



Privacy and mandatory data breach notification regime – Data your clients' core business

6th Annual 10 Points in One Day

28 February 2019

Parramatta, Australia

Annelies Moens

Managing Director

Privcore Pty Ltd

BSc, LLB (Hons), MBA

CIPT, FAICD, CMgr FIML





About us

Privcore's team with 40 years' combined experience helps business and government **make privacy core business** so they can deliver services with the trust and confidence of customers and citizens.

Privacy impact assessments

Data breach prevention and recovery

Audit and privacy health checks

Privacy by design

Privacy management frameworks

Algorithmic impact assessments

Privacy maturity models

Training or presentations

Privacy or related research

APEC Cross Border Privacy Rules



Making privacy core business



Overview

- Why professional service firms need to think about data and privacy
- Privacy and cyber risks
- What happens when you have a data breach
- Mandatory data breach reporting: one year on
- General Data Protection Regulation (GDPR): Does it apply to you?
- Key aspects of GDPR for professional service firms
- New developments



Making privacy core business

Why you need to think about data and privacy:

- Finance, legal and accounting and management service firms are targets because they hold large amounts of clients' personal information

Table 1.B — Kinds of personal information involved in breaches by percentage of notifications - All sectors

Kinds of personal information	% of NDBs received
Contact information	85%
Financial details	47%
Identity information	36%
Health information	27%
TFN	18%
Other sensitive information	9%

Source: OAIC
 Quarterly
 Breach
 Statistics
 Oct – Dec 2018



Making privacy core business

Finance, legal and accounting and management sectors are consistently the top 2 and 3 targets

Table 2.A – Top five sectors by notifications in the quarter

Top five sectors	NDBs received
Health service providers ¹	54
Finance (incl. superannuation) ²	40
Legal, accounting and management services	23
Education ³	21
Mining and manufacturing	12

Source: OAIC Quarterly Breach Statistics
Oct – Dec 2018



Making privacy core business

Even if you don't have to comply because you are an exempt small business and don't handle TFNs

- Are you willing to risk your reputation and deal with the aftermath of a data breach?
- Risk minimisation is critical – it is a highly likely to occur risk
- People care about privacy, their concerns are escalating





Why?

