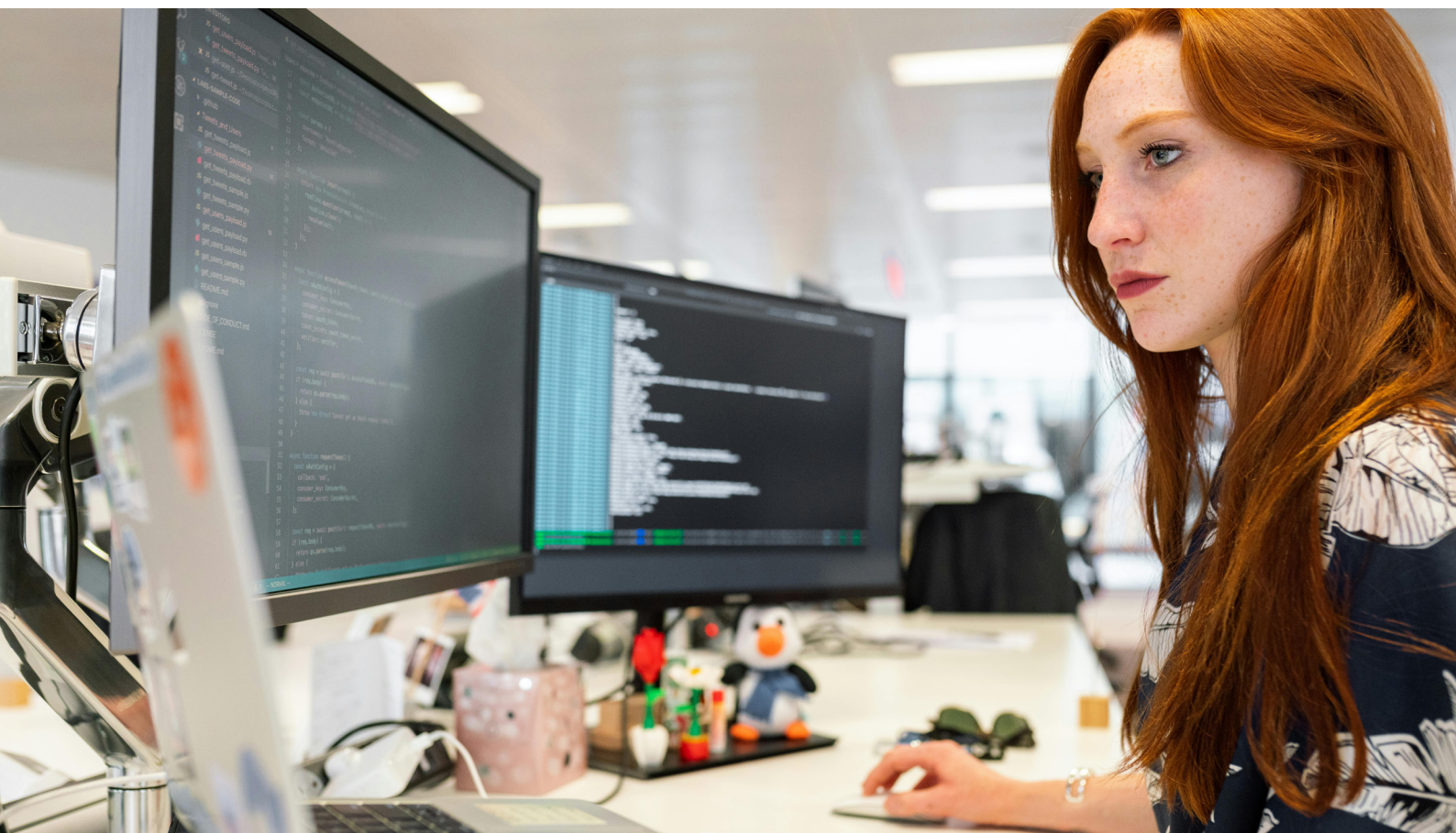




Human Rights Act Factsheet:

Digital Rights

What are digital rights?

