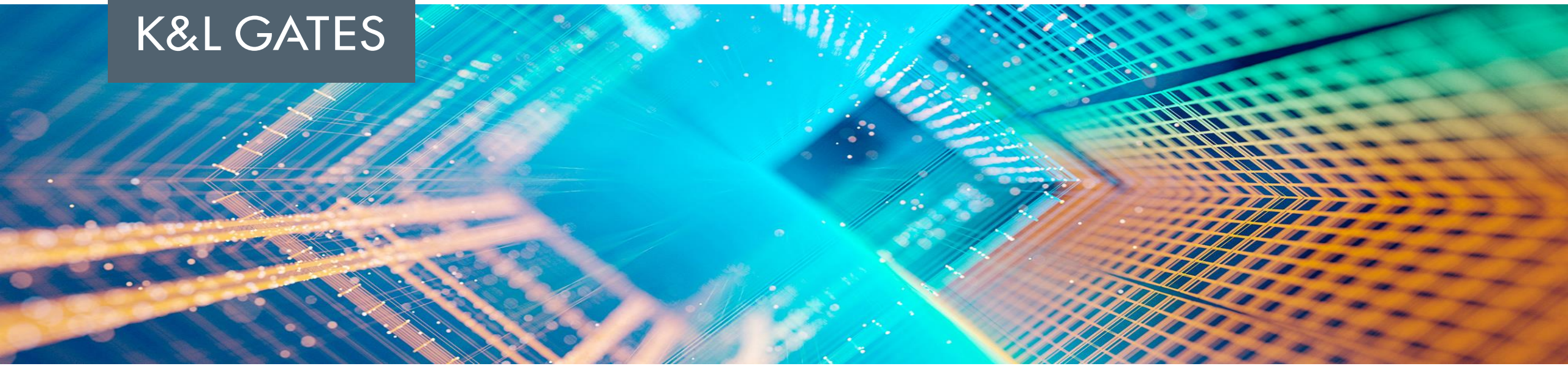
K&L GATES



Wednesday 15 February 2023

Giddyup!', 'Get Your House in Order' and 'the Best Time to Start was Yesterday': Privacy and Cyber Security Risks are Rapidly Changing

Rob Pulham, Special Counsel | Commercial Technology, Sourcing and Privacy
Stephanie Mayhew, Lawyer | Commercial Technology, Sourcing and Privacy

K&L GATES

Contents

Privacy Act Reform

Amendment to the *Privacy Act 1988* (Cth)

- On 12 December 2022 the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* came into force. It amends the following:
  - OAIC enforcement powers
  - OAIC information gathering powers
  - Increases civil penalties
  - Extraterritorial application of the Act

Increased civil penalities

The Enforcement Act increases the maximum penalties for serious or repeated privacy breaches. For body corporates/organisations this increases the penalty from the current AU$2.22 million to whichever is the greater of:

- AU$50 million
- If the court can determine the value of the benefit that the body corporate, and any related body corporate, have obtained directly or indirectly and that is reasonably attributable to the conduct constituting the contravention—3 times the value of that benefit
- If the court cannot determine the value of that benefit—30% of the adjusted turnover of the body corporate during the breach turnover period for the contravention

Greater Enforcement Powers

- Broaden the potential scope of determinations the OAIC can make, including permitting the OAIC to make declarations following the conclusion of an investigation that require the organisation to:
    - Prepare and publish or otherwise communicate a statement about the conduct
    - Engage, in consultation with the OAIC, a suitably qualified independent advisor to review the practices that were the subject of the investigation, steps taken to remediate the breach and any other matter relevant to the investigation and provide a copy of the review to the OAIC
- The Act also permits the OAIC to publish the determination on its website
- Enables the OAIC to issue an infringement notice for failures to provide information as required by the Act

