The Examiner, 16 November 2023; pg 7.

Your personal data may be under threat

Isabel Bird

SENSITIVE and personal data such as names and addresses held by Tasmanian businesses, sporting clubs and community organisations may be at risk of public exposure.

And if data is stolen, and your privacy breached, you may never even know that it has occurred.

Under current Tasmanian privacy law there is no mandatory requirement for non-government organisations to protect the personal information they collect about children and adults.

This includes voluntarily supplied names, addresses and phone numbers.

It also extends to sensitive information such as health data, political opinions and memberships, race or ethnic origin, sexual preferences, criminal records and trade union memberships.

This gap in legal protection exists in a technological world where identity theft and fraud is increasing, and where a personal data leak may result in discrimination, damage to reputation, financial loss and emotional harm.

The Tasmanian Law Reform Institute (TLRI) is reviewing the gaps in privacy regulation, looking to offer suggestions for improved legal protections in a contemporary era.

TLRI director Professor Jeremy Prichard has said some privacy protections are 20 years old.

"So we need to examine how well they apply to new surveillance technologies, facial recognition systems, biometric data and so on."

These privacy law gaps were noticed in 2019 when Independent MHA Meg Webb called for the TLRI to conduct a privacy law review.

The TRLI received funding in 2020, and released its Privacy Review Issues Paper this year after 16,000 education documents were hacked onto the dark web.

The TLRI, in its privacy review issues paper, said there are multiple gaps in the legislation's "scope, operation, and enforcement that can jeopardise privacy".

It said individual privacy is under threat in some circumstances. It also said that anyone impacted by a privacy breach has very few options for complaint or redress.

"There are no penalties imposed for breaching obligations, there is no mandatory data breach notification that compels information handlers to notify an individual where a breach of their privacy has occurred," it said.

"There is no ability for those handling complaints to order compensation, and there is no private right of action that allows individual to go to court to seek damages for financial or non financial harm suffered as a result of the breach."

The state's main piece of privacy legislation is the Personal Information and Protection Act (2004), which only applies to the government and its contractors.

When dealing in personal data they must apply 10 protection principles. These state that only necessary data can be collected, and it can only be used and disclosed for the purpose that it was collected for, a reasonable purpose, or with consent.