25 February 2022

BSA COMMENTS ON REFORM OF AUSTRALIA'S ELECTRONIC SURVEILLANCE FRAMEWORK

Submitted Electronically to the Department of Home Affairs

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to the Department of Home Affairs (**DHA**) on the reform of Australia's electronic surveillance framework, with reference to the associated Discussion Paper[2] and the Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community[3] (**Comprehensive Review**).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernise and grow. Many of BSA's member companies have made significant investments in Australia, and we are proud that many Australian organisations and consumers continue to rely on our members' products and services to support Australia's economy. BSA has previously provided comments on similar issues in respect of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and the *Telecommunications Legislation Amendment (International Production Orders) Act 2021*.[4]

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] Discussion Paper, Reform of Australia's Electronic Surveillance Framework, December 2021, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/reform-of-australias-electronic-surveillance-framework-discussion-paper.

[3] Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community 2020, December 2020, https://www.ag.gov.au/national-security/publications/report-comprehensive-review-legal-framework-national-intelligence-community.

[4] See:

a) BSA Comments on Access and Assistance Bill 2018, September 2018, https://www.bsa.org/policy-filings/australia-bsa-comments-on-access-and-assistance-bill-2018.
b) BSA Comments to PJCIS on Access and Assistance Bill 2018, October 2018, https://www.bsa.org/policy-filings/australia-bsa-comments-to-pjcis-on-assistance-and-access-bill-2018.
c) BSA Comments to PJCIS on Assistance and Access Act 2018, February 2019, https://www.bsa.org/policy-filings/australia-bsa-comments-to-pjcis-on-assistance-and-access-act-2018.
d) BSA Comments to PJCIS on Review of the Assistance and Access Act 2018, June 2019, https://www.bsa.org/policy-filings/australia-bsa-comments-to-pjcis-on-review-of-the-assistance-and-access-act-2018.
e) BSA Comments to INSLM on Review of the Assistance and Access Act 2018, September 2019, https://www.bsa.org/policy-filings/australia-bsa-comments-to-inslm-on-review-of-the-assistance-and-access-act-2018.
f) BSA Comments on Telecommunications Legislation Amendment (International Production Orders) Bill 2020, April 2020, https://www.bsa.org/policy-filings/australia-bsa-comments-on-telecommunications-legislation-amendment-international-production-orders-bill-2020.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

We appreciate the Government's goal of replacing the existing laws governing Australia's electronic surveillance authorities with a new and modernised legislative framework by 2023. We also applaud the Government's recognition that it is critical to work closely with a range of stakeholders throughout this process, to ensure a new framework is clear and consistent, well-adapted to the modern world, and in line with the principles and values of a democratic society.

BSA's members have worked closely with law enforcement and intelligence agencies in Australia, the United States, the United Kingdom, and elsewhere around the world to ensure that they can access digital evidence in support of investigations in a timely manner pursuant to appropriate safeguards. For these authorities to take advantage of the opportunities new technologies bring, and to overcome the array of associated challenges, digital evidence access must be approached collaboratively. The needs of law enforcement and intelligence agencies, businesses, and the consumers whose privacy and security interests are at stake are best met by policies and laws that provide for robust mechanisms for judicial oversight, transparency of activities, privacy and security protections, and clearly defined processes for bi-directional communication.[5] In addition, as data is stored by global organisations subject to laws in different countries, it is increasingly important that laws for government access be internationally interoperable. This review creates an opportunity to further collaboration between the technology, law enforcement, and intelligence communities on the range of issues raised by reforming Australia's electronic surveillance framework.

Summary of BSA's Recommendations

Australia should maintain foundational aspects of its electronic surveillance laws, including:

- Maintaining the definition of "communications";
- Distinguishing between content and non-content;
- Distinguishing between communications in transit and in storage;
- Reducing the potential for conflicts of laws on businesses, particularly those operating across international borders;
- Require warrants to have a nexus to a person;
- Recognising that different methods of obtaining information create different privacy concerns — and that a framework should recognise privacy issues based on both the type of information sought and the method by which it is obtained; and
- Strictly controlling which agencies may exercise surveillance authorities.

Australia should also implement more safeguards to ensure that the exercise of electronic surveillance powers is subject to considerations of privacy, security, transparency, and due process, including:

- Incorporating principles of specificity, using least intrusive means, and minimisation;
- Making prior review by independent judicial authorities available for orders relating to government access to data;

[5] See BSA Global Best Practices for Law Enforcement Access to Digital Evidence, https://www.bsa.org/files/policy-filings/09232019leaglobalbestpractices.pdf and appended to this submission.