Top 5 Global Risks in terms of Likelihood

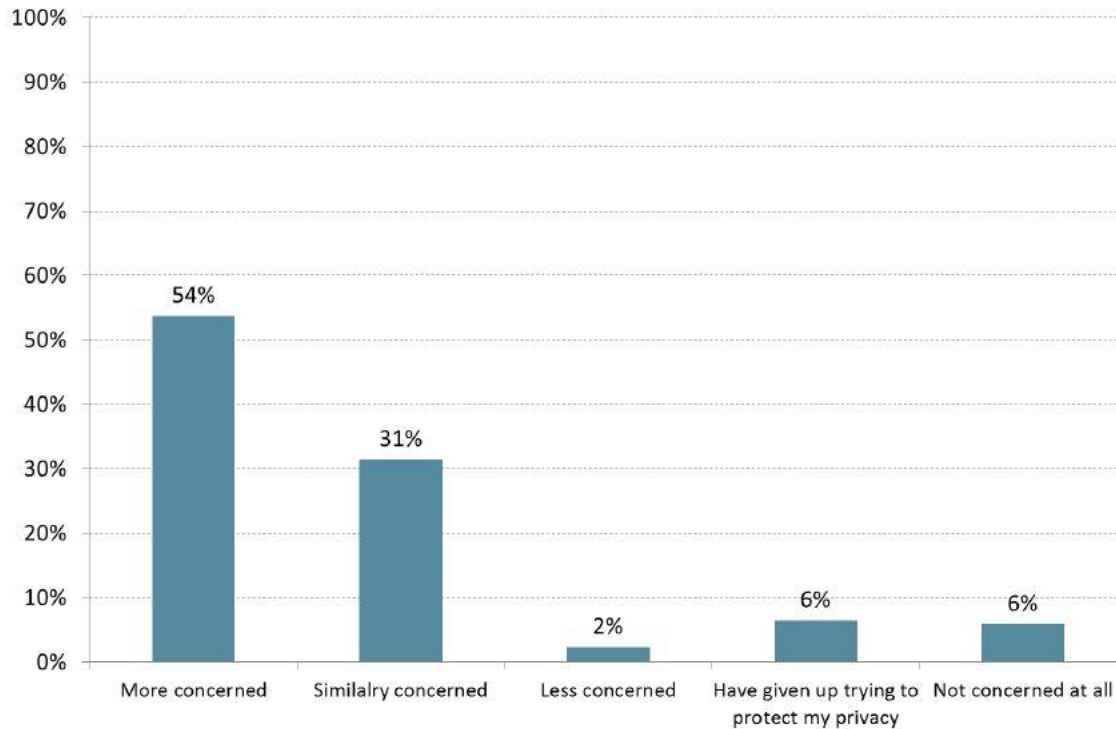


Source: WEF Global Risks Report 2019



Making privacy core business

Figure 20: Change in concerns about privacy of personal information over 12 months



ACCC Digital Platform Survey, 10 December 2018



Making privacy core business



Why?

Google top search terms in Australia 2018

- 1. How to opt out of My Health Record**
2. How to watch World Cup in Australia
3. How to win Powerball
- 4. How to delete Instagram**
5. Google Arts and Culture face match how to
6. How to buy bitcoin
7. How to lose weight fast
8. How to screenshot on iPhone X
- 9. How to delete Facebook**
10. How to lose belly fat



Making privacy core business



Privacy and cyber risks

Common risks:

- Over collection of personal information – think about lean data instead of big data
- Never deleting data
- Third party arrangements with vendors and suppliers that do not protect personal information
- Phishing attacks
- Human error – emailing personal information to the wrong recipient
- Loss or theft of data – eg: losing a USB



Making privacy core business



So what happens...?

So what happens WHEN you have a data breach?

KEY QUESTIONS:

1. How will you know you have been subjected to a data breach?

3. How do you minimise the risk/impact of a data breach?

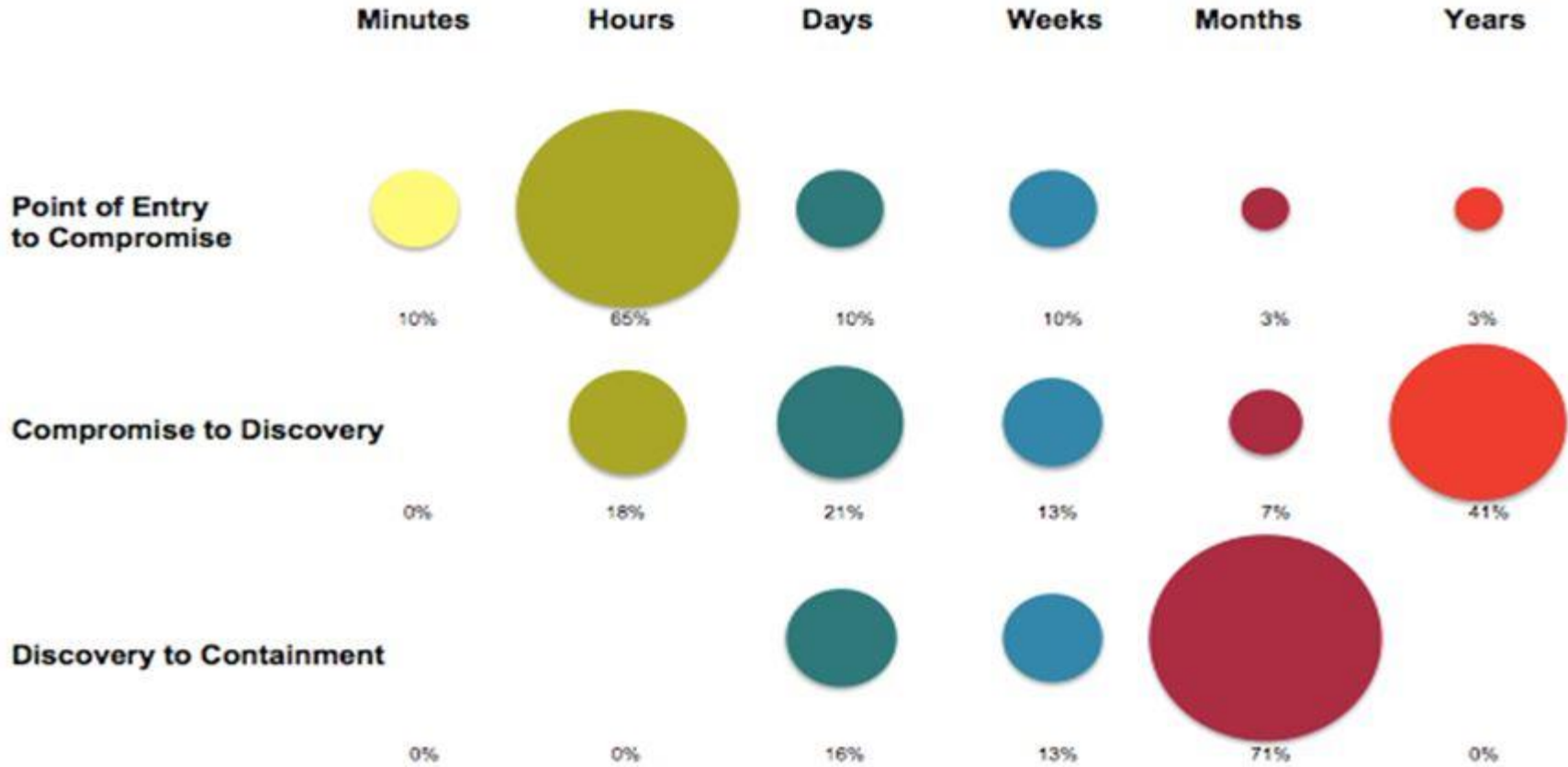
2. What's the impact of a data breach?

