Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Cyber-risk Insurance

Nick Abrahams
Partner
Norton Rose Fulbright Australia

Leisa Mikkelsen
Special Counsel
Norton Rose Fulbright Australia

September 2013

20182396.PPTX

Today

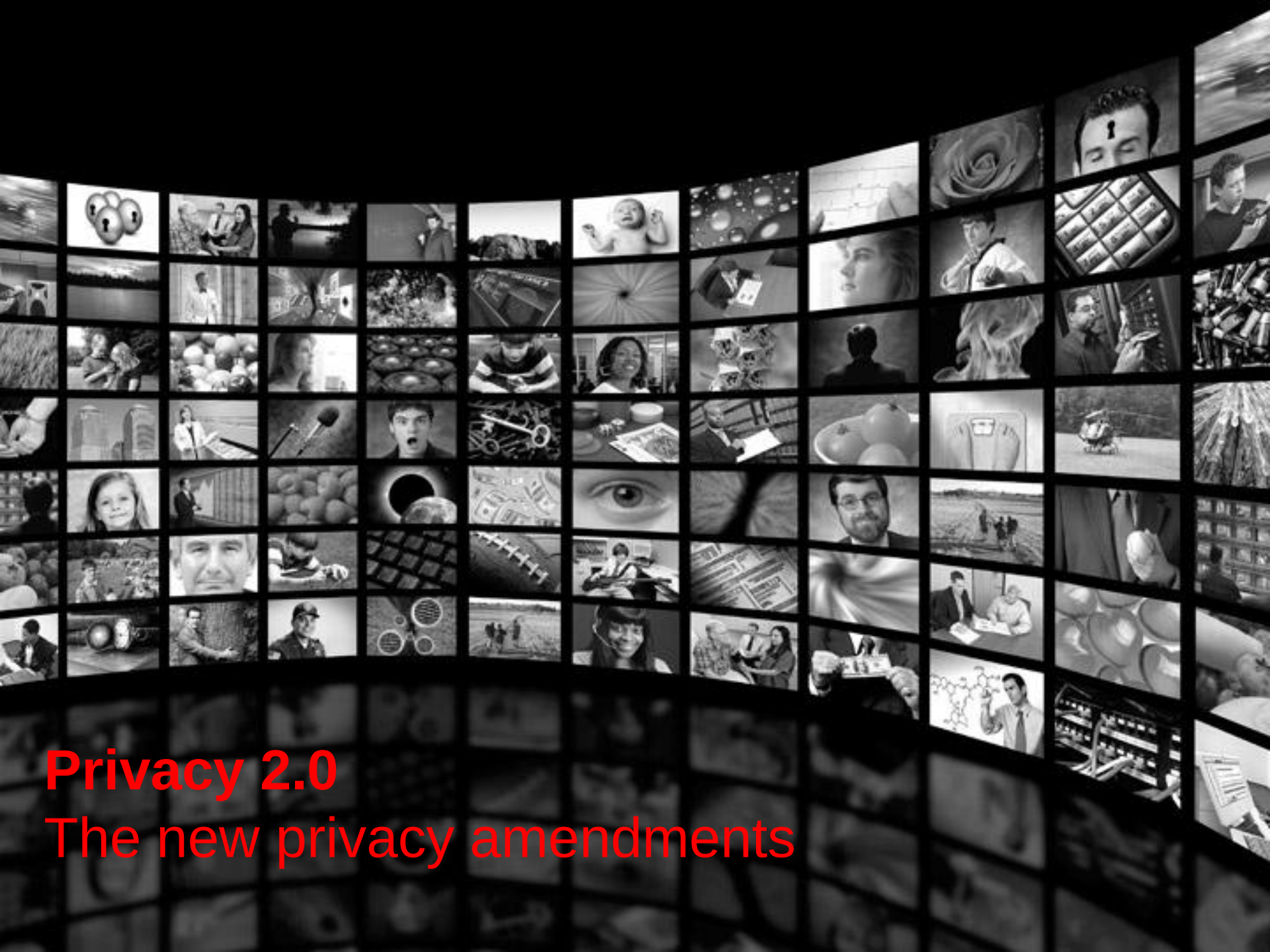
- Privacy breaches in Australia
- Upcoming changes to the Privacy Act
- Changes to the Privacy Commissioner’s powers
- Privacy breach notifications
- Security level needed for personal information
- The costs of a data breach
- Example policies

Cyber-risks

- Privacy breaches
- Loss of data
- Cost of reconstructing data
- Cost of identifying & rectifying breaches
- Loss of IP

Privacy breaches in Australia

- Sony PlayStation
  - 77 million users were affected globally when the Sony PlayStation network was hacked in 2011 - approximately 715,000 Australians were affected
  - Personal information such as names, billing details and email addresses all potentially accessed
- Telstra
  - In 2013 the personal information of thousands of Telstra customers could be found online using a simple Google search. Personal information disclosed included names, telephone numbers and home and business addresses
  - In 2010 a failed mail merge resulted in 220,000 letters going out with account information belonging to other customers
- Vodafone
  - Customer data was accessible by authorised users to check customer information in various stores
- Thousands more that have never been reported



Privacy 2.0

The new privacy amendments

Recent amendments – when do they start?

