Policy position:

Privacy and (Cyber) Security

As technology advances, privacy and cyber security issues are becoming dynamic concepts and significantly more complex; this requires foresight, planning and broad acceptance of responsibility to maintain confidence in the digital economy.

Why does this matter?

At the heart of the fourth industrial revolution are digital technologies. The Internet of Things (IoT), advanced robotics, automated vehicles, artificial intelligence, machine learning, nanotechnology, cloud computing, blockchain and data analytics used to underpin automated decision-making means privacy and cyber security is becoming more integral to business and government operations.

As well as keeping pace with emerging digital technologies, privacy and cyber security laws, policies and practices must also address progressively sophisticated cyber-attacks. Policies must evolve from technical, compliance-based matters to address socioeconomic issues and recognise shared responsibilities, with individuals, business and governments each having a role to play.

Addressing the challenges

Australia's current privacy and security assessment and compliance landscape remains fixed in traditional models and approaches which target generally well understood cyber threats and focus on legislative compliance.

For Australia to remain globally competitive in the fourth industrial revolution, we must balance effective governance, protective frameworks and legal and policy environments with support for innovation that doesn't impose unnecessary or costly burdens on business or individuals.

The assumption that responsibility for governance for both cyber security and privacy lies with the public sector must change. Educating individuals, industry and governments to support behaviours that protect their privacy and security online and share responsibility for privacy and security is critical in minimising the impact of cybercrime on the Australian economy.

Building cross jurisdictional mature security information-sharing mechanisms with common standards and protocols will assisting in building public trust in the online ecosystem and increase participation in the digital economy.

AIIA recommends:

Government, industry and research institutes collaborate to develop and implement:

- ✓ Agile and responsive security and privacy policies that deal with new types of cyber security threats from emerging technologies;
- ✓ A consultation framework with cross-disciplinary collaboration, crowd-sourcing issues, priorities and options to disrupt the idea that governance lies with the public sector;
- ✓ Strategies, road maps and measures to support educating the community and building skills and expertise in the privacy and security implications of new technologies;
- ✓ Legislation that strikes a balance between security and privacy with the business cost-implications for compliance and the combined impact on business innovation and export activities;
- ✓ Frameworks, rules, principles, fit-for-purpose-legislation and common standards for data collection and to promote open data flow and data use for better government and business service delivery. The framework needs to be underpinned by an information sharing framework incorporating privacy and security mechanisms to improve transparency and accountability in the collection, storage and use of data. The framework should be funded to to include regular reporting, supportive incentives and penalties.