- Providing businesses with a right of appeal;

- Creating a centralised oversight authority by merging the Inspector-General of Intelligence and Security (**IGIS**) and the Commonwealth Ombudsman;

- Including additional information in publicly available reports, such as information on the use of electronic surveillance information in hearings, the number of people who have been the subject of electronic surveillance, and occasions where issuing authorities have required agencies to provide further information in support of warrant applications;

- Allowing businesses to publish aggregate data on the occasions they have been ordered to assist with electronic surveillance; and

- Requiring pre-issuance consultations with businesses and allow notification of data subjects where possible.

Australia Should Maintain Foundational Aspects of its Electronic Surveillance Laws

The Discussion Paper indicates that the Government will reconsider a number of core concepts during the review, including the definition of a communication, the distinction between content and non-content information, the distinction between live and stored communications, the kinds of businesses that hold relevant information and data, and the kinds of information that may be obtained through surveillance and tracking devices.[6] These are critical issues that will determine the scope of surveillance authorities in Australia. As such, we encourage the Government to ensure that any new framework builds on foundational concepts — and requires authorities to meet high standards to exercise surveillance authorities while enabling strong oversight.

We encourage the Government to ensure any new framework reflects foundational aspects of electronic surveillance laws. These include:

- **Maintaining the definition of "communications" (Questions 5-7).** Communications are defined as including a "conversation and a message" under the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**). The Discussion Paper notes that it is "increasingly difficult" to determine which types of information constitute a communication,[7] particularly in situations such as machine-to-machine signals. The Discussion Paper proposes developing a new "technology-neutral" term that can reflect the broad range of information and data transmitted electronically. We are concerned that the effort to develop a new definition of communications may not ultimately resolve these increasingly difficult issues — which will recur in different forms as technology evolves — but instead may have the primary effect of creating new uncertainties, particularly around the intersection of a new definition with existing laws. We therefore suggest retaining the current definition of communications and focusing instead on providing clarity about how the new framework will apply to different types of content and non-content data sought by agencies.

- **Distinguishing between content and non-content (Questions 8-10).** Laws should distinguish between content data (i.e., the substance of a communication) and non-content data (i.e., information about the communication). Clearly distinguishing these two types of data ensures that content can be subjected to heightened safeguards that reflect the particularly intrusive nature of

[6] Discussion Paper (2021) at p. 20.

[7] Discussion Paper (2021) at p. 21.

allowing others to access it. For example, as the Discussion Paper recognises, agencies typically require a warrant to obtain content, while non-content information may be obtained on other bases.

  - *Content should be obtained pursuant to a warrant*. At times, the Discussion Paper suggests that any data falling under a potential new definition of "communication" would require a warrant.[8] That assumption does not reflect that it is content data — and not all communications — traditionally subject to this heightened protection.

  - *There are benefits to distinguishing between types of non-content data.* As the Discussion Paper recognises, non-content data may in some situations have increased sensitivity, particularly when that data is linked to an individual or can reveal sensitive information about an individual. One especially sensitive category of data is location data. Location data collected over time can be used to identify an individual with reasonable specificity, and her travel patterns over time can give away deeply personal information that is not intended to be shared, such as information on her health or religion.[9] At the same time, some non-content information may also have decreased sensitivity, such as basic information about the subscriber of an online account.[10] We encourage the Government to bear in mind these different levels of sensitivity among non-content data as it reviews Australia's surveillance authorities, and to implement appropriate safeguards that correspond to those levels of sensitivity (e.g., heightened safeguards for accessing location data).

- **Distinguishing between communications in transit and in storage (Questions 11-12).** The Discussion Paper notes that the distinction between live and stored data, while present in current legislation, is "less significant than it may once have been".[11] Still, the ability to intercept live communications in real time remains especially intrusive today. Even though it has, as noted in the Comprehensive Review, become the norm for people to communicate "spontaneously and instantaneously" via instant messaging and similar services,[12] conversations of a private or sensitive nature still take place over calls, videoconferences, and other communication methods that do not leave a paper trail of stored messages that may subsequently be sought by law enforcement. On that basis, the new electronic surveillance framework should continue to differentiate between live and stored data — it should establish a high procedural threshold for authorising real-time access to content data and subject this power to additional safeguards (e.g., such access should require a search warrant or equivalent order approved by an independent judicial authority). To the extent that the Government determines that there should be no distinction between access to content in real-time and access to stored content, we strongly encourage the Government to raise the standards for accessing stored content, rather than lowering safeguards for real-time content. Further, the new framework should not require businesses to capture and store real-time data for the purposes of facilitating access to such data by the relevant agencies at a later date. Imposing such a requirement would render any

[8] Discussion Paper (2021) at p. 22.