Expanded Information Gathering Powers

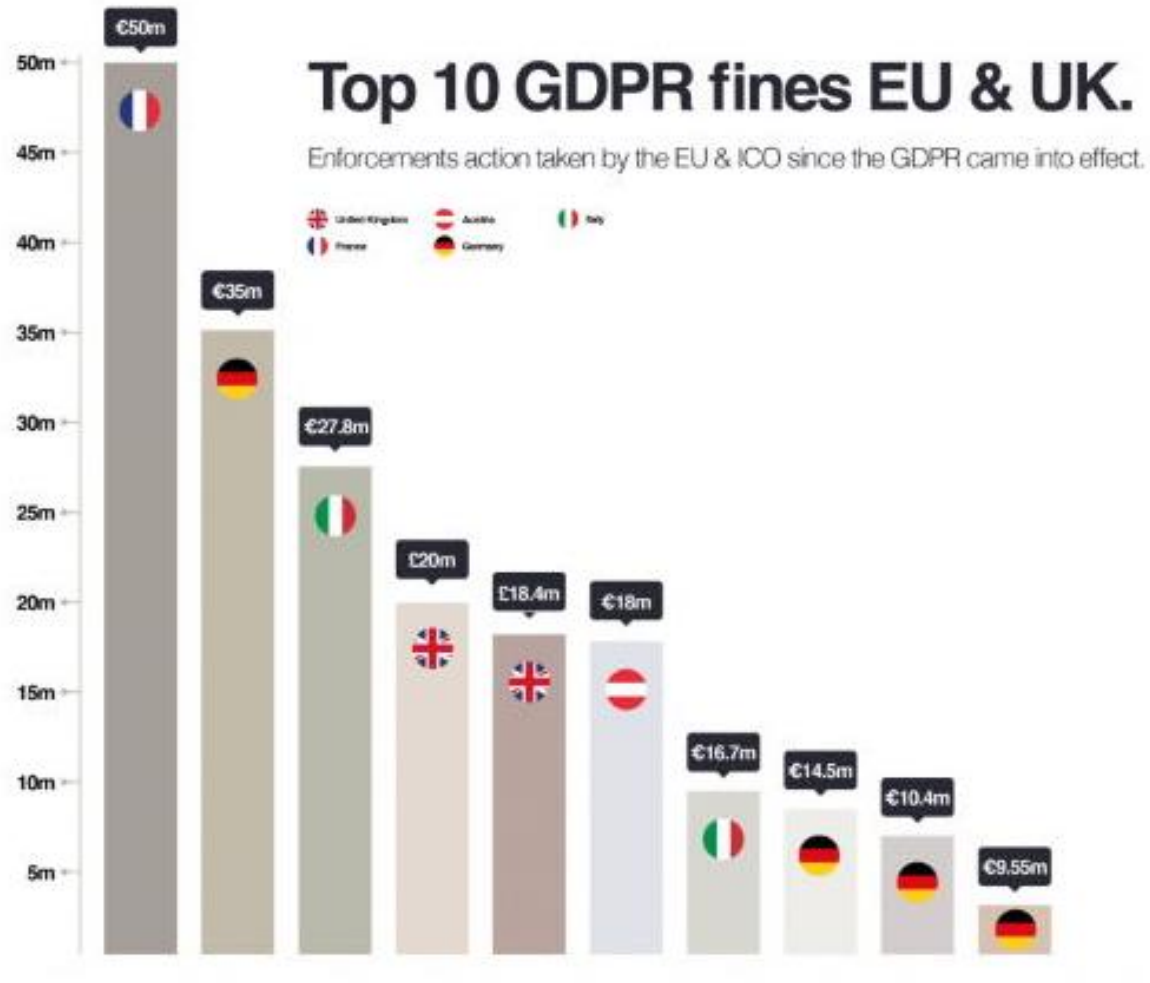
The Act provides the OAIC with the power to disclose/share information or documents with:

- An enforcement body
- An alternative complaint body
- A state, territory or foreign regulator that has functions to protect the privacy of individuals.
    - (The explicit information-sharing powers regarding foreign regulators continues the OAIC's focus on greater collaboration with equivalent foreign regulators given the increasing prevalence of cross-border data flows)

Expansion of the Extraterritorial Application of the Act

- An overseas business is bound to comply with the Privacy Act if the business has an "Australian link". Previously, to establish an "Australian link" the overseas business would need to:
    - Carry on business in Australia or an external territory
    - Collect or hold personal information in Australia or an external territory
- The Act removes the second requirement, with the effect that foreign organisations that do not collect or hold Australian personal information directly from a source in Australia are now subject to the Privacy Act if they carry on business in Australia

What's Next? - "European Style Privacy Laws" Expected



https://www.normcyber.com/smartbloc/gdpr-fine-tracker/

What we could see in following reforms:

- Removal of the employee records exemption and potentially the small business exemption
- Right to "be forgotten" (i.e. to erase data)
- Specific cookies requirements, and
- Cracking down on requiring more express consents.

