actlawsociety

legalsuper

The 2023 Intensive Conference

"Staying ahead of the game"

Conference papers

actlawsociety
1933–2023 Celebrating 90 years

MANAGING PRIVACY RISK AND COMPLIANCE

MILLS OAKLEY

Managing & Protecting Personal Information

ACT Law Society Intensive 2023:
Staying Ahead of the Game

Natalie Butler & Jason Symons
7 March 2023

Overview

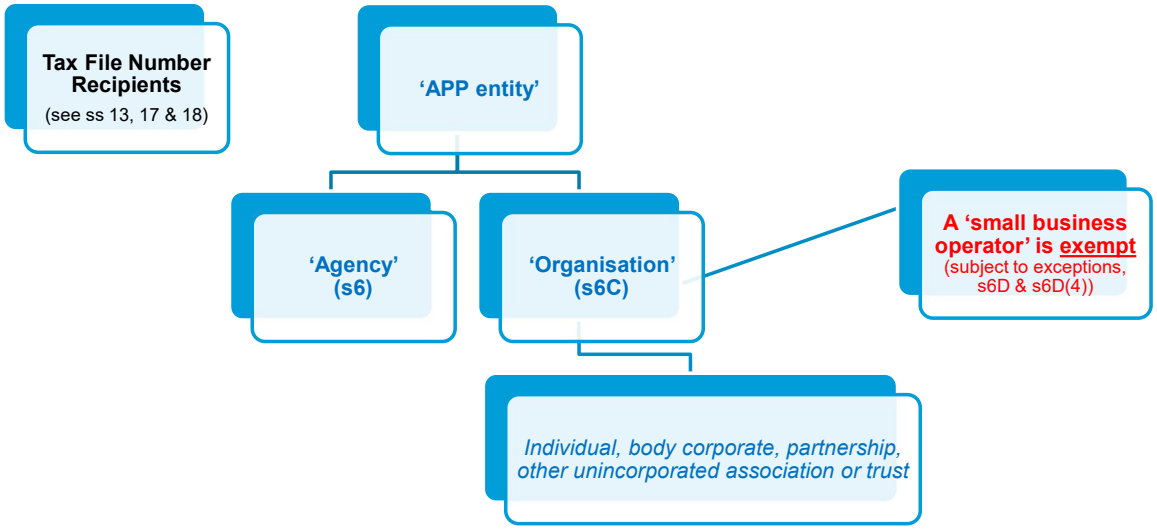
- **Privacy & Security obligations in the *Privacy Act 1988* (Cth)**
  - Regulated entities (who is covered by the Act?)
  - Relevant Australian Privacy Principles (APPs)
  - Anticipated reforms
- **Professional obligations**
- **When things go wrong**
  - Privacy complaints
  - Mandatory notifications to OAIC
  - Determinations & Penalties
- **Risk management & response**
  - Risk management, preparedness & governance
  - Cyber insurance

Regulated Entities

(and where do <u>you</u> sit within the regulatory matrix?)

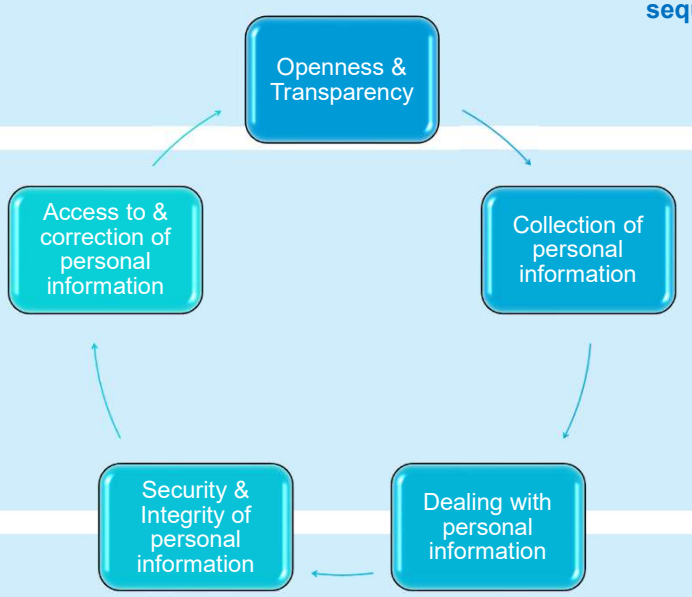
Regulated Entities

(Definitions, *Privacy Act 1988* (Cth))



What are the relevant APPs?

Data Lifecycle, as sequenced in the APPs



Security-related obligations imposed by the Privacy Act

Relevant APP & TPP	Obligation/ requirement
APP 1.2 TPP 1.2	Take reasonable steps to implement 'practices, procedures and systems relating to the entity's functions or activities' that will ensure APP compliance
APP 4.3 TPP 4.3	Destroy or de-identify unsolicited information (subject to exceptions)
APP 8.1 TPP 8.1	Ensure an overseas recipient does not breach the APPs in relation to personal information disclosed to it by the APP entity
APP 9.1	Organisations must not adopt a government identifier as its own identifier of the person
APP 11.1 TPP 11.1	Take reasonable steps to protect personal information against misuse, interference and loss, unauthorised access, modification or disclosure.
APP 11.2 TPP 11.2	Take reasonable steps to destroy or de-identify personal information that is no longer required.