[9] Relatedly, for this reason, we disagree with the Discussion Paper's observation that "tracking information may have less impact on privacy than other surveillance information" (see Discussion Paper (2021) at p. 44).

[10] For example, pursuant to the United States Electronic Communications Privacy Act (**ECPA**), law enforcement agencies may obtain seven specific types of subscriber data with a subpoena. See 18 U.S.C. 2703(c)(2) (addressing the ability of law enforcement to obtain the following "basic subscriber information": name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of services utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number). Other forms of non-content may only be obtained pursuant to a court order or warrant. See 18 U.S.C. 2703(c)(1), (d).

[11] Discussion Paper (2021) at p. 27.

[12] Comprehensive Review (2020), Vol 2, p. 258.

distinction between live and stored communications meaningless and runs counter to principles of necessity and proportionality.

- **Reducing the potential for conflicts of laws on businesses, particularly those operating across international borders (Question 13).** The Discussion Paper notes that different aspects of Australia's current surveillance authorities apply in different ways to "carriers," "carriage service providers," and "designated communication providers." As the Government develops a new framework for these legal authorities, it should seek to minimise the potential for these different kinds of businesses to face conflicting legal obligations. In particular, the Government should ensure that legal processes issued to businesses that operate internationally is consistent with all applicable international commitments. When issuing legal processes to businesses in the United States, Australian officials should ensure the legal processes are consistent with the Clarifying Lawful Overseas Use of Data Act (**CLOUD Act**) agreement between Australia and the United States. A legal process that is consistent with these international agreements reduces the potential for businesses to face conflicting legal obligations and ultimately helps speed their responses to such process.

- **Require warrants to have a nexus to a person. (Question 20)**. We agree with the Discussion Paper's recognition that surveillance powers should be directed to the person who is the subject of the investigation. To the extent that the Government considers providing "limited exceptions" to this person-based approach in relation to third parties, groups, and unidentified persons and foreign intelligence, these exceptions should be drawn narrowly and subject to additional safeguards that reflect the potential privacy implications on third parties who are not subjects of investigations. Even if some agencies may appropriately use such narrow exceptions, the Government should also carefully tailor such authorities so that they are not available to agencies for which this type of authority would be inappropriate. In considering this person-based approach, the Government should also consider the related issue of which business entities should be the subject of legal process. In particular, when the Government requests access to the digital evidence of a business, it should seek that information from the business itself rather than the business's vendors or data processors (e.g., enterprise service providers).

- **Recognising that different methods of obtaining information create different privacy concerns — and that a framework should recognise privacy issues based on both the *type of information* sought and the *method* by which it is obtained (Questions 15-17).** The Discussion Paper suggests that a new framework should emphasise "what information agencies are trying to collect, the intrusiveness and the matter being investigated" instead of the "current focus on how they intend to collect it."[13] That approach risks overlooking privacy concerns created by methods of collection that may be particularly intrusive. For example, the method of obtaining communications in real time as they are sent is particularly sensitive and should be afforded heightened protections, as noted above. The Discussion Paper's suggestion that an issuing authority could authorise access to certain types of information, without limiting the method used, may not reflect the need to ensure *both* the method of access and the information accessed are necessary and proportionate in connection with the specific investigation.[14] Indeed, the Comprehensive Review expressly recommends maintaining a requirement for agencies to obtain separate warrants for separate methods of access.[15] As such, the Discussion Paper's distinction

[13] Discussion Paper (2021) at p. 33.

[14] It is also unclear from the Discussion Paper how much importance should be placed on methods of collection and their impact on privacy. On page 34, the Discussion Paper suggests "shift[ing] the emphasis from a method-based framework to a more outcome-based framework", but on page 35, the Discussion Paper states that "the method of access will be a key consideration for the issuing authority when assessing the privacy impact of the warrant and its necessity and proportionality."

[15] See Comprehensive Review, Recommendation 76 ("Agencies should continue to be required to obtain separate warrants to authorise covert access to communications, computer access or the use of a listening or optical surveillance device under a new Act. The Act should not introduce a 'single warrant' capable of authorising all electronic surveillance powers.")

between "method-based" and "outcome-based" frameworks, as well as its recommendation to shift from the former to the latter, may not achieve the goal of ensuring access is necessary and proportionate. Instead, the Government should recognise that both the *type* of information sought and the *method* by which it is obtained will create privacy concerns, and should bear both in mind when determining whether to consolidate "functionally equivalent" powers.[16] In addition, any new framework should recognise that different agencies may appropriately be subject to different thresholds and safeguards to obtain information; for example, the requirements for law enforcement and national security agencies should be set at different and appropriate levels. It is important to ensure that both Parliament and the public understand the types of tools that agencies use to obtain information to ensure appropriate oversight of those authorities.

