Atlassian's Submission to the Department of Home Affairs in relation to the Reform of Australia's Electronic Surveillance Framework Discussion Paper

Electronic Surveillance Reform Branch
Department of Home Affairs
electronicsurveillancereforms@homeaffairs.gov.au

11 February 2022

We appreciate this opportunity to provide feedback to the Department of Home Affairs on the proposed reform of Australia's electronic surveillance framework, as set out in its Discussion Paper (the **Discussion Paper**).

Atlassian welcomes this foundational review and reform process, which builds upon the Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community (**Comprehensive Review**), as well as several recent inquiries and reviews conducted by the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**). This includes the PJCIS's reviews of the industry assistance measures set forth in the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth), which Atlassian (and others in our technology sector) previously participated in.

At Atlassian, we build enterprise software products to help teams collaborate, including for software development, project management and content management. As one of Australia's most successful home-grown technology companies — and one that provides products and services to customers around the world — we believe that we are in a unique position to comment on these reforms.

We know the critical role of data and information in powering the operations of our customers, and the digital economy more broadly. We appreciate that access to this information is important to combat serious crime and threats to national security, and to ensure the safety and security of all Australians. However, in designing when and how such access should be granted, it is equally critical to ensure the ongoing integrity, security, privacy and trustworthiness of our digital economy, our technologies, and the individuals and organisations who participate in and benefit from them.

We believe that these reforms present an ideal opportunity for the Government, in detailed consultation with stakeholders, to carefully assess and respond to these critical needs in a considered and holistic manner and build community and industry trust in the use of surveillance powers.

Our approach and key principles

In late 2020, Atlassian published eight Principles for Sound Tech Policy,[1] which are attached to this submission. These Principles are intended to not only guide Atlassian's own engagement on important matters of public policy, but to set forth guiding principles for what we believe sound technology-related public policy should look like more broadly.

[1] These Principles are also available for download at https://www.atlassian.com/blog/technology/regulating-technology.

Atlassian is also a founding signatory to the Trusted Cloud Principles,[2] together with several other enterprise cloud service providers (**ECSPs**). The Trusted Cloud Principles set forth our commitments to working with governments to ensure the free flow of data, to promote public safety, and to protect privacy and data security in the cloud.

In line with each of those Principles, we welcome and support the overall objectives of the reform as set out in the Discussion Paper, including the need for simplification and harmonisation of our current laws and for a unified, privacy-centric approach to be at the heart of any new framework. Further to Atlassian's fourth principle [*Consult early, consult openly*], we also appreciate that the reforms have commenced with an early, comprehensive and principles-based consultation on how this new legislative framework will operate. We look forward to further detailed consultation as the framework is further developed.

Through the lens of these Principles and our perspective on and approach to our electronic surveillance framework, this submission considers the matters raised in the Discussion Paper and proposes the following core objectives for these reforms:

