Atlassian's Submission in relation to the Discussion Paper: Strengthening Australia's cyber security regulations and incentives

Department of Home Affairs
techpolicy@homeaffairs.gov.au

25 August 2021

We appreciate this opportunity to provide input on the Discussion Paper in relation to Strengthening Australia's cyber security regulations and incentives (the **Discussion Paper**).

At Atlassian, we build enterprise software products to help teams around the world collaborate, including for software development, project management and content management. As a digital-first company, we know the critical role that cyber security plays in ensuring the confidentiality, integrity and availability (and accordingly the privacy and trustworthiness) of our own products and services.

We also understand that this is not just an issue for one company, one sector or one country. Our entire economy is increasingly digitised, highly interconnected (including globally) and strategically targeted by malicious actors, trends that have only accelerated in the past 18 months. Atlassian strongly supports efforts that seek to uplift cyber security capability and encourage better cyber security practices across the economy and across borders, in a way that acknowledges that responsibility for cyber security is shared by all of us.

Atlassian welcomes this consultation process and appreciates the comprehensive and well-considered treatment of the issues and proposals canvassed in the Discussion Paper. In the time since the publication of Australia's Cyber Security Strategy 2020, the urgent and critical need to take action to ensure the security and resilience of our digital economy has been recognised by governments, businesses and societies around the world.

This means that the Discussion Paper and its proposals come at a time when multiple governments and regulators are seeking to address many of the same complex issues, including by considering appropriate cyber security standards and expectations.

Key principles to inform this consultation process

Given this current landscape, we therefore strongly believe that the Australian Government's reforms should be considered and formulated by reference to clear guiding 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.

In line with those Principles, we accordingly propose the following key principles to guide this reform process:

1. **Cyber security compliance is increasingly a matter of *how*, not *why*.** The Discussion Paper acknowledges the important role that governments can play in encouraging and incentivising businesses to invest in cyber security. However, we would caution against any inference that the current level of cyber security

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

investment has arisen out of a lack of understanding of the importance of cyber security or an absence of regulatory or legal consequences for any failure to do so.

In our experience, it is often the case that under-investment arises because companies (especially smaller businesses, including start-ups and scale-ups) may not know how best to effectively implement security risk management in their organisations in a way that aligns with the complex landscape of their own requirements, industry best practices and recommendations and global compliance obligations. In line with Atlassian's third principle [*Treat the ailment, don't kill the patient*], these reforms should be designed to provide a clear and achievable response in this broader context.

2. **This complex and fast-moving area calls for international alignment.** The Discussion Paper acknowledges many of the global efforts underway to clarify cyber security standards and expectations. In accordance with our seventh principle [*Tech (and trust) is global*], this consultation process provides a real opportunity to establish and maintain alignment with these emerging international processes and regimes, including through cross-certification and recognition of international standards.

   We strongly believe that the best outcomes will be achieved through consistent, achievable and interoperable standards. In addition to improving our overall cyber security posture, this consistency will lower global barriers to entry for Australian companies that are, or are seeking to be, export-ready (as well as benefiting Australian consumers who would have access to a wider variety of secure solutions from both local and international companies).

We believe that these key principles, when applied to the proposals and issues canvassed in the Discussion Paper, demonstrate a real need for clear, actionable and internationally-aligned standards, expectations and guidance. Our more specific comments on certain of these areas are set out below.

Applying these key principles to the Discussion Paper's proposals

Governance standards for large businesses (Chapter 4): We generally support the development of voluntary standards as set out in the Discussion Paper. We agree that standards of this nature can send a signal to businesses and the customers that cyber security is taken seriously, and accordingly drive the right behaviours when it comes to security risk management. However, in light of the key principles above, any such standards should:

- either be based upon existing global standards in this area (such as the ISO 27000 series), or be able to be explicitly mapped to relevant global standards; and
- in order to truly "move the needle" and influence smaller businesses that may not be directly covered by the standard, be accompanied by appropriate implementation guidance and education campaigns.

Minimum standards for personal information (Chapter 5): We again appreciate the aims of this Chapter and the intent to achieve uplift through specifying minimum (rather than best practice) standards in this area. However, we are concerned that the option set out in the Discussion Paper for an enforceable code under the Privacy Act may not be the best mechanism to achieve these aims.

In particular, the limitations of the current Privacy Act mean that it will not apply to small businesses who may benefit most from its requirements, and would not be adapted to broader data practices beyond personal information. More broadly, such codes do not appear to be commonly used, and their enforceability in practice is likely to require greater overall investment in the enforcement of the Privacy Act (as we recommended in our earlier submission to the Privacy Act reform process).[2]

[2] See https://www.ag.gov.au/sites/default/files/2021-01/atlassian.PDF.

However, minimum standards could still provide an opportunity to align with current and emerging global standards for data security. For example, as mentioned in our Privacy Act reform submission, many companies operating globally are already subject to the higher standards imposed by the GDPR in this respect, and would welcome consistency and interoperability between jurisdictions. On the basis that minimum standards could and should instead be implemented through an alternative vehicle, such as a purpose-built voluntary standard or code, then the content of those standards will also need to be carefully considered in line with the above key principles.

As a further overarching principle, these minimum standards should provide companies with clear guidance (in light of the many options available) on where to focus their efforts and the reasons why. By way of example, as the Discussion Paper notes, the Australian Signals Directorate's Essential 8 could form the foundation for a minimum standard, and it has a number of features that could assist in this respect (including the tiered maturity model and existing implementation guidance). However, this would and should be complemented by:

- consideration of how these standards can evolve over time, and how they currently and will in future align to equivalent guidance and processes in other countries (including those published by NIST, the UK NCSC, the Cloud Security Alliance and Center for Internet Security); and
- having regard not only to the technical aspects of cyber security (technical risk management), but the equally important human and behavioural aspects (human risk management), including the need for education and training.

Responsible disclosure policies (Chapter 8): We strongly believe that responsible disclosure policies assist businesses in identifying and resolving vulnerabilities, and support measures that will encourage Australian businesses to increase their adoption of these policies. The Discussion Paper already notes that, as global adoption of these programs steadily increases, work is underway by NIST and the UK NCSC to provide guidance to industry on responsible disclosure programs. In line with the above key principles, we consider that the best approach would be to closely monitor and seek to mirror these international developments and guidance, rather than following a (potentially divergent) parallel process.

Atlassian is committed to working with the Government, industry and other stakeholders on these key issues and principles in order to uplift cyber security across our economy, and to ensure the future success of our digital economy.

Yours sincerely,

David Masters
Director of Global Policy & Regulatory Affairs
Atlassian

Anna Jaffe
Senior Counsel, 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.