4. How do you implement a data breach response plan?





1. How will you know?



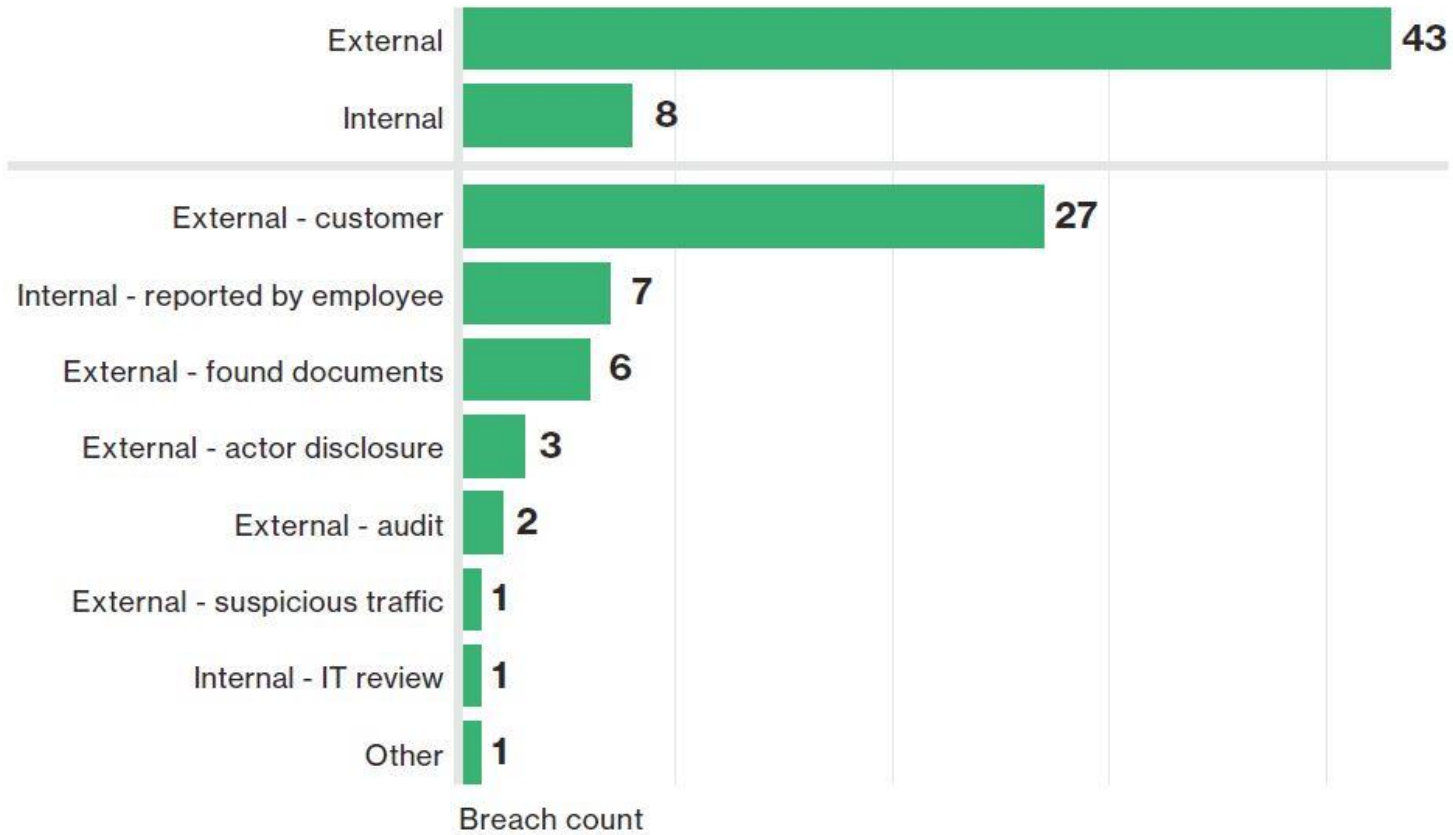
Source: Verizon's 2012 Data Breach Investigations Report

