## **8. Privacy-enhancing technology**

Data security and individual privacy rights are paramount considerations in the digital information age and an urgent global priority. Privacy-enhancing technologies (PETs) employ various measures to secure data by: (i) reducing or eliminating personal data, or (ii) preventing the unnecessary processing of personal data while preserving the functionality of the data system.[[1]](#footnote-2)

In addition to traditional cryptographic techniques, corporations and other entities may utilise a variety of PETS to achieve these goals. These include data obfuscation, encrypted data processing, data accountability tools, and federated and distributed analytics. The integration of these emerging technologies promotes a privacy-by-design or default paradigm. This approach typically involves incorporating PETs into system infrastructure from the outset and modifying how organisations collect and use personal data.

In Australia, entities are indirectly encouraged to use PETs to meet their obligations under the Australian Privacy Principles (‘**APPs**’) concerning personal information collection, retention, and handling.

## ***8a. Cryptography***

Cryptography is a fundamental method for enhancing individual privacy and serves as the foundation for many data security iterations, including private and hybrid blockchains, virtual private networks (VPNs), and distributed database systems. For entities gathering, retaining and transmitting sensitive personal information digitally, it offers a safeguard to protect individuals from unauthorised access, interception and data tampering.

The widespread use of cryptographic encryption is attributed mainly to the uptake of Pretty Good Privacy (‘**PGP’**) encryption programs. Encryption can enhance or undermine data protection, depending on how it is used. When individuals encrypt their personal information and retain the private key, they effectively maintain autonomy over disclosing their information. When an individual encrypts another person's personal information using a public key and withholds the private key, it mirrors the basic operations of ransomware. For more information on ransomware in cybersecurity, see [Simplilearn’s video](https://www.youtube.com/watch?v=-KL9APUjj3E).

Cryptographic encryption works by converting data into a ‘secret’ code, ensuring only authorised individuals may access, view and change the information contained within the data. Authorised individuals can use a cipher (a key) allowing the user to decrypt obfuscated data into its original format. The technology is interpolated into various messaging platforms such as [Meta](https://engineering.fb.com/2023/12/06/security/building-end-to-end-security-for-messenger/), [Wickr](https://wickr.com/security/) or [WhatsApp](https://faq.whatsapp.com/820124435853543) and remains a trusted security measure in the Wikileaks submission portal.

Cryptographic encryption requires three critical components:

1. **Data that needs to be protected**. This data could be confidential information such as a message, file, or other digital content.
2. **A sender who possesses a public key**. A public key is a cryptographic code that may be freely distributed and is used to encrypt the data. The sender utilises the public key to encrypt the data before sending it to the intended recipient.
3. **The receiver of the encrypted data holds the corresponding** **private key**. The private key is kept secret and is used to decrypt the received data that has been encrypted using the public key.

## ***8b. Regulation***

The proper use of PETs generally falls within the mandate of the Office of the Australian Information Commissioner (‘**OAIC**’) to ensure organisations take reasonable steps when handling personal information and maintain acceptable data retention practices in compliance with the *Privacy Act 1988* (Cth) and other relevant laws. The regulatory framework in Australia encourages but generally does not expressly require organisations to use privacy-enhancing technologies (PETs).

### ***8b(1). Law enforcement powers***

In Australia, law enforcement is conferred broad powers to compel certain private intermediaries to provide ‘technical assistance’ to garner access to encrypted communications concerning criminal investigations. Under the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 *(TOLA Act*), service providers must provide law enforcement access to decrypted communications or decryption tools, stripping anonymity or privacy of communications. These laws remain controversial globally and perhaps best explained in [Tim Cook’s open letter](https://www.apple.com/customer-letter/) to customers in 2016 following the company’s refusal to comply with FBI requests to remove cryptographic features. The*TOLA* Actarguably undermines the essential security features of encryption and infringes upon individual privacy rights.

### ***8b(2). OAIC powers***

The regulatory powers conferred on the OAIC govern the use of PETs by monitoring government and private entities' compliance with the APPs set out in Schedule 1 of the *Privacy Act*. The OAIC may commence an investigation based on individual complaints or the Information Commissioner’s initiative regarding potential breaches. Where entities report a data breach per their obligations under the Notifiable Data Breaches Scheme (‘**NDBS**’), the OAIC will assess the data breach and provide advice or further investigate the matter to mitigate and prevent further impacting personal privacy.

