PUBLIC CONSULTATION ON DOXXING AND PRIVACY REFORMS

SUBMISSION

April 2024

AISA

AUSTRALIAN INFORMATION SECURITY ASSOCIATION

TABLE OF CONTENTS

In a study aimed at assessing gender-based online violence, the prevalence rate for threats related to doxxing was found to be

55%

Proposed reforms

1. **A new statutory tort for serious invasions of privacy would allow individuals to seek redress through the courts if they have fallen victim to doxxing.**

Doxxing is a serious issue that has major ramifications for Individuals and even organisations affected by Doxxing campaigns. In a study aimed at assessing gender-based online violence, the prevalence rate for threats related to doxxing was found to be 55%. While it begins in the online realm, the damage extends into the personal life of the individual affected. AISA believes that victimisation from cyberbullying constitutes a significant harm issue, and there should be an imposition of appropriate privacy rights protections, supported by a Statutory Tort.

It is agreed that the current legal framework for resolution of Doxxing incidents is insufficient and the step to add a new Statutory Tort for serious invasion of privacy is progressive and timely with the increased adoption of technology. Enforcing civil penalties to deter doxxing and permitting individuals to pursue compensation is an effective strategy to discourage misconduct by instilling the fear of potential consequences for such actions. However, it is essential to carefully craft the Statutory Tort to ensure its application is solely for the protection of doxxing victims and not as a tool for extortion. Therefore, it is crucial to precisely delineate the damages caused by doxxing and establish clear criteria for validating claims related to the harm inflicted or claims of ongoing harm.

It is also crucial to consider the potential use of AI in gathering personal characteristics for profiling purposes, which could lead to discrimination or be utilised to train other large language models that might discriminate. Similarly, it is vital to ensure that organisations employing these technologies safeguard the data of personal characteristics against loss and theft, which could result in harm through doxxing.

2. **Give individuals greater control and transparency over their personal information, including the introduction of new or strengthened individual rights to access, object, erase, correct and de-index their personal information.**

AISA holds the position that the first step towards empowering individuals to manage their personal information and understand its usage is raising awareness. The current challenge is the general lack of knowledge about the risks and potential harm that can arise from seemingly innocuous acts of sharing information with companies or on social media platforms. The Optus data breach in 2022 highlighted this issue, as many customers were taken aback to learn that Optus had retained copies of their passports. At the time of service registration, the request for passport information may have seemed routine, however had customers inquired about the necessity of such information, its retention period and confirmation of its eventual deletion, it could have led to one of two outcomes: Optus revising its data handling procedures or customers choosing to patronise other service providers with better data management practices.

It is recognised that while esafety has launched several initiatives to enhance awareness, the real challenge lies in making a significant impact and encouraging broader participation from individuals. AISA believes that an industry association, through peak bodies such as AISA, can play a crucial role in increasing the engagement with awareness campaigns conducted by esafety.

The Safety by Design initiative from esafety, aimed at helping organisations in improving technology controls, assurance and policies, was a well-conceived strategy. However, most social platforms are not built with Safety by Design's fundamental principles in mind; instead, they are engineered to promote and exploit the oversharing of personal information. Altering the core code of these platforms to incorporate such protections is not only technically challenging but also conflicts with the commercial interests of these companies. Likewise, large language models are often 'black boxes', meaning the training data and operations that inform them are not transparent, which makes embedding safety or privacy by design principles exceedingly difficult.

In such circumstances, raising user awareness becomes the bedrock for the community to safeguard against the dangers of sharing personal information and the threat of incidents like doxxing. A fundamental shift in consumer behaviour could

A report indicates that by the age of 13, a child may have up to 1300 photos and videos shared on social media. This personal content then remains online indefinitely, often shared without the child's consent

compel the market to prioritise the protection of rights and personal data.

Parents often share their children's information on social media platforms without restraint, including names, birth dates, addresses, and sometimes even sensitive details such as medical conditions. A report indicates that by the age of 13, a child may have up to 1300 photos and videos shared on social media. This personal content then remains online indefinitely, often shared without the child's consent.

It's also worth considering for the government that although social media companies prohibit children under the age of 13 from signing up for their platforms, this age limit could be raised to at least 16 years. Many organisations are obligated to protect their staff from internet-related harm and are required to conduct annual awareness training. Similarly, there should be an obligation for these platforms to educate their users about the dangers of threats like doxxing and to provide guidance on secure usage of their services.

Enhancing awareness and providing a framework for affected individuals is crucial, as the more informed people are, the more effective prevention strategies will be. AISA envisions an opportunity to create a seamless and user-friendly portal or an app that guides affected individuals through the process of confirming a doxxing incident, and also outlines steps to access support for remediation, and - if necessary - assists in utilising the Statutory Tort for redress.

We believe it's essential to tackle the issue at its source. A 13-year-old may not understand the dangers of sharing personal information on social media.

A UK study warns that 'Sharenting' could account for two-thirds of identity theft cases by 2030.

3. **Progressing other privacy reform proposals contained in the Privacy Act Review that bring the Privacy Act into the digital age, uplift protections and raise awareness of obligations for responsible personal information handling.**

In relation to the other proposed changes to the Privacy Act, overall AISA is supportive of the changes to bring the Privacy Act into the Digital Age. Whilst it is accepted that these changes are part of a broader package of planned legislation reform, there is still much work to do to give individuals greater control and certainty over how their data is used, shared and managed by organisations.

One of the common themes of feedback AISA received is that there is still work to be done to harmonise legislative obligations in relating to holding data, with data retention and erasure a key topic. Understanding that this is difficult to do and needs to be handled over time, organisations and members of the public are still not clear on how the different forms of legislation impact data usage and retention.

The most impactful change we see again is the raising of awareness of obligations for the safe handling of personal information. We believe that done well, this would have the ability to raise the profile of not only the obligations of organisations that handle personal information, but also the strategies to manage data correctly. There is an opportunity to treat information retention and management as a key security control and there may be scope in the future to add Data Controls to the Essential 8 in a simple and streamlined manner that all organisations can consume.

*Enhancing awareness and providing a framework for affected individuals is crucial, as the more informed people are, the more **effective prevention strategies will be.***

About the Authors

Akash Mittal
Chair, AISA Board of Directors
akash.mittal@aisa.org.au

Michael Burchell
AISA Board Director
michael.burchell@aisa.org.au