Australian Information Security Association

The AISA Response to the Australian Law Reform Commission's Discussion Paper No. 80:

"Serious Invasions of Privacy in the Digital Age"

Date 12 May 2014

Australian Information Security Association

Executive Summary

The Australian Information Security Association (AISA) is Australia's primary information security professional representative body. AISA has over 2,000 members across Australia and local branches in all major capital cities. AISA is pleased to provide this submission in response to the Australian Law Reform Commission's Discussion Paper No. 80 on "Serious Invasions of Privacy in the Digital Era."[1]

The Discussion Paper makes recommendations and asks for submissions in relation to a range of topics. For information security professionals, there are three main areas of interest raised in the Discussion Paper:

- The civil right to sue for breach of privacy;
- New uniform surveillance laws; and
- Regulator Take Down notices.

AISA Information Security Research

AISA surveyed our over 2000 members in April - May 2014. AISA's submission to you is based on that survey. AISA developed this submission via a working party made up of AISA members from around the country as a part of our process to provide high quality information in response to Discussion Papers that raise issues relevant to AISA's members.

AISA Survey Results – General Highlights

- AISA supports the introduction of the right to sue for serious invasion of privacy.
- AISA supports the introduction of the right to sue for a serious invasion of privacy caused by negligence.
- AISA supports uniform surveillance laws.
- AISA supports a system for regulatory taken down notices.

On behalf of the Policy Committee

Arno Brok
National Director
Australian Information Security Association

[1] ALRC "Discussion Paper 80 Serious Invasions of Privacy in the Digital Era (March 2014)" < http://www.alrc.gov.au/publications/serious-invasions-privacy-dp-80> ("ALRC Discussion Paper")

Australian Information Security Association

Responses to the Discussion Paper

The questions posed by AISA to its members to inform its response to the ALRC Discussion Paper covered three areas:

1. Serious Invasion of Privacy;
2. Surveillance Laws; and
3. Regulator Take Down Notices

AISA submissions in response to questions posed in the Discussion Paper in each of these areas are presented below. All of the responses are based on AISA's survey of its members.

Right to Sue for Serious Invasion of Privacy

AISA supports the introduction of a right to sue for serious invasion of privacy.

According to the survey results, AISA members see the main benefits of the introduction of a right to sue for serious invasion of privacy are:

- Individuals will have a real right to seek compensation where there is a serious breach of privacy;
- Organisations will put more focus on ensuring that individual's private information is protected properly; and
- Reduction in the amount of private information held by organisations.

AISA supports the right to sue for negligent disclosures – as well as deliberate or reckless disclosure or misuse. Currently serious invasions of privacy from a failure to take reasonable care to protect information systems would be outside the scope of the action. The view of AISA's members was that they should be included.

AISA members also supported the inclusion of a definition of "disclosure." AISA members are concerned about the lack of certainty as to the meaning of disclosure pursuant to the *Privacy Act 1988* (Cth) in the context of both cyber attacks and failing to take reasonable steps to secure information. Given the lack of jurisprudence around the privacy laws in Australia it would be helpful for information security practitioners if terms such as "disclosure" and "unauthorised access" are clearly defined and supported by useful guidance clearly articulating the meaning and intended operation of these terms.

In regard to the protection of intermediaries, members were divided. Approximately 51% of respondents believed that internet intermediaries should have the benefit of a safe harbour protection. 30% believed they should not and 18% were unsure.

Members who believed that there should be an intermediary safe harbour provision, were of the view that that right should be dependent on:

- The intermediary removing, or take reasonable steps to remove, material that invades a person's privacy, when given notice; and
- The intermediary providing a privacy complaints system where the intermediary responds in a reasonable time to consumer complainants.

Members were not as supportive of the following, although each of these options was approved by more than 50% of the people responding to this question:

- The intermediary providing consumer privacy education or awareness functions, such as warnings about the risk of posting private information; and
- The intermediary providing individuals with a mechanism to remove private content they post on online platforms.