- ***Strictly controlling which agencies may exercise surveillance authorities*** **(Questions 3-4)**. The Discussion Paper recognises 21 Commonwealth, state, and territory agencies that may use electronic surveillance authorities — and contemplates providing additional agencies with such powers when they make a "clear and compelling case."[17] The Discussion Paper highlights a range of such agencies, including those focused on taxation and border measures. This has the potential to significantly expand the use of Australian surveillance authorities — and to the extent the Government does provide such agencies the power to use electronic surveillance authorities, it should carefully consider whether each agency should be provided the ability to use all surveillance authorities, or only a subset. Although providing different agencies with different powers would not achieve a completely uniform framework, it would help to ensure that these authorities are used only as necessary and appropriate given the function of a particular agency and the investigation it is conducting. In addition, to the extent that new powers replace cumbersome existing procedures the Government should consider whether that would result in an overall increased use of surveillance authorities that may or may not be desirable. For example, the consultation includes a case-study noting that for the Australian Taxation Office, additional powers could "potentially replace expensive, resource-intensive and intrusive physical surveillance operations"[18] — which may make them more likely to be used more frequently, increasing the need for additional safeguards and oversight.

Australia Should Implement More Safeguards on the Use of Electronic Surveillance Authorities

One of the main objectives guiding the electronic surveillance reform process is to ensure that "appropriate thresholds and robust, effective and consistent controls, limits, safeguards and oversight of the use of these intrusive powers".[19] BSA agrees that rigorous and consistent safeguards are critical to the appropriate use of electronic surveillance authorities. The exercise of electronic surveillance powers affects important individual rights, most notably the right to privacy, and therefore requires effective control mechanisms and oversight to prevent misuse and abuse.

---

[16] Discussion Paper (2021) at p. 39.

[17] Discussion Paper (2021) at p. 17 (suggesting such agencies may include the Australian Transaction Reports and Analysis Centre (which has a dual financial intelligence and regulatory role focused on the prevention of money laundering and terrorism financing), the Australian Taxation Office (for the purpose of protecting public revenue from serous financial crimes), state and territory corrective services (to monitor criminal offenders), the Australian Border Force (to use tracking devices to investigate border-related measures), and the Australian Criminal Intelligence Commission (to use its powers for a slightly wider range of investigations)).

[18] Discussion Paper (2021) at p. 18.

[19] Discussion Paper (2021) at p. 6.

We are encouraged to see that existing legislative safeguards will be retained in the new framework,[20] and in some cases, strengthened. However, more can be done to promote strong commitments to privacy, security, transparency, and the rule of law, while fostering constructive collaboration between law enforcement and the private sector. BSA encourages the Government to consider the following safeguards:

- **Incorporating principles of specificity, using least intrusive means, and minimisation (Question 23).** Because of the intrusive nature of electronic surveillance, the Government's powers should be used only as necessary and appropriate. The Discussion Paper views this requirement as meaning the exercise of powers must be "aimed at a legitimate and lawful objective and the intrusion on rights and privacy must not outweigh the benefits of that objective."[21] It also suggests the new framework should incorporate an "express requirement" to ensure powers are only used as necessary and proportionate. However, the Discussion Paper appears to anticipate that this will be carried out by requiring the issuing authority to make a determination in each instance about whether the specific use at hand is necessary and proportionate. While that may be an appropriate safeguard, we strongly urge the Government to ensure that other safeguards — including structural limitations on the use of surveillance powers — are built into the new framework to ensure powers used under that framework are exercised in a necessary and proportionate manner. In particular, the framework should incorporate the following principles:

    - *Specificity*. Laws should require that a request for data be as specific and narrowly targeted as possible. A request should articulate details about specific individuals, accounts, devices, and types of data to be targeted, and a specific time period over which they will be targeted. Requests should always be issued in connection to investigation of a specific crime and should include a reasonable justification based on credible and articulable facts.

    - *Least Intrusive Means*. Authorities should also be required to assess whether the data is critical enough to a particular investigation to justify the intrusiveness of the proposed access — and ensure the least intrusive method is used to obtain the data sought. As such, we support the Discussion Paper's suggestion that agencies seeking to invoke interception or surveillance powers should satisfy the warrant issuing authority that the "proposed methods of access are the least intrusive means available that would be effective in the circumstances."[22]

    - *Minimisation*. Authorities should be required to adopt minimisation procedures in connection with requests for access to data to ensure that only relevant data is produced and used. Minimisation procedures should be applied to the acquisition of data to ensure that only that data relevant to an investigation is produced in response to a request. Minimisation procedures should also be applied to the processing, retention, and dissemination of data acquired through requests in order to ensure that (1) data acquired by the agency is returned or destroyed if it is not relevant to the specific investigation for which it was requested; (2) such data is only used for lawful purposes; and (3) data is secured against unauthorised access or disclosure.