Making privacy core business





1. How will you know?



Source: Verizon's 2016 Data Breach Investigations Report



Making privacy core business



2. What's the impact of a data breach?

- Financial services and professional service sectors were the top two targeted sectors in 2018
- The average total cost per data breach in Australia was ~\$US 2 million in 2018
- Data breaches caused by a 3P, compliance failures or migration to the cloud resulted in higher costs
- Costs of data breaches decreased where data breach response teams were deployed or extensive encryption was in place
- Malicious and criminal attacks are the main cause and are also the most expensive, at \$US108 per record in Australia

Source: 2018 Cost of Data Breach Study: Global Overview, Ponemon Institute LLC (sponsor IBM), July 2018



Making privacy core business



2. What's the impact of a data breach?

MasterChef finalist caught in conveyancing hacker attack

etails, TFNs, personal details of job
nts potentially compromised in major
data breach



Clare Blumer, ABC Investigations

By Si

22 Jun

One Of The World's Biggest Accounting Firms Hacked After Basic Security Goof

April 15

Rhett Jones

Sep 26, 2017, 9:00am · Filed to: azure

Share

Equifax data breach could be the most costly in corporate history

The company's expected breach-related costs through the end of this year could be as much as US \$439 million



Making privacy core business



3. How do you minimise the risk/impact of a data breach?

Common mitigation strategies:

- Collect only the data needed – be clear about what is optional and what is mandatory
- Have a data destruction plan in place and execute it
- Have a data breach response plan in place – expect a data breach to happen
- Undertake privacy and phishing training for staff
- Never use the same password on accounts and use complex passphrases – use a password safe
- Enable multi-factor authentication
- Encrypt all storage devices – laptops and USBs
- Consider cyber insurance and undertaking a privacy health check





4. How do you implement a data breach response plan?

1. Contain the breach and do a preliminary assessment within 30 days
2. Appoint lead person to manage (internal and/or external) response team
3. Evaluate the risks associated with the breach
4. Consider breach notification (mandatory and voluntary)
5. Review the incident and take action to prevent future breaches