Human rights are essential for everyone, in every place and space, to enjoy equality, freedom, dignity and justice. 'Digital rights' are the human rights that are most relevant to our online lives and the way digital technology can be used.

Online spaces and digital technologies are now a part of everyday life. We rely on them for everything from work, study, accessing government services, engaging in public debate and seeking healthcare, to entertainment and connecting with friends and family.

While there is not an agreed list of 'digital rights' the term is used to cover human rights which have a particular connection to digital technology, including in how they are expressed or interpreted. Protecting digital rights is essential for everybody to have the capacity, capability and freedom to use the technology they need and participate in online spaces, while still being protected from harm.

Some of the human rights that fall under the umbrella of digital rights include:

- the right to privacy, which protects our data and personal information online.
- freedom of expression and association, which protects the right to share our thoughts online and to connect and organise with other people online without fear of censorship or punishment.
- the right to equality, which protects us from experiencing discrimination online and discriminatory bias, for example by AI algorithms. It also protects our right to have equal access to the internet.
- the right to participate in public life, which allows us to access information online and engage in public debates and discussions in online spaces.
- freedom of thought, which protects our right to keep our thoughts private, including protection from punishment for what we think and protection from having our thoughts changed against our will.
- cultural rights and linguistic rights in digital spaces, which protects our right to practice our culture and use the language of our choice online.

Digital rights must be carefully balanced against each other to ensure that the protection of one right does not allow the breach of another right. An exception to this is the right to freedom of thought, which is absolute and should not be compromised.

Many of the rights that fall under the umbrella of digital rights come from the International Covenant on Civil and Political Rights.

What is the problem in Australia?

While Australia has signed up to a number of international human rights laws, including the *International Covenant on Civil and Political Rights*, the rights included in these laws aren't automatically protected in Australian law.

To ensure these rights are protected, they must also be included in national legislation that applies to all of us, such as a national Human Rights Act. While some states in Australia, such as Victoria, Queensland and the ACT have created human rights acts which protect some digital rights, these laws only apply within the borders of those areas and only to matters of state/territory responsibility.

Other national laws that protect some of our rights in online spaces, such as the Privacy Act, were not designed with the protection of digital rights in mind. Newer technologies, like generative AI and neurotechnology, are so fast moving that attempts to use existing laws to protect digital rights cannot keep up.

Neurotechnology

The term neurotechnology refers to devices or processes that can monitor or influence brain activity by connecting to a person's brain or peripheral nervous system (the system that connects the various parts of the body to the central nervous system in the brain and spine). Neurotechnology devices can be either worn or inserted into the brain peripheral nervous system. An example of neurotechnology is a Cochlear Implant, which helps Deaf people to hear.

Some new neurotech devices use AI to process brain data in faster and more advanced ways. One example has seen a device collect data from a person's brain and then use that information to reproduce the image the person is seeing in real time; another piece of neurotech has shown it may be possible to decode a person's brain data to reveal the "inner speech" they are imagining. This technology is still in its early stages, but the more this technology develops, the more it will be possible to "read thoughts" using neurotechnology.

Commercial companies are starting to trial and introduce wearable neurotechnology devices with a range of purposes, and it's possible that consumer neurotech will soon be commonplace.

Neurotechnology has the potential to deliver major benefits, particularly in the treatment of neurological and psychiatric conditions, such as restoring the power of speech after a person experiences a stroke. However, without proper protections for digital rights, it also creates new threats to privacy, autonomy and freedom of thought. There are other associated concerns, including how to support patients and people with disabilities to use neurotechnology devices in circumstances where they are no longer supported by the original vendor. Australia does not have the necessary laws in place to protect against these risks.

Strong human rights are needed to protect against the risks connected with these new technologies, for example, where a person loses access to their neural data that's been captured through a neurotech device, or to ensure that people are protected from the risk of a neurotech device being able to alter or manipulate their thoughts against their wishes.



AI and social media

AI and social media are another example of technology with ever growing use that has exposed people to online harm. Social media platforms and other companies often collect huge amounts of personal information from the online activity of their users and sell it for profit. Additionally, the processes that social media platforms exploit to obtain consent to collect and sell data are rarely clear, meaning that many social media users are unaware of how their personal information and data are being used.