[20] Discussion Paper (2021), p. 62. These safeguards include: a) requirements to obtain a warrant or authorisation with appropriately strict thresholds; b) conditions placed on the activities authorised under a warrant; c) independent issuing authorities; d) independent advocates providing submission concerning warrant applications in some circumstances; e) limitations on how agencies can use and disclose information; and f) requirements to destroy information.

[21] Discussion Paper (2021) at p. 51.

[22] Discussion paper (2021) at p. 35.

- **Judicial oversight (Question 28).** Judicial oversight is a key enabler of the rule of law. We welcome the Discussion Paper's recognition that a new framework will continue to require law enforcement warrants be authorised by an appropriate independent authority.[23] BSA suggests that laws addressing government access should ensure that prior review by an independent judicial authority is available for any order (1) authorising government access to content data, other sensitive data, or technologies produced or controlled by businesses, or (2) mandating that businesses take specific actions impacting data or technologies. Although the Comprehensive Review contemplates that the activities of the Australian Security Intelligence Organisation (**ASIO**) will continue to be authorised by the Attorney-General,[24] we are encouraged by the recognition that additional judicial authorisation requirements should be imposed for international orders sought by ASIO. Specifically, the Discussion Paper recognises that any legal processes issued to businesses in the United States must meet requirements of the CLOUD Act, which requires orders to be "subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order."[25]

- **Right of appeal for businesses (Question 28).** As one aspect of ensuring judicial review, businesses subject to electronic surveillance orders should have the opportunity to challenge these orders before an independent judicial authority based on factors relating to feasibility, legality, propriety, and international comity. This is especially important in a situation where an infeasible or impractical order is issued to a provider, making it impractical or impossible for the business to comply. For example, a law enforcement agency may secure a warrant to compel a technology provider to disclose certain information about the provider's customer — but it may do so based on the mistaken understanding that the technology provider collects a specific type of data. If the technology provider in that case does not collect such data and cannot comply with the order, it may still be unable to convince the agency that it cannot comply — and could be found non-compliant with the order. In this scenario, the technology provider should be able to seek judicial review. The new framework should therefore include a judicial review process that permits businesses to challenge orders before an independent judicial authority.

- **Creating a centralised oversight authority (Questions 30-31).** The current framework draws a clear distinction between the oversight authorities for intelligence agencies and law enforcement agencies. The Inspector-General of Intelligence and Security (**IGIS**) oversees the activities of intelligence agencies such as the ASIO, whereas oversight of the law enforcement agencies' use of electronic surveillance powers is shared by the Commonwealth Ombudsman and "a range of state and territory oversight bodies".[26] To promote consistent oversight and to ensure all agencies that may exercise electronic surveillance authorities do so in an appropriate manner, we suggest consolidating the IGIS and the Commonwealth Ombudsman into a single, centralised body with oversight functions over the use of electronic surveillance powers in *all* instances. This can facilitate consistency in oversight and ensure all agencies that exercise surveillance powers are accountable to the same high standards. The consolidation of regulatory experience and technical expertise will also increase operational efficiency by cutting down on inter-agency coordination, which can impede oversight duties. The precedent for this approach is the United Kingdom's (**UK**) Investigatory Powers Commissioner's Office (**IPCO**). In his report on the Telecommunications and Other Legislation Amendments (Assistance and Access) Act 2018 and related matters,[27] the Independent National Security Legislation Monitor (**INSLM**) noted that the IPCO performs the

[23] Discussion Paper (2021) at 53.

[24] Discussion Paper (2021) at 54.

[25] See CLOUD Act, 18 U.S.C. 2523(b)(4)(D)(v).

[26] Discussion Paper (2021), p. 64.

[27] Trust But Verify: A report concerning the Telecommunications and Other Legislation Amendments (Assistance and Access) Act 2018 and related matters, Dr James Renwick CSC SC, June 2020, at https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf (**INSLM Report**).

functions undertaken in Australia by the IGIS and the Commonwealth Ombudsman.[28] The IPCO itself was formed by merging three precursor organisations.[29] The INSLM found that the IPCO was crucial in raising public trust and confidence in the exercise of electronic surveillance powers in the UK, and that a key part of its success is that the Investigatory Powers Commissioner and the judicial commissioners have "become very familiar with the work and the technology used by the agencies seeking the issue of intrusive warrants and bring that knowledge to bear in considering subsequent applications, ensuring both insight and efficiency."[30] Creating a centralised oversight authority based on this model can similarly lead to more efficient discharge of oversight duties and engender greater trust in the population regarding the use of electronic surveillance powers.