Mandatory data breach reporting

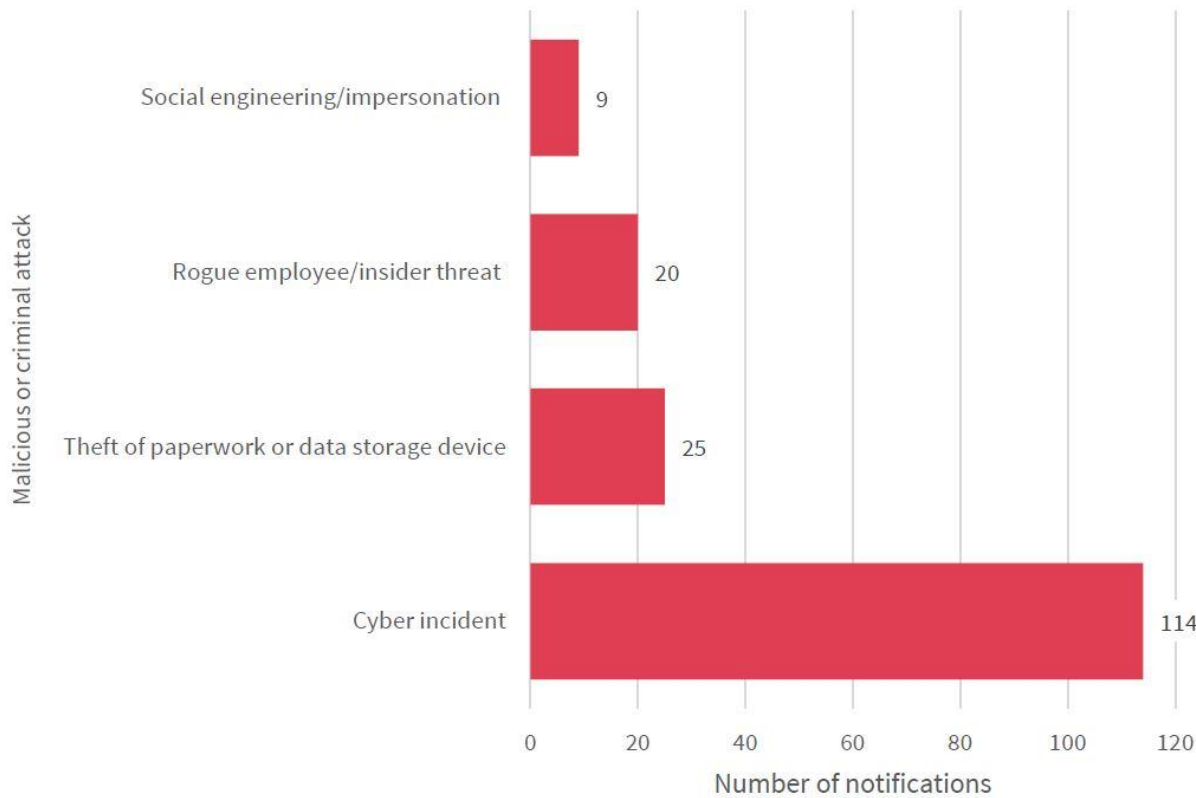
Privacy Amendment (Notification Data Breaches) Bill 2017 commenced on 22 February 2018 (in operation for one year)

- 812 data breaches notified between 22 Feb and 31 Dec 2018
- That means averaging around 1,000 per year or 20 per week
- Generally two-thirds of notified data breaches are due to malicious or criminal attacks and one-third due to human error