- ***Access should always relate to a person that is the subject of the surveillance***. We recognise that the current electronic surveillance framework, which focuses on methods of access, is complex and inefficient to navigate. In rethinking this framework and considering *what*, *how* and *when* information may be accessed (as set out in Parts 2 to 4 of the Discussion Paper), clear guardrails and guiding principles are critical to ensure that the new framework is proportionate and able to properly protect individuals' security, privacy and control over their data. In line with Atlassian's first principle [*Define the playing field*] and third principle [*Treat the ailment, don't kill the patient*], we believe a careful, targeted and consistent view of the subject of the surveillance in each case will help to meet these aims.
- ***Access should be sought at a level as close to the subject of the surveillance as possible***. As technology and communications supply chains become more complex, multiple avenues to obtain access to information may be available. For example, an ECSP like Atlassian may store or process the data of its enterprise customers, who control that data on behalf of their own individual end customers or users. In line with the Trusted Cloud Principles as well as Atlassian's third principle [*Treat the ailment, don't kill the patient*], agencies should always seek to request information from the enterprise customer in the first instance, and specify a clear process for any narrow exceptions that may apply. We set out what this process could look like in this submission below.
- ***The processes for obtaining access should be centralised where possible***. In order to best realise the benefits of a more streamlined, transparent and usable framework, it will be critical to ensure that requesting agencies have the information and expertise that they need. In line with Atlassian's second principle [*Engage with the issue, don't dumb it down*] and fifth principle [*Let the light in*], we believe that centralising these access requests through one or more 'clearinghouse' agencies would ensure that access requests benefit from increased consistency, clarity and technical know-how. This would then result in requesting agencies being able to more efficiently and effectively obtain the information and data that they need, and recipient organisations being able to more easily understand and respond to these requests. Further, the aggregation of these access requests through a centralised mechanism will provide stakeholders with a clearer and more comprehensive view of the access that is being requested, contributing to more accurate assessments of the necessity and proportionality of these requests.
- ***Requests for access should be subject to (centralised) independent review and authorisation***. Similarly, in order to ensure meaningful and effective oversight of our electronic surveillance regime, robust and effective controls and safeguards are

[2] These Principles are available at https://trustedcloudprinciples.com.

essential. In line with Atlassian's fifth principle [*Let the light in*], we believe that an independent review and authorisation process, which is able to benefit from the concentration (and further development) of expertise and experience in reviewing access requests over time, is best able to respond to these needs. We detail how this objective can be met in this submission below.

We believe that the application of these objectives to the matters covered in the Discussion Paper will result in an overall framework that is clear, usable and reliable not only for industry participants like Atlassian, but for the operational agencies and oversight bodies that need to grapple with the use of these increasingly complex surveillance powers on a daily basis. This would ultimately also help to realise Atlassian's eighth principle [*Build the foundation for shared success*].

Access requests and ECSPs

Objective: Access should be sought at a level as close to the subject of the surveillance as possible.

Atlassian appreciates that the new framework seeks to deliver a modernised, streamlined and integrated system for electronic surveillance powers, and that the Discussion Paper clearly identifies the importance of considering the full range of communications providers (broadly defined) to which the framework should apply. We agree that this approach will ensure that the new framework operates effectively and as intended, instead of creating ambiguities or uncertainty for industry stakeholders and authorities.

As part of this approach, it is important to recognise and account for the contexts in which some communications providers will encounter and interact with the electronic surveillance framework, which differ significantly from the more traditional communications service providers that have historically been subject to and part of this framework.

In particular, ECSPs face unique challenges relative to other providers, due to the nature of the products and services they provide, their relationships with their enterprise customers, and the manner and context in which they hold information and data that may be subject to the framework. ECSPs handle very high volumes of commercial and private information provided by or relating to their enterprise customers who may be located across the globe. This means that, in the development of powers seeking data from ECSPs, governments must be mindful that:

- Data held by ECSPs is often unique in its breadth and depth. This data is often a mix of personal information, financial information, commercial information and other highly sensitive or confidential information. Further, because customers of ECSPs typically operate across multiple jurisdictions, they hold information and data originated from a range of jurisdictions.
- Enterprise customers of ECSPs are themselves entities which may be the subject of requests for information. They will have significant legitimate concerns about maintaining the privacy and security of their information, as well as their own processes and preferences for responding to these requests. Where it is not clear to those customers how requests for access to their information may be fielded (and responded to) by their ECSPs in particular jurisdictions, this can lead to a breakdown in trust between customers and their ECSPs in those markets.
- Equally, enterprise customers are likely to have their own complex supply chains, of which any single ECSP is only one link in that chain. Where information is sought about a customer of an ECSP, it is therefore unlikely that any one ECSP will itself hold all relevant information when contrasted with the customer itself.

Given these factors, Atlassian believes that it is appropriate for the revised electronic surveillance framework to clearly set out the circumstances and processes through which enterprise cloud service providers will be expected to receive and handle requests for access to customer information.