- **Record-keeping and reporting (Questions 32-33).** Record-keeping and reporting requirements promote transparency about how electronic surveillance authorities are used and enable effective oversight. We agree with the Discussion Paper that Australia's current requirements could be revised to "ensure they support effective and meaningful transparency, accountability and oversight."[31] As a matter of practice, governments should regularly record and publish aggregate data on the number, purposes, legal authorities, and outcomes of law enforcement requests for digital evidence issued by law enforcement agencies in a covered timeframe. In this regard, while we note that both law enforcement agencies and the ASIO have reporting obligations, including a requirement to provide annual reports,[32] BSA supports including additional information in those reports. **Specifically, we recommend implementing recommendations in the Comprehensive Review to add the following information to the publicly available reports:[33]**

    - the use of electronic surveillance information in the hearings and reports of integrity agencies, in addition to its use in evidence in prosecutions — to ensure that the report provides a more complete picture of the purposes for which surveillance information is used;

    - the number of people who have been the subject of electronic surveillance, in addition to the number of warrants and authorisations issued — to ensure that the report provides more meaningful information about the extent of the use of surveillance powers; and

    - the number of occasions where issuing authorities have required agencies to provide further information in support of warrant applications or issued a warrant in terms other than those initially sought by the agency, in addition to the number of warrants issued and refused — to ensure that the report more accurately reflects the role that issuing authorities play in scrutinising applications.

  In addition, the review should ensure that businesses are not restricted from publishing their own aggregate data on the number, origin, and outcomes of orders to assist with electronic surveillance. Publication of this information fosters greater transparency and trust between businesses and their customers.

- **Pre-issuance consultations with businesses and notification of data subjects.** As previously highlighted, BSA is concerned with situations in which an order is issued to a business, but it is

[28] INSLM Report (2020), paras 2.31 and 11.21(d).

[29] The previous organisations were the Office of Surveillance Commissioners, the Interception of Communications Commissioner's Office, and the Intelligence Service Commissioner's Office.

[30] INSLM Report (2020), para 11.18.

[31] Discussion Paper (2021), p. 67.

[32] Discussion Paper (2021), p. 67-68

[33] Comprehensive Review (2020), Vol 2. p. 440.

neither practicable nor feasible for the business to comply with that order. This situation can arise when the affected business has no ability to comment on the order until after it has been issued. This is a significant weakness in the process, as the best entity to assess if a request is technically feasible is the technology provider itself. In addition, the business is the only entity capable of assessing whether its systems contain the data sought. As such, BSA supports implementing a process that supports consultation with businesses ***prior to*** the issuance of an order. Relatedly, a technology provider subject to an order should not be restricted from notifying the subject of a data request unless non-disclosure is justified on an exceptional basis for a limited duration. Any new framework should ensure that businesses have the right to request further information from an agency or object to non-disclosure requirements when such notification is prohibited.

Conclusion

We thank the DHA for the opportunity to comment on the reform of Australia's electronic surveillance framework and appreciate DHA's consideration of our above comments. We hope that our concerns and recommendations will assist in the development of enduring solutions to electronic surveillance authorities in Australia.

Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Tham Shen Hong
Manager, Policy – APAC

The Software Alliance

BSA

BSA Global Best Practices for Law Enforcement Access to Digital Evidence

As the types and volume of data proliferate, digital evidence is increasingly important to law enforcement agencies. While the value of digital evidence to criminal investigations has grown substantially, so, too, have challenges in accessing it. Incomplete legal structures, insufficient law enforcement capacity, and underdeveloped investigatory processes often hamstring investigations and create unnecessary tension between law enforcement agencies and technology providers. Policymakers, law enforcement agencies, and technology providers should work collaboratively to shape laws, policies, and procedures that enable access to digital evidence in alignment with robust protections for due process and civil liberties, and that ensure providers can meet their obligations to their customers.

BSA recommends the following best practices relating to law enforcement access to digital evidence for policymakers, law enforcement agencies, and technology providers. These best practices promote strong commitments to privacy, security, transparency, and the rule of law, while fostering constructive collaboration between law enforcement and technology providers in activities aimed at fighting crime and making communities safer.

Best Practices for Governments and Law Enforcement Agencies

Law enforcement agencies have access to more data than at any time in history. Accessing that data can present tremendous challenges to the privacy and security of technology users unless law enforcement investigations are guided by carefully crafted laws, policies, and procedures. BSA recommends the following best practices to policymakers and law enforcement agencies. The best practices would empower criminal investigators to access digital evidence without compromising the security of the technology or the safety, rights, and opportunities of citizens. The best practices are organized around five guiding principles: safeguarding fundamental rights, narrowly targeting requests, cooperating across borders, ensuring transparency, and maintaining collaborative relations with technology providers.

