



Submission to

Australian Law Reform Commission

Subject

Serious Invasions of Privacy

Date

12 May 2014

Introduction

The Interactive Games and Entertainment Association (**IGEA**) welcomes the opportunity to respond to the Australian Law Reform Commission's (**ALRC**) discussion paper on serious invasions of privacy in the digital era (**Discussion Paper**).

Set out below is a brief description of IGEA, our general comments on the proposed statutory cause of action and our response to the Discussion Paper proposals and questions that are particularly relevant to the games industry and IGEA.

About IGEA

IGEA is an industry association representing the business and public policy interests of Australian and New Zealand companies in the computer and video game industry. IGEA's members publish, market, develop and/or distribute interactive games and entertainment content and related hardware. The following list represents IGEA's current members:

- Activision Blizzard
- All Interactive Distribution
- Disney Interactive Studios
- Electronic Arts
- Five Star Games
- Fiveight
- Gamewizz Digital Entertainment
- Microsoft
- Mindscape Asia Pacific
- Namco-Bandai Partners
- Nintendo
- Sony Computer Entertainment
- Take 2 Interactive
- Total Interactive
- Ubisoft
- Warner Bros. Interactive Entertainment
- ZeniMax Australia

IGEA General Comments

IGEA recognises the limited scope of the ALRC's inquiry as set out by the Terms of Reference. The ALRC stated in the issues paper for this inquiry that, "it is not useful to ask again ... whether respondents support or oppose a statutory cause of action"¹. Notwithstanding this, IGEA also recognises that the comprehensive reforms to Australia's privacy laws have only recently become effective and it is simply too soon to determine whether the proposed statutory cause of action is actually warranted.

The reforms set out by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* commenced on 12 March 2014 and will certainly act to protect Australians from, and reduce instances of, serious invasions of privacy. Following significant public awareness campaigns by the Office of the Australian Information Commissioner and a wave of increased compliance costs for APP entities to update policies and processes to acknowledge the reforms, there has undoubtedly been a substantial impact on how personal information is collected, retained and disclosed. Accordingly, the recent reforms should be given appropriate time to operate before any further reforms are considered. More particularly, the statutory cause of action proposed by the ALRC in the Discussion Paper should only be considered after recent reforms have been tested and a demonstrated need for the cause of action is evidenced. Until this time, IGEA does

¹ ALRC, "Serious Invasions of Privacy in the Digital Era (IP 43)", paragraph 14.

not consider the proposed statutory cause of action for serious invasions of privacy to be necessary.

ALRC Discussion Paper Questions and IGEA Response

While IGEA does not support the introduction of a statutory cause of action for serious invasions of privacy, the following input has been prepared for the benefit of the ALRC's consideration.

Proposal 5-2 Second element of action: The new tort should be confined to intentional or reckless invasions of privacy. It should not extend to negligent invasions of privacy, and should not attract strict liability.

IGEA supports the proposal that the tort should not extend to negligent invasions of privacy and should not attract strict liability. While an inadvertent disclosure of personal information may attract the attention of the Australian Information Commissioner to determine compliance with the Australian Privacy Principles, such conduct should not fall within the scope of the proposed tort.

Question 10-3 What conditions should internet intermediaries be required to meet in order to rely on this safe harbour scheme?

Australia's legislation must not inhibit the development or provision of innovative products and services in Australia, particularly those products or services that enhance freedom of expression and ideas or information sharing. Accordingly, any conditions that are imposed on the proposed defence for internet intermediaries should not undermine the intended purposes of such a defence. For example, the defence should not be conditional on internet intermediaries moderating user-generated content or assuming any responsibility for determining whether a third party's conduct would amount to a breach of the proposed statutory cause of action. IGEA does not support conditions being imposed that will mandate the implementation of costly or unworkable processes by intermediaries to the detriment of the continued development and provision of innovative products and services in Australia. Such intermediaries will already be subject to the requirements of the Australian Privacy Principles and any further requirements should be avoided.

Proposal 15-2 A new Australian Privacy Principle should be inserted into the *Privacy Act 1988* (Cth) that would:

- (a) require an APP entity to provide a simple mechanism for an individual to request destruction or de-identification of personal information that was provided to the entity by the individual; and
- (b) require an APP entity to take reasonable steps in a reasonable time, to comply with such a request, subject to suitable exceptions, or provide the individual with reasons for its non-compliance.

IGEA does not support proposal 15-2.

The Australian Privacy Principles already require APP entities to destroy or de-identify personal information that is no longer required for a specific purpose under the APPs. While this principle may not be as strong as the one proposed by the ALRC, the existing principles should be thoroughly examined and tested before any new principles are introduced.

If the proposed principle is ultimately introduced, the wording of the principle should be carefully framed to ensure that the choice of 'de-identification' or 'destruction' is one for the APP entity rather than the individual. The use of anonymised and aggregated data is a critical aspect of business in a digital era and therefore we must ensure that Australian law does not prevent the use of such data. Balanced with appropriate consents to collect personal information as required by the Australian Privacy Principles, APP entities should be entitled to use de-identified data without restriction.

Question 15-1 Should the new APP proposed in Proposal 15-2 also require an APP entity to take steps with regard to third parties with which it has shared the personal information? If so, what steps should be taken?

APP entities should not be required to take steps with regard to third parties with which it has shared personal information. The Australian Privacy Principles already provide adequate protections to address the issue of third party disclosure of personal information. The following principles are particularly relevant:

- APP 1 – the requirement for an APP entity to manage personal information in an open and transparent manner, including by having a privacy policy that stipulates how personal information will be disclosed (with particular emphasis on whether personal information will be disclosed to an overseas entity).
- APPs 4.3 and 11.2 – requirement for the destruction or de-identification of personal information that is no longer required by the APP entity.
- APP 6.1(a) – the requirement for consent before the disclosure of personal information to a third party for secondary purposes.
- APP 8 – requirements concerning cross-border disclosure of personal information.

The Australian Privacy Principles already ensure that the third party collection and handling of personal information is conducted in a transparent, appropriate and legally compliant manner.

In some instances, personal information may be distributed widely with the appropriate consent of the individual. In these circumstances, the costs of tracking or taking steps to identify such widely distributed information would be costly and most likely ineffective. Accordingly, any attempt to require steps to be taken with regard to third parties with which an APP entity has shared personal information will introduce an unnecessary, costly and ineffective burden on APP entities.