We recommend that these processes would involve the following key features.

Access to customer information should generally be requested from the customer in the first instance (and not a provider with secondary access to such information).

In addition to the Trusted Cloud Principles and Atlassian Principles outlined above, we believe that this default approach would align with the principle of necessary and proportionate authorisation of powers considered in the Discussion Paper, and minimises the intrusion on privacy relative to requests of the same information from an ECSP.

Where such requests are made within a target- and outcomes-based framework as contemplated in the Discussion Paper, we believe that a default approach whereby the enterprise customers themselves directly receive and respond to requests for access to their information in the first instance would require, and result in:

- clearer and more accurate consideration of privacy impacts, the reasonable nexus of the request to the investigation at hand and justification of methods; and
- greater efficiency and speed for the enterprise customer, ECSP and the requesting agency.

Recognising that there are some limited situations where requests need to be made to an ECSP, these should always be clear and demonstrated justification for such requests.

There may be some situations where operational agencies will nevertheless need to issue a request for access to customer information to an ECSP rather than to the customer itself. Atlassian believes that this should only be the case in limited, specific circumstances, that is:

- where the customer has considered the initial request, and considers it necessary and proportionate for the ECSP to receive a similar request for access to the relevant information the subject of that initial request;
- where the customer refuses to assist or where, after a reasonable time has passed, the customer has failed to assist;
- the enterprise customer itself is the subject of the investigation; or
- where other exceptional circumstances apply, such as secrecy requirements or national security considerations which mean that it would be prejudicial to disclose the request to the customer itself.

Further, Atlassian considers it appropriate for the operational agency issuing the request to specify and prove in the application for the use of electronic surveillance powers:

- the limited circumstances under which it is necessary and proportionate to issue a request for customer information to an ECSP;
- if an initial request has been made to the customer to which the relevant information relates, why the operational agency and/or customer consider it necessary and proportionate for the ECSP to provide access rather than the customer (noting that ECSPs should not receive requests for access, or technical assistance or capabilities, as a matter of mere commercial convenience from the customer’s perspective);
- if no initial request has been made to the customer to which the relevant information relates, the applicable exceptional circumstances and (depending on the relevant circumstances) the extent to which the ECSP can or cannot disclose the receipt of such request to the customer; and
- the specific nature of the customer information sought, as ECSPs handling customer information must be able to handle requests in a manner that minimises intrusions of privacy and provides certainty to customers regarding the information provided.

Given the intrusive nature of electronic surveillance powers and the environment in which ECSPs operate in relation to customer information, the onus should always be on the operational agency to justify the necessity and proportionality of seeking customer information from an ECSP. This will also be essential to provide certainty to the Australian and international technology sector regarding the specific circumstances under which ECSPs will be asked to provide access to customer information.

The framework should include default presumptions about how an ECSP will handle such requests in the context of the relationship between the customer and the ECSP.

Where a request for access to customer information is issued to an ECSP, it will also be helpful to for the new framework to include default presumptions about how an ECSP will handle such request with respect to the relationship between the customer and the ECSP.

Most importantly, given the context in which the ECSP holds the customer information and as set forth in the Trusted Cloud Principles, the ECSP should be able to disclose the request for access to, and engage with, the customer (and its advisors) while handling such request by default. Any exceptions to this default presumption should only apply in specific defined circumstances; namely, where there is a reasonable nexus to the reason why the ECSP has received the request (for example, secrecy requirements where the customer has no knowledge of an investigation). It may also be helpful to specify the extent to which a customer may remain involved in the ECSP's response to a request.

These default presumptions would provide significant certainty to both ECSPs and their enterprise customers regarding the compliance requirements and practical procedures required by the new framework, and ensure that the requests for access to customer information are handled in a way that meets industry expectations.

The criticality of appropriate review mechanisms for all requests

Objective: Requests for access should be subject to (centralised) independent review and authorisation.