THE RISING IMPORTANCE OF DIGITAL EVIDENCE

Over the last 30 years, data sources have exploded. Billions of individuals have moved from telephone and written communications to digitally transmitted and stored emails, text messages, phone calls, instant messages, social media postings, and other communications. The European Commission now estimates that electronic evidence is needed in roughly 85 percent of criminal investigations, and in more than half of all criminal investigations law enforcement agencies require access to electronic evidence stored outside their country's borders. In the US, the Federal Bureau of Investigation has found that the average digital forensic examination can yield nearly a terabyte of data — equivalent to 250,000 pages of typewritten documents.

Safeguarding Fundamental Rights

The first obligation of governments and law enforcement agencies is to the citizens they protect. Laws and policies should ensure that safeguards for the rights and liberties of citizens are incorporated at all stages of law enforcement investigations involving digital evidence.

Judicial Review. Laws should ensure that prior review by an independent judicial authority is available for any order (1) authorizing government access to content data, other sensitive data, or technologies produced or controlled by technology providers, or (2) mandating that technology providers take specific actions impacting data or technologies. Technology providers subject to such an order should have the opportunity to challenge it before an independent judicial authority based on factors relating to feasibility, legality, propriety, and international comity.

Privacy. Laws should establish robust substantive and procedural protections for privacy and civil liberties in connection to data requests and their fulfillment, including measures to protect fundamental rights to free speech and expression; prevent extralegal search and seizure of digital evidence; bar use of unlawfully obtained evidence in criminal proceedings; and prohibit bulk collection of content data.

Due Process. Laws should protect due process, including the right to fair trial, the presumption of innocence, prohibitions against arbitrary arrest and detention, and judicial redress.

Emerging Technologies. Emerging technologies often create new data sources not anticipated by existing policies. Policymakers should continue to update laws to ensure emerging technologies and associated data are covered by the same robust privacy and due process protections as traditional sources. Data from facial recognition technologies, home assistant software, and medical Internet of Things devices offer current examples of emerging data sets that should be covered by protections similar to those generally afforded to content information.

Narrowly Targeting Requests

Law enforcement agencies should target requests only to information vital to an investigation and develop such requests through appropriate legal processes. Doing so not only builds confidence among citizens in the authorities and activities of the investigators but also improves the efficiency and effectiveness of the investigations themselves.

Specificity. Laws should require that a request for data be as specific and narrowly targeted as possible. It should articulate details about specific individuals, accounts, devices, and types of data to be targeted, and a specific time period over which they will be targeted. Requests should always be issued in connection to investigation of a specific crime, and should include a reasonable justification based on credible and articulable facts.

Content vs. Non-Content. With regard to accessing stored data, laws should create a distinction between content data and non-content data, and tailor legal processes to each category in ways that ensure robust due process and privacy protections. Content data includes the content of an electronic exchange. It requires special safeguards because of the particularly intrusive and sensitive impact of third-party access to that data. Non-content data encompasses subscriber data (information on the identities of the senders and recipients of an electronic exchange) and traffic data (metadata including the timing, frequency, and duration of such an exchange).

Real-Time Access. Laws should establish a high procedural threshold for authorizing real-time access to traffic data, conduct of remote searches, and interception of content data; such access should require a search warrant or equivalent order approved by an independent judicial authority.

Minimization. Laws should require that law enforcement agencies adopt minimization procedures in connection with requests for access to data to ensure that only relevant data is produced and used. Minimization procedures should be applied to the acquisition of data to ensure that only that data relevant to an investigation is produced in

response to a request. Minimization procedures should be applied to the processing, retention, and dissemination of data acquired through requests in order to ensure that (1) data acquired by the law enforcement agency that is not relevant to the specific investigation for which it was required is returned or destroyed; (2) such data is only used for lawful purposes; and (3) data is secured against unauthorized access or disclosure.

Cooperating Across Borders

Cross-border cooperation is necessary to enable law enforcement agencies to access data, which is increasingly stored in facilities dispersed around the world. Moreover, such cooperation provides mechanisms to reinforce procedural protections and legal safeguards.

Comity Analysis. Policymakers should ensure that their governments have a process in place to identify potential conflicts of law prior to the issuance of requests, incorporate comity analysis into judicial proceedings regarding the issuance and enforcement of requests, and provide opportunities for impacted stakeholders to provide comity analyses relevant to their position in such proceedings.

Notification. Governments should notify a foreign country — either where the data is located or where the person of interest resides — when its law enforcement agencies are requesting access to digital evidence stored in the foreign country, and to grant the foreign country and technology provider the opportunity to object.

