab

Proven. Transparent. Independent.

Assistance and Access Bill 2018 Public Consultation

An opinion of Kaspersky Lab

Kaspersky Lab is global cybersecurity firm known for its continued commitment to fight transnational cybercrime. We assist national authorities and international LEAs in cybercrime investigations by providing our technical expertise and analysis of malicious programs. We also lead the efforts to improve the industry's transparency and accountability through our Transparency Initiative, which among other aspects includes independent third-party review of our source code and development practices.

Kaspersky Lab supports the intention of the Australian Government to ensure safety and security for its citizens in cyberspace. We are grateful for an opportunity to highlight our concerns regarding some provisions of the Assistance and Access Bill, and their potential effect on providers of cybersecurity services.

Assessing Proportionality and Feasibility

We appreciate that the Bill clearly states that the decision-makers must evaluate the individual circumstances surrounding each notice in order to determine whether the provision of particular technical information is reasonable and proportionate (317V) as well as considerate of the interests of the agency, the provider (likely business impact) and public interests, such as its potential impact on privacy, cybersecurity, and innocent third parties (317D).

However, in our view there are significant omissions and procedural loopholes that create risks to providers' business and users' safety without necessarily reaching the stated objectives of the Bill.

a) While the Bill Explanatory Document highlights that provider will be consulted with prior and after serving her a notice, the consultation process and its impact on decision making are not defined

In the case of complex automated systems, such as today's anti-virus or malware detection solutions, it is reasonable to foresee a scenario where after series of consultations the decision-maker is assured that the new capability is feasible, while the provider is certain that it would be technically impossible to create one without compromising the quality and integrity of the service in question.

Specifically, in case of encryption there is broad industry agreement that a third party access to encryption keys weakens encryption for all users, including those not targeted by the encryption agency. This argument has been explored in more details by the Citizen Lab and the Canadian Internet Policy and Public Interest Clinic (CIPPIC) report[i] and in our view is applicable to other technologies.

The obligation to provide decryption keys and access to data under a technical assistance notice (317L) will also undermine users' confidence in the most essential software products. More so, for the products and services where transparency is an essential component it will be downright impossible to introduce the new capability *and* conceal it at the same time, as described by the Subsections 317E(1)(c) and 317E(1)(j).

Specifically, under Kaspersky Lab Global Transparency Initiative software updates will be reviewed by an independent third party in Switzerland to verify the integrity of our products and limit the ability to implement undocumented functionality in our products. Hence an attempt to stop a release of updates for specific systems or adding new hidden functionalities under a technical capability notice will likely be discovered, putting company's employees at risk of imprisonment as stipulated in the subsection 317ZK.

b) While the Act outlines the requirement for the decision maker to consider whether the notice is *technically feasible*, there are no obligations to take *legal implications of* the notice into account

Due to exterritorial nature of the Bill, a provider might compelled to hand over data on its overseas users or grant access to devices in other countries. There are various avenues of obtaining the required information, and the Bill is unclear in what instances this avenues shall be explored by an interception agency prior to serving provider with a notice.

For instance, the ability to obtain digital evidence, including seizing records, data, traffic, and encryption keys overseas is already covered by the existing mechanisms of judicial and law enforcement cooperation, such as over 25 MLATs of which Australia is a party[ii] or the Council of Europe Convention on Cybercrime (Budapest Convention)[iii] which Australia ratified in 2013. Budapest Convention specifically includes provisions allowing law enforcement to access and preserve computer data and traffic (Articles 29 and 30), collect real-time traffic (Article 33), and intercept content data (Article 34). The Convention also allows delivering Production Orders (Article 18) to assist with data decryption and force whomever has the keys to encrypted data to release them to law enforcement authorities.

While acknowledging that these cooperation mechanisms are far from perfect, the legal experts remind that the formal process was developed to protect the state sovereignty as well as the rights of the accused, and that the '*requests for evidence or information not in police possession must be authorized through the proper legal channels'*[iv]. By enabling direct access to foreign users' machines through the technology provider, rather than through the approved cooperation channels, the Bill may instituonalize circumvention of the standardized procedures of formal mutual legal assistance requests on the grounds of urgency or secrecy. More so, to the regulators in jurisdictions where a mutual legal assistance regime with Australia is absent, such access might be considered the violation of nation's sovereignty. When served with a notice to access data in those jurisdictions *and* conceal this action, providers may face a stark choice of which country's laws they will have to violate.

c) While section 317ZK outlines arbitration process in exceptional cases it still leaves the matter largely in hands of the same interception agency issuing the notice in the first place.