- *Privacy (Enhancing Privacy Protection) Act 2012*
  - received royal assent on 12 December 2012
  - will come into force on **12 March 2014**
  - new single set of Australian Privacy Principles

- Privacy Commissioner – no more Mr Nice Guy

Enhanced powers of the Privacy Commissioner

- The amendments strengthen the powers of the Privacy Commissioner:
  - may conduct a performance assessment of Australian government agencies and private sector organisations to determine whether they are handling personal information in accordance with APPs, credit reporting provisions and relevant codes
  - may access remedies when he/she has conducted an investigation on his/her own initiative
  - may make a determination
  - may accept written undertakings that will be enforceable through the courts
  - may apply for civil penalty orders of up to $340,000 for individuals and up to $1.7 million for companies in the case of serious or repeated breaches of privacy
  - likely to be $1.7 million for breaches over a short period of time, however there is no judicial guidance at this stage and it could be $1.7 million per breach

Key amendments – Disclosure

Increased disclosure requirements

- Privacy policies must include:
  - the kinds of personal information collected and held
  - how it is collected and held
  - purposes for which it is collected, held, used and disclosed
  - details of how to access and rectify personal information
  - complaint process for interferences with privacy
  - details of possible disclosure to overseas recipients and, if so, the likely countries (if practicable to specify)

Key amendments – Various

Dealing with unsolicited personal information

- Social media platforms can result in receipt of unsolicited personal information

Direct marketing same as Spam and DNCR

Exporting personal information

- Restrictions on exporting PI
- Need to notify individuals
- Responsible for breaches of the overseas recipient

Privacy Amendment (Privacy Alerts) Bill 2013

- Mandatory data breach notification bill – currently delayed due to ALP leadership change and subsequent Federal election

- Proposed amendments require notification when there has been a "serious data breach" that that results in a "real risk of serious harm" to the individuals

- If an APP entity believes there has been a serious data breach it must prepare a short statement to the OAIC and either:
  - send a copy of the statement to each affected individual; or
  - publish a copy of the statement to their website and publish a copy in at least one newspaper in each State.

- Penalties of $1.7M
- If passed come into effect March 2014

Data protection – new obligations

APP 11 – Security of information

- APP entities must take *reasonable steps* to protect personal information that they hold from misuse, interference, loss and unauthorised access, modification or disclosure

- APP entities must also take *reasonable steps* to destroy or de-identify personal information they hold if it is no longer needed to any purpose for which it may be used or disclosed, it is not contained in a Commonwealth record, and the entity is not required by or under an Australian law or a court or tribunal order to retain it

Security level for personal information

- 2013 *OAIC Guide to Information Security: Reasonable Steps to Protect Personal Information*
- Varies depending on:
  - the nature of the entity holding the personal information
  - the sensitivity of the personal information
  - the harm that is likely to result to individuals
  - how the agency or organisation stores, processes and transmits the personal information
  - the ease with which security measures can be implemented
- Privacy impact statements
- Staff training – security awareness and education
- Technological measures – encryption and intrusion detection
- Monitoring and review – penetration testing
- Standards - AS/NZS ISO 27000 and AS/NZS ISO 31000

Security for information - APRA

- Standards relating to the use of data by banks and financial institutions
- APRA requires banks and financial institutions, wishing to outsource a material business activity (such as data hosting) to an overseas provider, to first consult with APRA and demonstrate that risk management procedures are in place
- APRA requires a right to audit regulated entities and their service providers

If you have a data breach now

- 2012 OAIC Data breach notification guide
- Notification of a data breach supports good privacy practices
- Appropriate security safe guards should be implemented as set out in NPP 4 and IPP 4
- In the event of a data breach individuals and the OAIC should be notified, however this is not required by the Privacy Act
- Four recommended steps in responding to a data breach:
  - Step 1: Contain the breach and do a preliminary assessment
  - Step 2: Evaluate the risks associated with the breach
  - Step 3: Notification
  - Step 4: Prevent future breaches

The Costs and Losses of a breach

Costs and losses of a breach – identity theft

- ABS Personal Fraud Survey 2010-11: Australians lost $1.4 billion due to personal fraud, with 1.2 million Australians aged 15 years or over victim of at least one incident of identity fraud in the 12 months prior to the survey
- If your identity is stolen a criminal could:
  - apply for a credit card in your name
  - apply for any benefits in your name
  - register a vehicle in your name
  - apply for a passport in your name
  - apply for a mobile phone contract in your name