Quotes

> Major cyberattacks that occurred last year such as to Optus were a “wake-up call” for company directors…cyber should always have been a top risk facing corporate Australia *ASIC Chairman, Joe Longo, Financial Review 9 January 2023*

> For all Boards, cyber resilience has got to be a No.1 risk facing everyone *ASIC Chairman, Joe Longo, Financial Review 9 January 2023*

Cybersecurity

- *Security of Critical Infrastructure Act 2018 (Cth):*
  - Applicable to the critical infrastructure areas: data storage and processing sector, communications sector, financial services and market sector, water and sewerage sector, energy sector, health care and medical sector, higher education and research sector, food and grocery sector, transport sector, space technology sector, defence industry sector (s8D)
  - Section 9 lists the critical infrastructure assets such as critical telecommunications asset, critical gas asset, critical domain name system, critical public transport asset etc.
  - Reforms came into effect at the end of 2021 which increased reporting requirements for affected entities and assets
  - There are a number of positive obligations imposed by the SOCI Act which attract hefty fines if not complied with
  - In addition to reporting obligations under the Notifiable Data Breach Scheme, SOCI entities are required to also notify under the SOCI Act – often on much shorter timeframes. Up to AU$55,500 fines (for corporations) can be imposed for failing to do so

Cybersecurity – Data Breaches

- What is a Data Breach?
  - When data is inadvertently shared with or maliciously accessed by an unauthorized person or third party
  - A data breach can be the result of an accident (e.g. email sent to incorrect person in human error) or because of security breach
- There isn't a 'bullet-proof' system to avoid data breaches, however there are a number of mechanisms you can put in place to reduce risk and consequences of a data breach, and to help smooth out the response and mitigate the fall out and consequences that result from one
- There are notification requirements under both the Notifiable Data Breach Scheme and the SOCI Act (if applicable to your entity)

Optus Data Breach

Commissioner Falk has urged all organisations to review their personal information handling practices and data breach response plans to ensure that information is held securely, and that in the event of a data breach they can rapidly notify individuals so those affected can take steps to limit the risk of harm from their personal information being accessed… and to only collect what is reasonably necessary to your business

OAIC – Media Statement, 11 October 2922

- Ransomware attack
- The OAIC commenced investigation into the personal handling practice of Optus and its related entities on 11 October 2022 – this is ongoing and is coordinated with ACMA
- The investigation will focus on whether the Optus companies complied with APP 11 including whether the information collected and retained was necessary to carry out their business
- The investigation will also consider whether the Optus companies took reasonable steps to implement practices, procedures and systems to ensure compliance with the Australian Privacy principles (APPs), including enabling them to deal with related inquiries or complaints
- Facing penalties of up to AU$2.2 million for each contravention