International Agreements. Governments should establish procedures and mechanisms for accepting and responding to requests under mutual legal assistance treaties on a timely basis, including, where feasible, digital portals for accepting requests. In addition, to the extent feasible, governments should establish or negotiate other mechanisms, including bilateral and multilateral international agreements, to facilitate cross-border law enforcement access to data under appropriate circumstances.

Data Localization. Policymakers should avoid data localization mandates for the purposes of ensuring law enforcement access to data, to avoid myriad unintended negative consequences data localization policies often generate. The data storage location should not be the governing factor in establishing jurisdiction or access rights.

Ensuring Transparency

Transparency is vital for sustaining public confidence in the authorities granted to law enforcement agencies and the conduct of the agencies in executing those authorities.

Notification of Data Subjects. Technology providers should not be restricted from notifying the subject of a data request unless non-disclosure is justified on an exceptional basis for a limited duration. Procedures should ensure that technology providers have the right to request further information or object when such notification is prohibited.

Public Reporting. As a matter of practice, governments should regularly publish aggregate data on the number, purposes, legal authorities, and outcomes of law enforcement requests for digital evidence issued by law enforcement agencies in a covered timeframe. Technology providers should not be restricted from publishing aggregate data on the number, origin, and outcomes of law enforcement requests for digital evidence they receive in a covered timeframe.

Maintaining Collaborative Relations With Technology Providers

Building collaborative relationships that recognize the equities of all stakeholders involved provides the most effective way to ensure sustainable, effective mechanisms to access digital evidence in accordance with the law.

Controllers vs. Processors. When requesting access to digital evidence, law enforcement agencies should seek data first from the data controllers, which determine the means and purposes of processing personal data, before going to data processors, which process data on behalf of data controllers.

Technical Capabilities. Technology providers should not be required, under any circumstances, to alter or weaken technologies, or to build or modify technical capabilities, in ways that risk creating systemic weaknesses or vulnerabilities. Specifically, no law or policy should obligate technology providers to create access to security technologies such as encryption mechanisms, to implement technical measures to enable law enforcement to access encrypted communications, or to maintain a capability to decrypt protected communications.

Rights of Technology Providers. Laws should establish that technology providers cannot be held liable for responding to lawful government requests for data and should include protections to prevent intellectual property, trade secrets, and other proprietary and sensitive information (including source code) from being exposed as a result of law enforcement requests.

Request Verification. Law enforcement and government agencies should ensure that request recipients are able to establish viable processes to verify the validity and accuracy of law enforcement requests for data.

BSA Recommendations for Technology Provider Best Practices

Technology providers play an important role in responding law enforcement efforts to requests for digital evidence in criminal investigations, but legal and procedural shortcomings can also undermine their ability to do so. Providers are obliged to protect the trust and confidence of their customers, including in relation to customer privacy and security, and cooperation with criminal investigations should not compromise these investigations.

Not all technology providers receive law enforcement requests in significant numbers; but those that do should follow best practices described below to improve responsiveness to legitimate law enforcement requests while sustaining commitments to customers around privacy and security.

Accessibility and Standardization. Technology providers should maintain a clearly identifiable online mechanism to receive law enforcement requests for data and to provide dated, electronic confirmation of receipt of the request. Technology providers should also strive to standardize request forms.

Responsiveness. Technology providers should establish a policy requiring, absent exceptional circumstances, an initial response to general law enforcement requests within a reasonable and defined timeframe. The policy should also outline expectations for accelerated response to designated law enforcement requests in exigent circumstances involving danger of death or serious physical injury to any person.

Point of Contact. Technology providers should identify a single point of contact or contact mechanism that ensures accountability for the processing of and response to law enforcement requests. Further, they should maintain a mechanism for law enforcement agencies to communicate promptly with appropriate personnel in the event of an emergency.

Guidance. Technology providers should maintain and make public up-to-date, complete guidance on the types of data law enforcement agencies may access with appropriate authorization and the procedures for accessing it.

Training. Technology providers should, where relevant, provide training to law enforcement agencies at the federal, state, and local level and to prosecutors and judges on the types of data that may be available via their platforms or services, methodologies for appropriately specifying data requirements, considerations about privacy and feasibility, and other relevant matters.

Notification. Absent exceptional circumstances, including imposition of non-disclosure requirements by a requesting government, technology providers should notify data subjects when they receive a law enforcement request for the data subject's data.

Privacy. Technology providers should establish policies and mechanisms to prevent over-responsiveness; customers' data should be provided to law enforcement agencies only in connection to legitimate criminal investigations and only in response to properly authorized requests made in accordance with appropriate laws and court orders. Only the information that is relevant to and specifically authorized by their submitted request should be provided.