Costs and losses of a breach – notifications

- Significant costs incurred in notifying individuals and regulatory bodies in the event of a data breach
  - Symantec / Ponemon 2013 'Cost of Data Breach Study' – average notification cost for Australia was $220,000
  - Forensic investigation
  - Notification costs to regulatory bodies
  - Call center costs
  - Credit monitoring
- Notification can operate as an important mitigation strategy – establishes trail of evidence
- Relevant factors include the ability of the individual to take steps to avoid or mitigate possible harm if notified (eg by changing account passwords)

Costs and losses of a breach – PR cost

- The public relations damage as a result of a data breach can be ongoing and costly
  - Symantec / Ponemon 2013 'Cost of Data Breach Study' – average lost business as a result of a data breach in Australia was just under $2 million
- Lost or reduced revenue due to network downtime
- Future loss of opportunity and diminished customer acquisition
- Loss of clients and goodwill
- Distraction to senior management

Costs and losses of a breach – stopping the intrusion

- Necessary to first find and then stop the problem
  - Symantec / Ponemon 2013 ‘Cost of Data Breach Study’ – average detection cost for Australia was just under $1.2 million
- Cost of external security consultant
- Cost to repair, replace or restore systems and data as a result of breach
- Cost of downtime while system is fixed
- Crisis team management
- Audit services

Costs and losses of a breach – litigation

- Cost of potential class action litigation
- Currently prevalent in North America, but perhaps reflective of the state of the legal market there
- Probability of litigation is often correlated with the number of records lost and the sensitivity of the personal information compromised
- Plaintiffs will seek relief for harms such as actual financial loss from identity theft, emotional distress, costs of credit monitoring, and anticipated future losses

Sony Gaming Network and Customer Data Security Breach Litigation

- In April 2011 hackers gained unauthorised access to personal and financial information from an estimated 77 million users of Sony's Playstation Network and Qriocity service
- The plaintiffs in the US class action allege that:
  - Sony knew or should have known of its system's vulnerability
  - Sony negligently failed to maintain proper security
  - Sony failed to encrypt data and establish adequate firewalls to handle intrusions
  - They were injured because their personal information was stolen, exposing them to an increased risk of identity theft and fraud
- Proceedings are ongoing

Zurich American Insurance Company & Ors v Sony Corporation of America & Ors

- Zurich denied cover under its Commercial General Liability Policy
- Zurich has sought declaratory relief in the Supreme Court of the State of New York that it has no duty to defend or indemnify Sony against the class actions
- The basis for denial is:
  - No claim for "personal and advertising injury"
  - No "Oral or Written Publication Offence" which provides cover for "injury arising out of publication of material that violates a person's right to privacy"
  - No intentional publication by Sony itself
  - No "publication" of confidential information
  - "Insureds in Media And Internet Type Business" exclusion
- Proceedings ongoing

Need for cyber insurance

- Limitations on cover in traditional policies, eg CGL policies
- Coverage usually required for first party losses as well as third party liabilities
- Main risks faced by insureds:
  - Regulatory: investigations, fines and penalties, data breach costs
  - Third party claims: possibly negligence actions
  - Internal costs: can run into millions and include costs surrounding detection, investigation, containment, recovery, cost of business interruption and cost of equipment damage

Examples of policies in the market

- **Losses resulting from**:
  - A hacking virus that has emanated from or passed through either the insured's computer system or a cloud computing provider's system
  - The inability to access either the insured's system or cloud computer provider's system due to failure or impairment resulting from a hacking attack or virus
  - Loss or theft of an insured's data arising from a hacking attack or virus
- **First party cover can include**:
  - Public relations, crisis management, forensics and security specialist services
  - Data breach costs
  - Information and communication asset rectification costs
  - Cyber business interruption costs
  - Cyber extortion cover

Examples of policies in the market (cont.)

- **Third party liability**:
  - Compensation, damages or awards where the claim arises out of a failure by the insured or service provider to properly handle, manage, store or otherwise control personal information or third party corporate information, or failure of the insured to protect against unauthorised access to information by a hacker, or arising out of an infringement of intellectual property rights arising from multimedia activities
  - Defence costs
  - Extensions can include: dishonesty of employees
  - Regulatory defence and penalties: insurable at law
- **Exclusions**:
  - Claim for loss of goodwill and reputational harm

Summary

- The countdown to 12 March 2014 has begun
- It will take time to identify the required changes and then bed down appropriate policy and operational changes
- Privacy Amendment (Privacy Alerts) Bill 2013, if enacted, will be a game changer
- The cost and impact of a data breach could be very substantial
- Cyber insurance covers a series of risks that are not currently covered by the traditional basket of insurances

Questions?

Nick Abrahams

Partner

Norton Rose Fulbright Australia

nick.abrahams@nortonrosefulbright.com

+61 2 9330 8312

Leisa Mikkelsen

Special Counsel

Norton Rose Fulbright Australia

leisa.mikkelsen@nortonrosefulbright.com

+61 2 9330 8392

NORTON ROSE FULBRIGHT


NORTON ROSE FULBRIGHT

Disclaimer

NORTON ROSE FULBRIGHT