In considering appropriate review and oversight mechanisms for requests under the reformed electronic surveillance framework, we believe that principles raised through earlier consultation and review processes relating to the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (**TOLA**) are applicable and relevant in this context. We also consider that the solutions identified through the TOLA processes are equally applicable to the framework contemplated by the Discussion Paper.

Further to our previous submissions to the PJCIS and the Independent National Security Legislation Monitor (**INSLM**) in relation to their reviews of TOLA, Atlassian considers it critical that our electronic surveillance framework include a mandatory 'double-lock' oversight and authorisation mechanism that is:

- applicable to all warrants, requests and information or assistance orders relating to any form of electronic surveillance, from all requesting authorities and agencies;
- entirely independent from the operational agencies issuing requests, to ensure that a single organisation or chain of command within government does not have decision-making power for both the initial issuance and the subsequent review or approval of a request; and
- informed and supported by both legal and technical expertise, to ensure appropriate decision-making, through the making of binding decisions based on a full understanding of all legal and technical complexities of the electronic surveillance powers and their application to the matter at hand.

An independent and robust mechanism of this type will be critical in ensuring both public and industry confidence, domestically as well as internationally, in any new electronic surveillance framework. The expertise and experience that will be applied (and developed) through the use of this mechanism will also contribute towards ensuring that operating agencies are able to issue clearly tailored and effective requests to providers that can more easily comply with and understand their obligations under the new framework. Review mechanisms will also assist providers to clarify or manage disputes in relation to technical or complex aspects of these requests.

We also support the view of the Comprehensive Review that any oversight models should be integrated into legislation at an early stage, rather than being addressed at a later point and considers that this will be a crucial factor in increasing public and industry confidence in a new framework.

Ultimately, Atlassian firmly believes that giving extensive consideration to, and implementing, these measures will be to the benefit of all stakeholders and Australians.

We support the INSLM's proposal to implement this mechanism via an IPC.

We consider that this objective can be achieved either through the judiciary or the establishment of an Investigatory Powers Commissioner (**IPC**), as extensively outlined by the then-INSLM, Dr Renwick, in the '*Trust But Verify'* review and report on TOLA.

In brief, under Dr Renwick's proposed model, the IPC would be a retired judge heading a new Investigatory Powers Division of the Administrative Appeals Tribunal (**AAT**), supported by a pool of legal and technical experts as part-time AAT Deputy Presidents and Senior Members respectively. Dr Renwick considered that this model would best allow these members to develop the necessary policy and technical expertise in considering electronic surveillance requests, and to allow for appeal of decisions by communications providers.

The IPC model is based on the Investigatory Powers Commissioner's Office (**IPCO**) in the UK, which Dr Renwick considered at length and concluded worked well in theory and practice. In particular:

- Dr Renwick found that the IPCO was crucial in raising public trust of and confidence in the electronic surveillance powers in the UK and the authorities' use of them.
- This was due in part to its Technical Advisory Panel (**TAP**), which provided technical expertise both generally and in relation to the exercise of investigatory powers, particularly in relation to privacy impacts. Dr Renwick suggested that a standing pool of experts would support this more than the occasional appointment of ad-hoc technical experts and that familiarity with both the technical subject matter and the new framework would be a significant advantage to the IPC's decision-making capacity.
- Ultimately, Dr Renwick attributed much of the success of the UK model to the fact that '*the IPC and the judicial commissioners 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*'.

In the TOLA context, Dr Renwick considered that the proposed IPC would operate to authorise the initial issuing of technical assistance notices and technical capability notices. We agree with Dr Renwick's conclusions and further believe that, given the legal and technical expertise that would be built up within the IPC model, this body would also be appropriate in playing a broader role in relation to authorisations and reviews across the unified framework contemplated by the Discussion Paper.