Making privacy core business

Chart 1.6 — Malicious or criminal attacks breakdown — All sectors

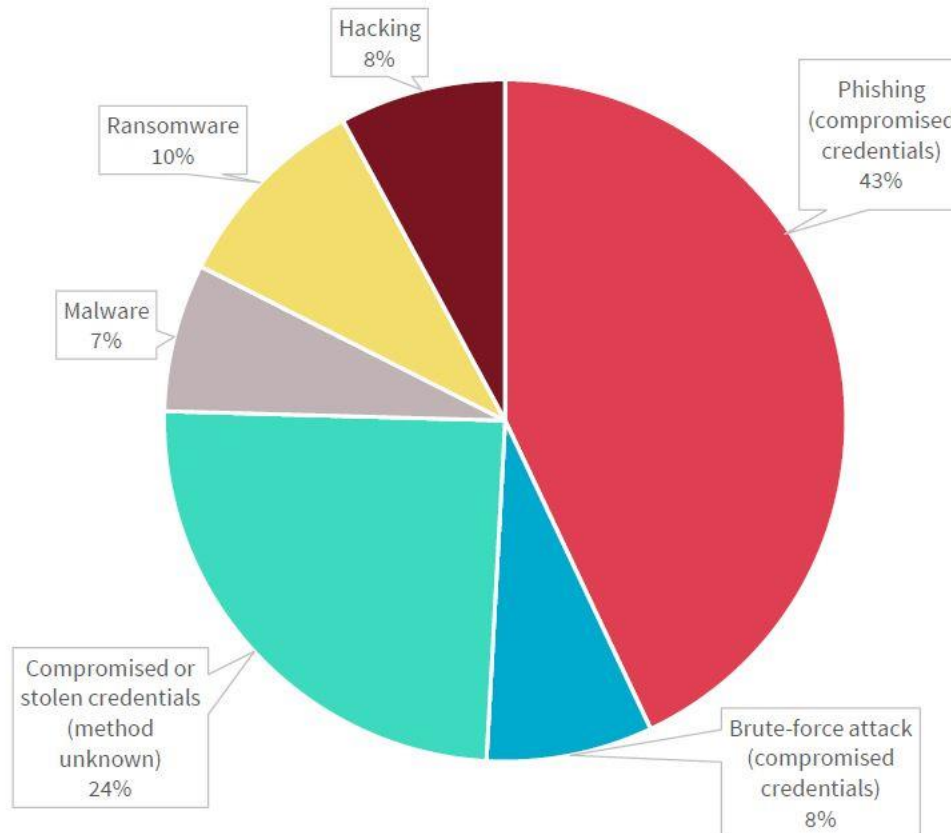


Source: OAIC
Quarterly Breach
Statistics
Oct – Dec 2018



Mandatory data breach reporting

Chart 1.7 — Cyber incident breakdown — All sectors



Source: OAIC
Quarterly Breach
Statistics
Oct – Dec 2018



Making privacy core business



Mandatory data breach reporting

- Australian Information & Privacy Commissioner:
“Multi-factor authentication is a reasonable step to take to secure personal information”
- APP 11: Security of personal information
- If that reasonable step (multi-factor authentication) is not taken then the regulated entity is in breach of the Privacy Act

Source: Senate Estimates, 22 October 2018, Legal and Constitutional Affairs Legislation Committee



Making privacy core business

Mandatory data breach reporting

30 days to undertake assessment

Direction to notify

Serious harm

- This Part sets up a scheme for notification of eligible data breaches.
- An eligible data breach happens if:
 - (a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
 - (b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.
- An entity must give a notification if:
 - (a) it has reasonable grounds to believe that an eligible data breach has happened; or
 - (b) it is directed to do so by the Commissioner.





Examples of serious harm

Reasonable person test

Access/
disclosure or
loss would likely
result in serious
harm



Making privacy core business

Exceptions



- Action is taken to remediate before the breach results in serious harm
- Other entities involved in data breach and one of them has already notified the regulator and affected individuals
- Enforcement body has a breach when conducting enforcement activities
- Inconsistent with federal secrecy provisions
- When notification is instead required under the My Health Records Act
- Commissioner's declaration that no notification is required (on own initiative or by application) ○ ● ● ●

Making privacy core business

Notification



- Notification – must set out the following:
 - Identity and contact details of entity
 - Description of the data breach
 - The kind of information in the data breach
 - Recommendations on what affected individuals should do in response to the breach





GDPR: Does it apply to you?

Extra-territorial application – key as there is no small business exception in GDPR

Organisations need to comply with the GDPR if they:

- are established within the EU;
- offer goods or services to individuals in the EU; or
- monitor the behaviour of individuals in the EU (e.g. by tracking or profiling those individuals)




Making privacy core business










GDPR: Does it apply to you?

Offering goods or services to individuals in the EU

Website or app accessible in the EU alone
not enough 

Factors that may indicate offering goods or services:


-  language, currency
 -  delivery in the EU
 -  client testimonials from the EU
 -  marketing directed to EU
 -  EU contact numbers
 -  Use of top-level domain name of EU member state
- 

Making privacy core business



GDPR: Does it apply to you?

Monitoring the behaviour of Individuals in the EU

No specific purpose in mind not enough to constitute monitoring 

Factors that may indicate monitoring behaviour:

-  behavioural ads
-  geo-localisation activities
-  cookies, fingerprinting online
-  CCTV
-  individual market surveys
-  personalised health services - wearables



Making privacy core business

How does it extend beyond Australian privacy law?