The investigative powers conferred on the OAIC provide authority to compel the provision of information regarding data access, record-keeping, and internal policies. The OAIC may conduct Privacy Assessments to evaluate an entity's compliance with the *APPs*. Where the OAIC determines non-compliance with or a breach of the *Privacy Act*, it may order data handling practices to cease or change, issue infringement notices, or apply to the Federal Court seeking orders of injunctive relief and financial penalties for repeated and serious breaches.

The OAIC may also publish investigation outcomes and issue public notices regarding potential non-compliance, breaches and privacy issues associated with the practices of specific organisations. This ensures transparency, alerting the public to the privacy risks associated with organisations, and acts as a deterrent for other organisations lacking or inappropriately handling personal information. For example, in the wake of the Facebook and Cambridge Analytica political data-sharing controversy,[[2]](#footnote-3) the OAIC investigated with the Commissioner, bringing proceedings against Facebook for serious and repeated interferences with privacy. While pending determination, the OAIC has published the particulars of the allegations highlighting breaches of APP 6 and 11.

## ***8c. Case studies***

### ***My Health Records Act 2012* (Cth) and *Health Identifiers Act 2010* (Cth)**

My Health Records facilitates identifying and maintaining patient records, enabling informed communication between healthcare providers regarding individual healthcare recipients. An individual health identifier (‘**IHI’**) is assigned to a collection of personal information from those recipients per s 7(3) of the *Health Identifiers Act 2010 (Cth)* (‘**HI Act**’) for use in the My Health Record data system. Personal information such as names, addresses, dates of birth, government identifiers, and the resultant IHI constitutes personal information under s 33C(1)(a) of the *Privacy Act*.

Healthcare providers must also take reasonable steps to protect IHIs from unauthorised data use, misuse, or loss (s 27). In addition to the range of compliance obligations regarding personal information under the *Privacy Act,* the *HI Act* sets a higher privacy standard, making individuals liable to face criminal and civil penalties for unauthorised disclosures and data misuse (s 26). Concurrently, a breach of the HI Act will interfere with the affected parties' privacy for any regulatory action taken under the *Privacy Act*.

The OAIC’s role involves investigating privacy matters arising from data handling personal information in the My Health Record system. Part V of the *Privacy Act* sets out the OAIC’s investigative powers. However, the Information Commissioner has a broader power under s 73(4) to “do all things necessary or convenient to investigate” contraventions of the *My Health Records Act*.[[3]](#footnote-4)

While seemingly broad, [commentary](https://www.theguardian.com/australia-news/2019/nov/25/my-health-record-failed-to-manage-cybersecurity-and-privacy-risks-audit-finds) following My Health Record system [audits](Auditor-General%20Report%20No.%2013%20(2019-20),%20Implementation%20of%20the%20My%20Health%20Record%20System%20(Australian%20National%20Audit%20Office).) shows it lacked proper management of shared cyber security risks. Specifically, there was no assurance framework monitoring third-party software connecting to the system nor a means to monitor compliance with the security requirements per the legislation. [[4]](#footnote-5) At that time, the My Health Record system boasted a robust core infrastructure, though third-party applications, such as a [Microsoft OS update](https://www.abc.net.au/news/2024-08-07/drt-crowdstrike-root-cause-analysis/104193866), could undermine the system's security.

1. [https://www.edps.europa.eu/data-protection/data-protection/glossary/p\_en#pets](https://www.edps.europa.eu/data-protection/data-protection/glossary/p_en" \l "pets) European Commission, 2023. Glossary of the European Data Protection Supervisor. [↑](#footnote-ref-2)
2. Katherine Sainty and Belyndy Rowe, 'OAIC v Facebook' (2020) 39(2) *Communications Law Bulletin* 17. [↑](#footnote-ref-3)
3. See also, *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (Cth). [↑](#footnote-ref-4)
4. See, Auditor-General Report No.13 2019–20 Implementation of the My Health Record System at 17-18 [↑](#footnote-ref-5)