We note that the PJCIS, in its review of TOLA, also found that appropriate oversight and accountability mechanisms are '*critical in ensuring the public's ongoing confidence in the use of the powers*', and provide both industry and operating agencies with assurance on how these powers will be used and applied. The PJCIS also acknowledged the benefits of a double-lock model, noting the UK IPCO model, and concluded that the Government should give further consideration to the INSLM's recommendations in this respect.

Ultimately and on balance, we believe that the establishment of an IPC to head a new Investigatory Powers Division of the AAT (supported by a pool of legal and technical experts as part-time AAT Deputy Presidents and Senior Members) with a remit applying to all warrants, assistance requests or other authorised orders issued by any relevant authority, will best meet this objective.

However, this mechanism can also be implemented through the judiciary if preferred.

Notwithstanding this conclusion, Atlassian would also support a judicial solution or implementation of this double-lock mechanism if the INSLM's proposal is not supported.

Although we do not agree with the Department of Home Affairs' earlier statements, in its submissions to the PJCIS's review of TOLA, that the INSLM's recommendations would not be suitable because of the way in which they depart from the '*usual processes of the AAT*', if the establishment of a new division of the AAT is not the Government's preference, then there remains a clear judicial path forward to implementing a double-lock mechanism.

There are undoubtedly challenges with a court exercising such powers through the need to ensure separation of judicial power from the executive and legislature. However, there is no 'bright line' defining this boundary, and we think these challenges are manageable. There are present-day examples of the inclusion within the scope of judicial power of traditional functions of the courts which are not limited to hearing and deciding disputes. It is also the case that some functions are administrative in the hands of an administrative agency and judicial in the hands of a court. Judges of the Federal Court, for example, routinely carry out many non-judicial functions and sit with non-judicial members on various tribunals. There is also the option, as discussed by Dr Renwick, of ensuring that appropriate members of the judiciary exercise their function in such matters *persona designata*.

While Atlassian believes that there are options in how such a body is constituted, we ultimately believe that such a double-lock mechanism is a critical step in building trust in a reformed framework for electronic surveillance. We also strongly believe that law enforcement and national security agencies will benefit significantly in the concentration of expertise in the use and authorisation of such powers, given the increasing complexity in both technology and the methods of surveillance.

Further recommendations

Atlassian is a proud founding member of the Technology Council of Australia. In addition to the principles and recommendations set out above, we endorse the specific recommendations set forth in the submission provided by the Technology Council to the Department of Home Affairs.

Atlassian would be pleased to discuss these comments with the Department of Home Affairs, and is committed to working with the Government and other stakeholders to ensure that our electronic surveillance laws are best able to meet the objectives and guiding principles set forth in the Discussion Paper.

Yours sincerely,

David Masters
Head of Global Policy & Regulatory Affairs
Atlassian

Anna Jaffe
Director of Regulatory Affairs & Ethics
Atlassian

Atlassian
Public Policy

Atlassian Principles for Sound Tech Policy

Table of Contents

Atlassian Principles for **Sound Tech Policy**

Preamble

We at Atlassian are strong believers that the future of human endeavour and economic prosperity will increasingly flow from innovation and technology. And as 2020 has shown us, ever-greater digitisation is not only tomorrow's trend, but also today's urgent requirement.

But the pace of technology development means that all of us – individuals, private industry and government – must together develop policy frameworks that unleash the positive potential of technology for society while reducing any negative effects.

We know that developing a sound policy framework requires carefully considering the interests and rights of all vested stakeholders, as well as the potential impacts on them. This complex undertaking requires dedicated planning and process--as well as guardrails for the ultimate result. It is not surprising then that sometimes such policy efforts come up short of their intended aims.

This is why we think it is time for a reset on the conversation around tech regulation--one that fully encompasses the positive contributions of the tech sector to society, the legitimate regulatory requirements of government and protection of individual rights, as well as the need for a consistent and reliable environment for shared economic prosperity.