Use of Surveillance Devices

The AISA Member survey noted the following summarised version of the proposals put forward in the discussion paper:

- Surveillance device laws and workplace surveillance laws should be made uniform throughout Australia;
- Surveillance device laws should include a technology neutral definition of 'surveillance device';
- Offences in surveillance device laws should include an offence proscribing the surveillance or recording of private conversations or activities without the consent of the participants. This offence should apply regardless of whether the person carrying out the surveillance is a participant to the conversation or activity, and regardless of whether the monitoring or recording takes place on private property; and

- Defences in surveillance device laws should include a defence of responsible journalism, for surveillance in some limited circumstances by journalists investigating matters of public concern and importance, such as corruption.[2]

Members were asked to comment on these proposals. Based on those responses:

- AISA supports a uniform approach to surveillance in Australia;
- AISA also supports more pro-active regulation of work place surveillance.

Members were divided in regard to the need for consent before recording a private exchange. A number of people were in favour of participants having the right to record interaction they were engaged in as well as the recording of activities where there is a reasonable expectation of recording (for example, use of voice mail). However there were also some who believed that consent should be secured before any recording.

One member raised concerns regarding the supervision of the use of surveillance, suggesting it should be carried out by an independent tribunal.

AISA also supports a technology neutral definition of surveillance device. However, one member noted that it should still be possible to use technologies commonly used as part of information security such as automatic email scanning using anti-virus (which could be "surveillance"), data leakage prevention and web/mail usage logging and monitoring.

In terms of regulating the installation and use of surveillance devices by private individuals, 57% of members who responded to the survey did not believe that local councils were the appropriate entity. A number of responses suggested that a Federal regulator would be more appropriate as part of a uniform federal approach to regulating surveillance devices. Possible problems with consistency between private and business use of surveillance where councils and workplace regulators were involved were noted. Another member suggested that, rather than regulating via a Council, there should be a separate complaints process whereby such devices could be considered, perhaps managed by the Privacy Commissioner.

[2] ALRC Discussion Paper at p196

Regulatory Take Down Mechanism

AISA supports a regulatory take down system. Over 85% of respondents were in favour of a regulatory take down system.

Members were less sure of which regulator would be the most appropriate to manage this function. 73% supported the Privacy Commissioner having this role while 60% supported a Magistrate or other Tribunal having authority.[3] Members were not so supportive of the involvement of ACMA, the ACCC or Fair Work Australia in these decisions.

The majority of respondents supported the use of the take down mechanism in cases where there is a serious invasion of privacy, rather than any invasion of privacy.

AISA also supports the role of Australian courts and tribunals in determining what is in the public interest in a way that would ensure the protection of freedom of speech, although the need to ensure the correct balance was noted. One respondent suggested that some notice that a take-down has occurred should be posted to ensure there are no 'secret' takedowns. The same respondent suggested that there should be a clear appeal process available from a take down order, with a requirement that that appeals body promptly process all appeals.

Conclusion

AISA hopes that the above submissions are helpful in terms of the feedback being sought in response to the ALRC Discussion Paper.

We would be happy to discuss our findings further and engage more closely with the ALRC in regard to issues such as surveillance and regulatory take down mechanisms in the future.

AISA would like to thank for you the opportunity to be involved in this process.

[3] Members were able to select more than one answer to this question which is why the total adds to more than 100%.

Australian Information Security Association

Contacts and Further Information

Arno Brok
AISA National Director
Arno.brok@aisa.org.au
Phone: 0404 885 373

Jodie Siganto
AISA Policy Committee Chair
jodie.siganto@aisa.org.au
Phone 0438 603 307

The Australian Information Security Association

The Australian Information Security Association (AISA) is an Australian representative industry body for the information security profession.

Formed in 1999, AISA is focussed on individual membership. AISA aims to be the Information Security Voice of Australia by means of:

- generating and increasing the awareness of information security issues among individuals, the community, educational institutions, business and government;
- increasing knowledge, skills and capacity of those working in, or wanting to know about, the information security field;
- conducting research and development activities which improve information security;
- providing an ongoing forum to share learning, knowledge, skills, experience ideas and innovation in the information security field.

Our broad membership base consists of information security professionals from all industries including education, finance, government, healthcare, manufacturing, mining, oil and gas, transportation, and utilities. Our members range from company directors and managers, lawyers, risk professionals, architects, highly skilled technical security specialists, professors and researchers.