- Overall similar – two key distinctions
 - Scope – applies to all small businesses
 - Higher penalties - Fines up to 20 million euro, or 4 percent of annual worldwide turnover (whichever is higher)
- Other differences
 - Distinction between data controllers and processors in GDPR
 - 72 hours to determine whether data breach notification required
 - Right to erasure of data (“right to be forgotten”)
 - Right to object to processing (in relation to automated decision-making, direct marketing / profiling)
 - Right to data portability



Making privacy core business



New developments

Treasury Laws Amendment (Consumer Data Right) Bill 2018

- Consumer data right (more like a data portability right) – intended for individuals and small businesses
- Can apply to any sector as designated by the Treasurer
 - Banking
 - Telecommunications
 - Energy and potentially other sectors
- Initially meant to come into operation on 1 July 2019, but has been delayed due to privacy and security concerns – legislation has not passed - it has been referred to the Economics Legislation Committee for inquiry



Making privacy core business



New developments



Making privacy core business



New developments

Preliminary Report – Digital Platforms Inquiry:

Exploitation of information asymmetries and the bargaining power imbalance that exists between digital platforms/other businesses and consumers.

To address this the ACCC recommends the following:

- Direct right of action to go to court
- Increased resourcing for OAIC
- Increasing penalties under the Privacy Act for breaches to whichever is greater:
 - Three times the value of the benefit received
 - 10% of the entity's annual turnover in the last 12 months
 - Fine increased from \$2.1M to \$10M



Making privacy core business



New developments

Continue - Preliminary Report – Digital Platforms Inquiry:

- Strengthening notice and consent requirements (clarifying that it be express and opt-in)
- Making unfair contract terms in privacy policies and terms of use illegal under consumer law
- Introduction of 3P certification scheme to demonstrate compliance with privacy requirements for certain entities
- Implementation of a Code of Practice for digital platforms outlining further and in more detail their privacy obligations



Making privacy core business



New developments

The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

- Designed to compel communications providers to assist intelligence and interception agencies with accessing encrypted data
- AustCyber and ASPI survey – major concerns for businesses – from a global perspective a perceived loss of trust in Australian tech companies
- Perception that Australian encryption products/services are less secure than competitors due to the Act

Source: Australian Strategic Policy Institute, funded by AustCyber
“Perceptions Survey: Industry views on the economic implications of the Assistance and Access Bill 2018”, December 2018



Making privacy core business

New developments



APEC CBPR – Australia joined in November 2018

- Facilitates cross-border data flows whilst protecting personal information

Upcoming ISO standard – ISO 27552 – Privacy information management – requirements and guidelines

- Builds on existing security standards

New NIST Risk Management Standard – 800-37

- Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy, December 2018





More information

- Quarterly Notifiable Data Breach Statistics Reports, Office of the Australian Information Commissioner
<https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/>
- Explanatory Memorandum to the Privacy Amendment (Notifiable Data Breaches) Bill 2017
http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5747_ems_ed1_2b5bb-d3b3-4a6a-9536-53bb459a00df/upload_pdf/6000003.pdf;fileType=application%2Fpdf
- 2018 Cost of a Data Breach Study: Global Overview, Ponemon Institute LLC (sponsor IBM), June 2018
<https://www.ibm.com/security/data-breach>
- Data breach preparation and response - A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth), Office of the Australian Information Commissioner, February 2018
<https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response#part-3-responding-to-data-breaches-four-key-steps>



Making privacy core business



More information

- European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR, 16 November 2018
https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en
- ACC Digital Platform Survey, 10 December 2018
<https://www.accc.gov.au/system/files/ACCC%20consumer%20survey%20-%20Consumer%20views%20and%20behaviours%20on%20digital%20platforms%2C%20Roy%20Morgan%20Research.pdf>
- ACC Digital Platforms Inquiry - Preliminary Report, 10 December 2018
<https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/preliminary-report>
- Australian Strategic Policy Institute, funded by AustCyber
“Perceptions Survey: Industry views on the economic implications of the Assistance and Access Bill 2018”, 20 December 2018
<https://www.austcyber.com/resources/perceptions-survey>





Questions?

operations@privcore.com

www.privcore.com



Making privacy core business