To contribute to this renewed conversation, Atlassian offers the following set of guiding principles to help government, industry, and the public converge on the essential qualities of sound regulation in the technology sector. If implemented, we believe that these guiding principles will result in targeted and proportionate policies, informed by a collaborative process, that ultimately unleash the positive potential of technology while fully addressing individual and societal interests – a true "win win" outcome for all of our communities.

Lastly, as these Principles make clear, we believe that collaboration is key to sound tech policy. As part of our drafting process, we engaged with numerous members of the tech sector, industry associations, and civic organizations who share our common vision. But to ensure that collaboration and improvement can continue even after publication, we are licensing these Principles under a **Creative Commons** license, so that others can adopt, modify and build upon these ideas as the dialogue continues.

Atlassian Principles for **Sound Tech Policy**

I. Define the playing field

Sound tech policy should have clear objectives. This means that everyone should be able to understand the specific problems that regulation seeks to solve, or the interests it seeks to support. More importantly, the regulatory solution should be clearly targeted at that identified problem. Unclear intent breeds distrust and concern.

II. Engage with the issue, don't dumb it down

Sound tech policy should be developed with a clear understanding of the relevant technology. Lawmakers and regulators may not all be technical experts, but if they engage with these experts and other stakeholders to understand the relevant technology and business models, they will be better positioned to respond to them through regulatory means. This can assist in identifying which regulatory means can be used effectively, and which ones are impractical or overly burdensome.

III. Treat the ailment, don't kill the patient

Sound tech policy should be proportionate, and should always seek to minimise unintended consequences. If regulatory responses are not properly considered and tested, they can overreach or lead to unintended and undesirable consequences. These consequences can be just as devastating to companies and their users as failing to act at all. Regulations should be surgical; government should not use a regulatory hammer where a scalpel is appropriate for its goals.

IV. Consult early, consult openly

Sound tech policy should be developed through open, consultative processes. When all relevant stakeholders are engaged early in regulatory processes, potential risks and unintended consequences can be identified and addressed before decisions are made. Open engagement also fosters greater trust in regulatory processes and creates space for both sides to clearly state their objectives or concerns. Early and extensive consultation is an obvious way to try to mitigate against a lack of understanding of the relevant technology or the business model of companies, and the consumer use cases. It also helps governments to ensure that regulations are as effective as possible.

V. Let the light in

Nothing is more uncertain than "black box" exercise of government discretion outside of the public eye. Sound tech policy should provide for transparency in government decision-making and set forth fair procedures that allow meaningful challenge of and detailed inquiry into those decisions.

VI. Address behaviour, don't punish success

Sound tech policy should seek to mold and target behaviours across a sector or drive outcomes on a systemic basis. It should not target specific individuals or companies. An approach that singles out individual organisations does not take into account the diversity and dynamism of the tech sector. More importantly, such an approach is not a sound long term approach addressing future challenges. This does not stop laws from ultimately being enforced in relation to identified individuals or entities, but regulations should not be made out against them specifically in the first place.

VII. Tech (and trust) is global

Sound tech policy should be coherent and consistent, mindful of global standards and able to enhance global interoperability. Local conditions must of course be considered, ensuring that any regulation forms part of a coherent local landscape. However, if competing regulatory frameworks are not also considered, there is a high risk that technology regulation will develop in a piecemeal manner that increases the burden on innovation, business, and consumers alike.

VIII. Build the foundation for shared success

Sound tech policy should provide a consistent and reliable framework for business and investment. We fully appreciate and support governments' legitimate interest in meeting regulatory goals and protecting consumers and the public, and the responsibility that all businesses share to ensure that this is achieved. It is equally important that the legislative process and outcome should be measured, fair, and reliable, in a manner that provides business stakeholders with the confidence to grow and invest in jobs, infrastructure, and improved products and services for their customers.

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit:
https://creativecommons.org/licenses/by/4.0/