New risks are emerging as AI becomes more integrated with social media. The data collected by social media companies before many AI products were possible is being repurposed without consent to train AI models.

The AI algorithms used by social media platforms are designed to push content to users that will attract the most attention, often amplifying content that is likely to elicit a strong emotional response such as discriminatory, false and/or harmful content to people and communities with the least power in society. People can also easily create and share realistic AI generated content of real people, known as deepfakes, which can deceive social media users or be used to perpetrate abuse.

Without a person's knowledge or consent, social media platforms and AI systems can infer deeply sensitive information about individuals, including their political opinions, sexual orientation, or even if they are pregnant. There are risks that the personal information and data that someone provides to an AI bot, like ChatGPT, will not be properly protected by the companies that own and operate AI tools.

How could an Federal Human Rights Act help?

A federal Human Rights Act would recognise the human rights of everyone in Australia. A Human Rights Act should include the broad range of human rights that are required to protect digital rights. It will require governments to consider the way that technology will impact people's human rights when they are creating new laws and policies.

A Human Rights Act would also mean that if someone does experience a breach online of their human rights, they would be more likely to have a pathway available to them to make a complaint and have their rights upheld. Existing laws that protect human rights in Australia, such as anti-discrimination laws or the Privacy Act have limited effectiveness in protecting digital rights.

The broad scope of rights provided under a national Human Rights Act are more likely to provide protection in the face of new technological developments.

Below are examples of how human rights in the digital space have been protected in countries that have enshrined broad rights, either in their Constitution or through a national Human Rights Act. Australia's current laws are insufficient in both situations.



Example 1

Chile: Enshrining neuro-rights in the Constitution



In 2021, Chile amended its Constitution to guarantee citizens protections relating to personal data and the right to mental privacy and the integrity of brain data ('neuro-rights'). In 2022 a Chilean man, Guido purchased a headset that could measure and record brainwaves. Guido learned the company who sold him the headset had stored (and possibly used) his sensitive brain data without his clear and informed consent. The company had put his data behind a paywall and Guido was unable to access it unless he paid for the upgraded subscription to the company's platform.

Guido took the company to court claiming they had violated his constitutionally guaranteed rights. The Supreme Court of Chile found that the company's collection and storage of Guido's data was a violation of his right to psychological integrity and privacy as brain data is extremely sensitive information and collection is only allowed after express and informed consent is provided from the person from which it is being collected. The company also failed to have safeguards which adequately protected user's brain data. The Court ordered the company to delete all of Guido's data, update its privacy policy and had national authorities scrutinise the technology closer before further commercialisation.

Example 2

Canada: Protecting your IP address



In Canada, police obtained a person's IP address from a third-party payment provider, then used it to get the person's identity from their internet company – all without a warrant. An IP address is series of numbers that act like a digital street address. It shows where you are online, what device you are using and allows authorities (or companies) to trace your internet activities. In this case, once the police had the person's identity, they obtained and executed search warrants which then lead to a conviction.

The Canadian Charter of Rights and Freedoms protects against 'unreasonable search or seizure.' This covers personal information and online activity where people have a reasonable expectation of privacy. The Supreme Court of Canada found that even on its own, an IP address can reveal information about an internet user's activity, including sensitive information like the websites a user visits. For this reason, because an IP address can act like a key to other personal information – which can lead authorities to ultimately reveal an internet user's identity – the Court said people have a reasonable expectation of privacy in their IP addresses.

This means the police needed to have a warrant to get the IP address from the start, and because they did not, the Court set aside the conviction.

In Australia, IP addresses are usually only protected as personal information if they are linked to identifying data. This means that, even though IP addresses have the potential to reveal sensitive information, they don't automatically attract privacy protections unless tied to an individual.

Learn more about an Australian Human Rights Act at humanrightsact.org.au

Human
Rights
Law
Centre



**DIGITAL
RIGHTS
WATCH**