The Bill entrusts people who occupy the positions at the highest level of Government ultimate right to judge reasonableness and proportionality of any new requirements. However, a *subjective state of mind of the administrative decision-maker* cannot serve as a criteria for what is essentially a technical discussion, which requires specific knowledge and technical competence. This knowledge may not always be readily available in the public sector, a fact noted by the recent *Digital Delivery of Government Services* Report[v].

The only path to resolve the principal disagreements allowed by the Bill is an arbitration process led by an arbitrator appointed by the Australian Communications Media Authority or the Attorney-General office. That however further prioritizes subjective assessments of the government officials and allows little clarity on provider's capacity to debate these assessments.

No other conflict resolution mechanism – be it taking a specific matter to a technically-competent third party or relying on industry's best practices – is outlined for such cases. Without a third party's technical expertise and balanced technical opinion on the requests to weaken encryption, install software given by an agency or process with other things authorized under the Bill, security and integrity of software products, including ours, might be greatly undermined.

Conclusion

Despite the recent Five Country Ministerial memo supporting the measures outlined in the Bill, the debate about necessity, proportionality and efficiency of these intrusive capabilities is far from over even within the Five Eyes pact countries. In the US bipartisan draft ENCRYPT act, which advocates stronger encryption to protect users from cybercrime, received support from tech industry bodies such as Consumer Technology association[vi] and ITI[vii]. Australian participants of the cyber security–focused policy exercise co-organized by RAND Corporation and the National Security College at the Australian National University also '*saw little justification for an invasion of privacy that may come with increased security*'[viii] without immediate threat. Similar laws in EU countries, such as Germany' Data Retention Law, were *de-facto* overturned in December 2016, when the European Court of Justice ruled they were disproportionately wide[ix].

Looking from a business perspective, the Bill may undermine the confidence of law-abiding consumers in software products and software companies. It will also further contribute to the regulatory fragmentation of cyberspace along the geopolitical lines. As we noted in our submission to the Australian Parliament Joint Standing Committee on Trade and Investment Growth, regulatory fragmentation in cyberspace may lead to reciprocal measures in other markets of the Indo-Pacific region, hampering the potential of exportability and competitiveness of software products and services, including those made in Australia[x].

In the meantime, we remain strong advocates of the cooperation between the government and industry to ensure that cyberspace is there for good. Encryption and access are no black-and-white matters, and in our view the legitimate interests of interception agencies shall not undermine no less legitimate interests of companies and users. We consider that working on the Bill regulators might have engaged companies in a constructive dialogue at an earlier stage – and that this engagement is essential moving forward.

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company which has been operating in the market for over 20 years. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into next generation security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

---

i Shining a Light on the Encryption Debate: A Canadian Field Guide. Citizen Lab, Canadian Internet Policy and Public Interest Clinic (CIPPIC), May 2018.
ii Fact sheet – Mutual assistance overview, Attorney-General's Department
iii Convention on Cybercrime, Council of Europe
iv Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime. Adam Palmer, The Center for Cyber and Homeland Security, 2018
v Digital delivery of government services. Finance and Public Administration References Committee, 27 June 2018
vi Tech consumers should not be forced to sacrifice privacy for security. Gary Shapiro, CNBS, 16 July 2018.
vii Tech Industry Welcomes ENCRYPT Act. ITI Press Release, 07 June 2018
viii Exploring Cyber Security Policy Options in Australia. RAND Corporation and ANU, January 2017
ix Berlin wants European Court of Justice to assess Germany's data retention law. Politico, 31 August 2018
x Submission to the Australian Parliament Joint Standing Committee on Trade and Investment Growth. Kaspersky Lab, February 2018

For more information, or to discuss the contents of this submission in more detail, please contact Oleg Abdurashitov, Head of Public Affairs Asia Pacific, Kaspersky Lab

T: [redacted] | email: [redacted]