The Institute of Internal Auditors Australia

Factsheet: Privacy

Privacy in Real Life

September 2022
Investigations are ongoing after a data breach at Australia's second largest telco Optus enabled cybercriminals to access the personal data of millions of current and former customers.

The group behind the attack reportedly released the personal information of 10,000 customers on a data breach forum and threatened to continue releasing data unless Optus paid a ransom.

Later that day, an account claiming to be from a hacker posted on the forum saying they had dropped the ransom demand and had deleted the 10 million customer records taken from Optus.

The Australian Federal Police is investigating the incident, with questions raised over cybersecurity, the dark web, and what people can do to protect themselves.
Source – AAP

What is Privacy?

The organisation Privacy International describes privacy as:

> *A fundamental right essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built.*

Privacy enables creation of boundaries to protect people from unwanted interference in their lives and to limit who has access to our bodies, places and things, as well as our communications and information.

Privacy is an essential way to protect people and society against use of power by reducing what can be known about us and done to us, while protecting us from others who may wish to exert control.

The Office of the Australian Information Commissioner defines privacy as three things:

- To be free from interference and intrusion.
- To associate freely with whom you want.
- To be able to control who can see or use information about you.

Why does Privacy Matter?

In modern society, the debate around privacy is about modern freedoms. Technology is intertwined with the right to privacy. The paradigm is that there are now greater privacy protections than ever before, but surveillance capabilities are now without precedent.

It is possible for companies and governments to monitor all our conversations, every commercial transaction we undertake, and everywhere we go.

A big challenge is that privacy can be compromised without us knowing about it. With most human rights, people will be aware of being detained, censored or restrained and who is responsible. With surveillance via avenues such as CCTV and data, people are none the wiser.

Is Privacy a Right?

Privacy is a fundamental human right articulated in human rights instruments including:

- 'United Nations Declaration of Human Rights (UDHR) 1948' Article 12: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".*
- 'International Covenant on Civil and Political Rights (ICCPR) 1966' Article 17: *"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation. 2. Everyone has the right to the protection of the law against such interference or attacks".*

The right to privacy is also included in many other laws, conventions and charters.

What are Privacy Principles?

The Australian Privacy Principles are the cornerstone of the privacy protection framework and are contained in the Australian Government 'Privacy Act 1988'. They apply to any organisation or agency the Privacy Act covers being (a) government agency (b) organisation. An organisation includes an Australian individual, body corporate, partnership, unincorporated association or a trust. Australian small

business including a sole trader with an annual turnover of $3 million or less does not qualify.

However, a small business will qualify if they are:

- A private sector health care provider for example:
  - A traditional health care provider – hospital, medical practitioner or pharmacy.
  - A complementary therapist such as a naturopath or a chiropractor.
  - A gymnasium or weight loss clinic.
  - A childcare centre, a private school or a tertiary educational institution.
- A business that sells or purchases personal information.
- A credit reporting body.
- A contracted service provider for an Australian Government contract.
- An employee association registered or recognised under the 'Fair Work (Registered Organisations) Act 2009'.
- A business that has opted-in to the 'Privacy Act 1988'.
- A business that is related to a business covered by privacy law.
- A business prescribed by the 'Privacy Regulation 2013'.

There are 13 Australian Privacy Principles governing standards, rights and obligations around:

- Collection, use and disclosure of personal information.
- An organisation or agency's governance and accountability.
- Integrity and correction of personal information.
- Rights of individuals to access their personal information.

The Privacy Act is principles-based law. This gives an organisation or agency flexibility to tailor their personal information handling practices to their business model and the different needs of individuals. They are also technology neutral, which allows them to adapt to changing technologies.

A breach of an Australian Privacy Principle is an 'interference with the privacy of an individual' and can lead to regulatory action and penalties.

The Privacy Act does not specifically cover surveillance but there are situations where it may apply.

What are the 13 Australian Privacy Principles?

Privacy Principle 1 – Open and transparent management of personal information

Privacy Principle 2 – Anonymity and pseudonymity (use of a pseudonym)

Privacy Principle 3 – Collection of solicited personal information

Privacy Principle 4 – Dealing with unsolicited personal information

Privacy Principle 5 – Notification of the collection of personal information

Privacy Principle 6 – Use or disclosure of personal information

Privacy Principle 7 – Direct marketing

Privacy Principle 8 – Cross-border disclosure of personal information

Privacy Principle 9 – Adoption, use or disclosure of government related identifiers

Privacy Principle 10 – Quality of personal information

Privacy Principle 11 – Security of personal information

Privacy Principle 12 – Access to personal information

Privacy Principle 13 – Correction of personal information

Are there Other Rules that Apply?

If an organisation has customers or other individuals who are the subject of data collection and these people live outside Australia, there may be laws from other jurisdictions that apply – these may include:

- The European Union General Data Protection Regulation (GDPR).
- The California Consumer Privacy Act of 2018 (CCPA).

Why Should this Interest Internal Auditors?

The 'International Standards for the Professional Practice of Internal Auditing' require internal audit to be risk-based, with Internal Audit Standard 2010 'Planning' stating:

> *The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organisation's goals.*

Therefore, privacy-related risk should be included in the risk-based internal audit planning process to ascertain whether it should be included in the plan – this could occur in the following ways:

- An audit to ascertain whether the organisation is in compliance with the Australian Privacy Principles.
- A discrete internal audit engagement where application of the Privacy Principles within the organisation is reviewed.
- A component of individual internal audit engagements where there may be a privacy element, for example an audit of data governance.

Caveat

Application of privacy law can be complex. This Factsheet is intended to provide general awareness and does not provide legal advice. Internal auditors asked to address application of privacy requirements within their organisation are reminded of Internal Audit Standard 1210 'Proficiency':

> *Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.*

Acknowledgement

This Factsheet has drawn upon information from the organisation Privacy International and the Office of the Australian Information Commissioner.

Useful References

Office of the Australian Information Commissioner, n.d. Australian Privacy Principles. [Online]
Available at: https://www.oaic.gov.au/privacy/australian-privacy-principles

Office of the Victorian Information Commissioner, n.d. Privacy. [Online]
Available at: https://ovic.vic.gov.au/privacy

Privacy International, n.d. PI. [Online]
Available at: https://www.privacyinternational.org

The Institute of Internal Auditors Inc, 2017. International Professional Practices Framework. Lake Mary, FL, USA: Internal Audit Research Foundation.