Ransomware/Malware Attacks

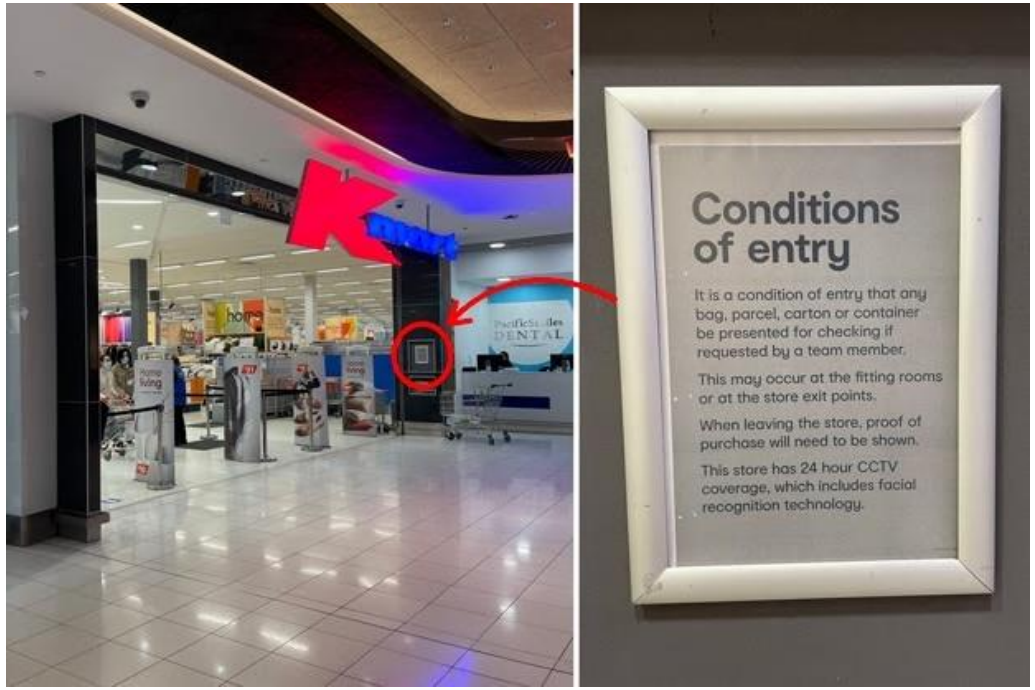
- What is it?
- Average ransom payments are almost a quarter-million dollars around the world
- Should you pay a ransom?
- Maersk ransomware attack – one of the largest globally with devastating impacts
    - One of the largest shipping and logistics company in the world
    - NotPetya – disguised as ransomware however was a malware that wrecked the master boot records of a computer hard drive – in other words it was designed to destroy IT systems
    - NotPetya took advantage of weak identity and access controls
    - A remote backed-up server located in a remote office in Ghana essentially saved the company
    - Some staffers have reported that some of the corporations severs up until the attack were still running on Windows 2000
    - After the attack – a huge security revamp occurred
    - Cost Maerk between AU$250 million to AU$300 million but it is believed their accountants low balled this figure
- No shame in getting infected – you need to learn from the mistakes and lessons shared from other businesses who have suffered it

Cyber Security/Breach Response Planning

- Being ready is about following frameworks, good IT and security practices and ensuring you have realistic processes in place
- There are a number of frameworks / standards to follow these days such as the ISO's ISO 27001 Information and Security Manual, the NIST Cybersecurity Framework, and ASD's Essential Eight
- It is prudent to ensure:
    - Your organisation has a plan ready to deal with an attack
    - The right people to deal with an attack are identified early - they know they're part of it, and are senior enough to be listened to and taken seriously
    - The process is clear, readily accessible and can be easily followed when needed

Growing Privacy Trends – Facial Recognition

- The process of identifying or verifying a person using their face. The process captures the face into a set of digital information based on the person's facial features and then face matches to verify if two faces belong to the same person
- Common every day uses – smartphones (unlocking your iPhone), pubs and clubs for security purposes, banking to verify identity, policing and national security, border access and control
- Bunnings, Kmart and The Good Guys – investigations by OAIC and Choice into activities involving facial recognition:
    - The OAIC opened investigations into Bunnings and Kmart following a report from consumer advocacy group CHOICE
    - Preliminary inquiries have commenced with the Good Guys following reports that company had paused its use of facial recognition technology



Where to now?

Getting your house in order - Our best tips for basic privacy compliance:

- **Audit -** Review your information holdings to understand what you collect
- **Downsize -** Information holdings: need to have vs nice to have
- **Update -** Privacy policy/collection statements/all relevant policies
- **Secure -** Current (up-to-date) security measures
- **Promote -** Embed a strong privacy culture throughout your organisation
- **Monitor -** Make sure you stay up to date with latest developments, advice from regulators, and major contributors to other breaches

Contacts

Cameron Abbott

Partner
Melbourne
+61 3 9640 4261
Cameron.Abbott@klgates.com

Rob Pulham

Special Counsel
Melbourne
+61 3 9640 4414
Rob.Pulham@klgates.com

Stephanie Mayhew

Lawyer
Sydney
+61 2 9513 2371
Stephanie.Mayhew@klgates.com

K&L GATES