Submission to

Australian Law Reform Commission

Subject

Serious Invasions of Privacy

Date

November 15, 2013

Introduction

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

Set out below is a brief description of IGEA followed by a detailed response to the Issues Paper questions that are particularly relevant to the games industry and the 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
- All Interactive Entertainment
- 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

ALRC Issues Paper Questions and IGEA Response

Question 14 What, if any, other defences should there be to a statutory cause of action for serious invasion of privacy?

The following matters should be addressed by the ALRC in crafting any offence and the relevant exemptions or defences.

Internet Intermediaries

In paragraph 74 of the Issues Paper, the ALRC invited comments on the defences that may be appropriate for Internet intermediaries or Internet sites hosting material posted by third parties. We need to ensure that Australia's legislation does 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. The ALRC may consider a defence that is similar to section 230 of the United States of America's *Communications Decency Act,* whereby providers and users of interactive computer services that publish information provided by others are immune from liability.

Discretion of the disclosing party

The ALRC should consider introducing a defence for circumstances where disclosure is required or compelled by law to protect the health and safety of consumers including children, and to prevent other criminal activity, *with reasonable discretion resting with the disclosing party*. Discretion is essential to prevent the disclosing party from failing to protect consumers for fear of legal repercussions.

Protection of the disclosing party

A defense should also be available to protect the legitimate interests of the disclosing party including to prevent fraud, intellectual property theft, cybercrimes or to address dispute allegations and the like. Reasonable discretion in such matters should rest with the disclosing party to ensure that criminals or other wrongdoers do not have an unfair advantage.

Consent

In paragraph 64 of the Issues Paper, the ALRC states that 'consent' should be relevant to considering whether the threshold for serious invasion of privacy has been established, rather than as a defence. Whether in the establishment of the offence or as a defence, there should be no liability if appropriate consents have been received.

Anonymised data

The use of anonymised and aggregated data is a critical aspect of business in a digital era. For example, game developers or publishers may collect information about a user's gameplay time, frequency, and spending habits to further improve and enhance consumer experiences. We must ensure that Australian law does not prevent the use of such data. It is therefore important for the ALRC to consider whether the use of such data could amount to an offence under proposed legislation and whether a defence or exemption should be introduced accordingly.

Cybercrime

Cybercrime is an unavoidable risk in the digital era, with the victims of such sophisticated crimes including both the individuals affected and the businesses that are implicated. No security mechanism is 100% secure, however the law should clearly recognise and protect those businesses that have implemented and used reasonable security measures. Accordingly, the ALRC should consider a defence or exemption for those businesses that have implemented and used reasonable security measures. Such protection will encourage transparency about the loss of consumer data, even if such disclosure is not a legal requirement.

Data processing

In paragraph 73 of the Issues Paper, the ALRC has included 'the circumstances justified the conduct as a matter of necessity' as a possible defence to a statutory cause of action for serious invasion of privacy. Disclosure is often necessary to fulfill contractual obligations or throughout the provision of certain products and services. This is particularly relevant for third-party subscription management services and payment gateways. Accordingly, it would be important to have a relevant defence or exemption for such circumstances.

Question 16 Should the Act provide for any or all of the following for a serious invasion of privacy:

- a maximum award of damages;
- a maximum award of damages for non-economic loss;
- exemplary damages;
- assessment of damages based on a calculation of a notional licence fee;
- an account of profits?

Data is essential to the health of the economy and the ability for industry to innovate and provide meaningful, useful and lucrative products and services to consumers. Responsible and innovative data processing should be encouraged to stimulate the economy with new technologies that inure to the benefit of consumers.

Monetary remedies that are disproportionate to the potential for consumer harm can only quash that innovation and prevent the efficient development of technology. Accordingly, monetary remedies should be directly tied to proven economic loss by the consumer.

Exemplary damages should be provided for only when the violation is intentional and causes direct economic loss. Statutory penalties and notational damages will serve only to stifle innovation to the detriment of consumers.

Question 24 What provision, if any, should be made for voluntary or mandatory alternative dispute resolution of complaints about serious invasion of privacy?

Arbitration is an effective means of resolving disputes and reasonable arbitration clauses in consumer contracts should be enforceable.

Further Comments

Consent

Paragraphs 166, 167 and 168 of the Issues Paper explore the role of 'consent' in relation to an offence for serious invasions of privacy. It is worth emphasising that reasonable consumer consent should be adequate for the collection, use, sharing and disclosure of personal information. While the existence of consent will be determined with reference to the Australian Privacy Principles, the level and form of consent will usually be guided by what a reasonable consumer would expect in the relevant circumstances. Industry-standard practices and guidelines from the Office of the Australian Information Commissioner would also provide businesses with useful guidance on this matter.

Right to be forgotten

Paragraphs 169, 170 and 171 explore the prospect of providing individuals with an enforceable right to the removal of certain information with reference to the recently proposed 'right to be forgotten and to erasure' in Europe. Complete data deletion is nigh-impossible in light of back-up systems, report generation and the otherwise complex nature of database infrastructure, therefore any right to be forgotten should be limited to active databases that fuel continued

disclosure of personal information on social network and similar services within the control of the disclosing party.

Online tracking

Paragraph 173 of the Issues Paper discusses the use of online tracking systems and refers to the overseas interest in the use of 'Do Not Track' requests. Online tracking systems allow businesses to not only assess the viability of their services, but also provide more customised and enhanced experiences to consumers. Do Not Track requests, if mandated at all, should be limited to circumstances where there is a significant privacy impact of the tracking and should not extend to first party tracking. Any mandatory do not track requests should be limited to third party behavioral tracking so as to not stifle innovation.

Geolocation Data

Paragraph 174 of the Issues Paper explores the use of Global Positioning System receivers to determine and record the location of users. The use of geolocation data enables industry to provide useful products and services to consumers. The definition of 'geolocation data' should be carefully considered, differentiating between precise coordinate-level geolocation and approximate geolocation. Appropriate consent adequately ensures that collection of such information comports with the reasonable expectation of consumers.