Commercial and Administrative Law Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

The Digital Industry Group Incorporated ("DIGI"), welcomes the opportunity to make this submission to the Attorney General's Department on the proposed Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (the "Bill").

ABOUT DIGI

DIGI is a not for profit industry association whose members include Google, Twitter, Facebook, Yahoo! and Microsoft and its' objectives are to:

1. Protect the open nature of the Internet for Australians as an environment for innovation and freedom of access to information, communications and commerce;
2. Promote the benefits of the Internet to government, community and other key stakeholders; and
3. Advocate for a balanced and common sense approach to policy development for the online world.

Collectively, the organisations that make up DIGI provide various digital services accessible by Australians, ranging from social media and networking sites, to search engines and other digital communication platforms.

COMMITMENT TO PRIVACY + CURRENT VOLUNTARY SCHEME

All of DIGI's members are strongly committed to the privacy and security of our customer's data. Our success is ultimately tied to ensuring that people have positive experiences on our platforms and securing and maintaining users' trust is fundamental to this. It is imperative for customer retention, trust and growth that we continue to maintain these commitments to privacy and in that vein, we all continue to voluntarily notify users of incidents that put them at a real risk of serious harm.

Per DIGI's submission, (then, "the AIMIA Digital Policy Group"), of 5th December 2012, we continue to maintain that the current voluntary data breach notification arrangements are being put to good use by the Australian business community. This position is supported by research from the Office of the Australian Information Commissioner's (OAIC) annual report showing a 64% increase in voluntary data breach notifications from 2013-2014 to 2014-2015.

There has also been a significant increase in privacy complaints generally over previous years which, as speculated in the report, may reflect a growing awareness among the community of privacy and awareness of the formal right to bring a complaint provided by the *Privacy Act* 1988 (Cth). Businesses are increasingly reporting data breaches voluntarily. Consumers appear to respond well to receiving privacy notices as the Deloitte Australian Privacy Index 2015 reported that 34% of consumers who had received a privacy breach notice trusted the company more as a result of their transparency.

For all DIGI members, the privacy, safety and security of the people who engage with our services is our top priority. For the digital industry to thrive, it is in our best interests to ensure that our users have full confidence and trust in our systems and frameworks. We are highly supportive of the existing voluntary breach notification arrangements and working collaboratively with the OAIC, as appropriate.

In considering the need for and the structure of any mandatory data breach notification scheme, we encourage the Government to consider the range of varying and, at times, inconsistent notification schemes around the world. Without a global consensus on how businesses should deal with data breaches, variations on triggers, notification time frames and what constitutes "serious harm," can prove extremely challenging for organisations to develop notification schemes that correspond to the requirements of all of these different regimes and requirements.

SPECIFIC COMMENTS ON PROPOSED LEGISLATION

Whilst we believe that the current voluntary notification scheme is working well, if the Government chooses to adopt a mandatory data breach notification scheme, we encourage it to ensure some aspects of the current proposal are retained but that others are removed.

Given the strong commitment of industry to notify in the event of data breach, we encourage any legislative implementation to be sufficiently flexible to allow for the different nature of services, the different types of breaches that may occur and to also avoid placing industry in a position where it is impossible to provide notifications that are consistent with all legislative schemes that exist in different parts of the world.

If the Government chooses to legislate, we encourage the retention of a definition of serious harm being set at a high standard. We note that it is proposed to mean "physical, psychological, emotional, economic and financial harm, as well as harm to reputation" and the requirement that the risk of harm is "real" and not "remote" sets a strong threshold. Similarly, the notification bar needs to be set at an appropriately high level – as is presently proposed -- to ensure that notifications are mandated in the most serious of circumstances. We note that the existing OAIC voluntary data breach notification guidelines encourage notification of incidents that result in a "real risk of serious harm" and we recommend that any law implemented as a result of this Bill adopt similar language. A high threshold minimises the administrative burden on the part of the OAIC, and notification fatigue on the part of the individuals, which has the potential to undermine the efficacy of any scheme.

Any law that is passed should also acknowledge that a reasonable amount of time is needed for organisations to investigate and assess whether an incident meets the criteria for notification, and also to fully understand what has happened to properly redress and reduce further potential exploitation of any system or process that lead to the incident. We note that the Bill envisages 30 days and we believe that this will ensure that the administrative burden can be shared between industry and the OAIC as well as enable a full and thorough investigation, in most instances, into the specific circumstances of any incident before needing to notify.

DIGI members also welcome the flexibility of the notification process outlined within the Bill including the acknowledgment that, "There may be circumstances in which it is impracticable to provide a notification to each affected individual".

The Bill states that "a civil penalty would only be required where there has been a serious or repeated non-compliance with mandatory notification requirements". We would prefer that no penalty or sanction be applied in one-off instances where the notification requirements are not met and where the organisation is able to provide strong reasons for not meeting a requirement. At a minimum, we respectfully request that the Bill include more detail regarding what would qualify as serious non-compliance with mandatory notification requirements.

We believe that the system should be designed to provide for reasonable sanctions against bad actors, including those organisations that repeatedly fail to fulfil their obligation to notify. This clause regarding civil penalties would need to be clarified, in order to clearly identify a threshold for non-compliance and to avoid onerous penalties for well-intentioned and responsible actors.

Finally, in comparing the Bill with other international examples we note that the requirement to make recommendations for steps that affected users can take to minimise harm is unique. As mentioned above, the circumstances of individual breaches can differ wildly depending on the nature of the vulnerability, the number of affected users, the role of any third party organisations involved in processing data and the complexity of the remedy.

Once an individual is provided with clear guidance on the nature of the breach and the information impacted, we feel that they are best placed to undertake an assessment of their risks and the actions that should be undertaken to mitigate that risk. Organisations may not have the full picture of the extent of an individual user's risk and the impact of any breach. Requiring organisations to provide guidance to each user on steps that they should take carries significant risk that such guidance will not be fully informed by the broader circumstances of a user and that further harm may arise as a result of this uninformed advice.

IMPORTANCE OF EDUCATION & AWARENESS

DIGI members believe that the best additional remedy to any data breach occurring, in addition to industry's own voluntary disclosure practices, is to promote and educate all Australians about the small steps they can all take with respect to their accounts, device and data to ensure that they are maintaining best security practices.

Even for those instances that may not arise to the level of requiring a broad notification, any time that an individual's information is compromised, is one instance too many.

All DIGI companies work to develop and deploy tools to protect user data and seek to educate our users and customers on how to promote good privacy and security practices. In particular, we all make available advanced security features for accounts and take steps to encrypt data to prevent unauthorized access.

We also regularly partner with the Australian Government on information awareness initiatives such as Privacy Awareness Week, Stay Smart Online Week and Consumer Fraud Awareness Week.

We thank the Attorney General's Department for considering our comments and welcome the opportunity to provide any additional information in relation to this submission at your request.

Contact:
admin@digi.org.au