Security-related obligations imposed by the Privacy Act

APP 11 – security of personal information

- Must take **reasonable steps** to protect personal information that an APP entity **'holds'**
  - Holds = possession and control of a record containing personal information
  - More than physical possession. A right to deal with the information.
- **Protect** the personal information from:
  - Misuse, interference and loss; and
  - Unauthorised access, modification or disclosure

- Must take reasonable steps to **destroy or de-identify** personal information if it's no longer needed
  - Unless part of a Commonwealth record or otherwise required by law to be kept

Security-related obligations imposed by the Privacy Act

Factors that will inform what amounts to 'taking reasonable steps' (APP 11)

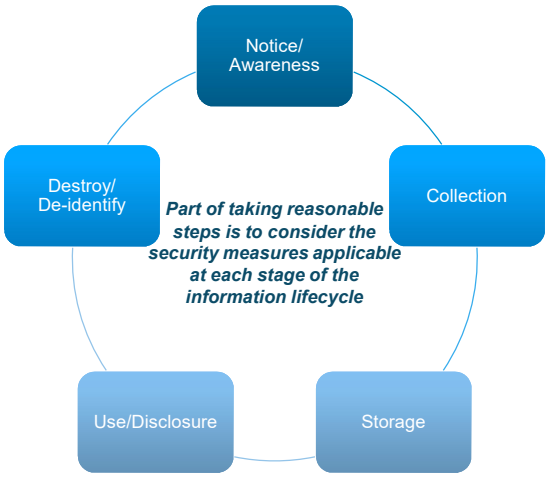
- Nature of the entity (i.e. size; resources; complexity of operations)
- Amount and sensitivity of the personal information. As the volume of the information increases, or the nature of the information is more strictly regulated, the more steps required
- Possible adverse consequences for an individual in the event of a breach. The more serious the risks and adverse consequences, the more rigorous the steps should be
- Practical implications of implementing a security measure. Whether factors such as time and cost would be an excessive burden
- Is the security measure in itself privacy invasive? Can you collect more to protect more?

Melbourne | Sydney | Brisbane | Canberra | Perth

Security-related obligations imposed by the Privacy Act

Reasonable steps should include these strategies:

- Governance, culture & training
- Internal practices, procedures, systems
- Standards (internal/external)
- Physical security
- ICT security & access security
- Managing / framing third party provider arrangements
- Destruction & de-identification patterns
- Data breach response & management plans



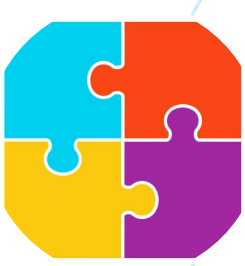
Anticipated reforms

(The Privacy Act Review Report)

- Reasonable steps for APP 11.1 to include technical & organisational measures (P 21.1)
- Specify 'baseline privacy outcomes' for APP 11, informed by the Government's 2023-2030 Australian Cyber Security Strategy (P21.2)
- OAIC guidance about the reasonable steps to secure information should draw on technical advice from the Australian Cyber Security Centre (P21.3)
- Take reasonable steps to protect de-identified information (P21.4) and more OAIC guidance about de-identification (P21.5)
- Review statutory requirements about retaining personal information. Weigh policy objective vs. privacy risks (P21.6)
- APP 11 to require entities to establish their maximum and minimum retention periods (P21.7) and refer to those periods in privacy policies (P21.8)

Information Law Mosaic

The Information Management Mosaic



- **Contract**
  - Client retainers
  - Panel contracts
- **Breach of Confidence & LPP**
  - Elements of confidence
  - LPP is not a right of action (*Glencore v Cmr of Taxation (2019)*)
- **Privacy Act**
  - TFN rules
  - APPs
  - Notifiable Data Breach Scheme
- **Professional Standards**
  - Legal Profession Act
  - Conduct Rules

Image: istockphoto

Data privacy & data security as a practicing solicitor

Professional obligations

Solicitor's Conduct Rules

- Rule 9, Confidentiality
  - i.e. don't disclose confidential information other than in permitted circumstances
  - Is there a 'disclosure' by the practitioner?
- Rule 30, Another Solicitor's or Other Person's Error
  - An error might involve or relate to information
- Rule 31, Inadvertent Disclosure
  - Is the disclosure inadvertent?

Professional obligations

Legal Profession Act 2006 (ACT)

- Unsatisfactory professional conduct

s386 What is unsatisfactory professional conduct?

unsatisfactory professional conduct includes conduct of an Australian legal practitioner happening in connection with the practice of law that falls short of the standard of competence and diligence that a member of the public is entitled to expect of a reasonably competent Australian legal practitioner.

Professional obligations

What do the industry regulators say?

- Failure to take appropriate steps to protect and impose proper cyber security practices includes a **risk of breaching your professional obligations** as a legal practitioner in South Australia (under the Australian Solicitors' Conduct Rules).
  The Importance of Cyber Security for Practitioners and Legal Practice, The Law Society of South Australia

- Where a cyber attack results in confidential client information being stolen there are different possible outcomes. For example, the use of the confidential information may result in the client suffering a loss. If the client claims that loss from the firm the policy will cover that claim. Or, the client may make a **misconduct complaint** to the Victorian Legal Services Board and Commissioner **for allowing the confidential information to be disclosed**. When you protect your client's information, you protect yourself and your practice.
  Cybersecurity FAQs, The Law Institute of Victoria

Melbourne | Sydney | Brisbane | Canberra | Perth

Professional obligations

What do industry regulators say (contd.)?

- Under the Rules practitioners have a fundamental ethical obligation to deliver legal services competently and diligently. Relevant aspects of that obligation are:
  - Maintaining effective control of data stored on cloud computing services.
  - Ensuring adequate reliability of applications and access to data.
  - **Ensuring adequate security of data**.

  Ethical and Practice Guidelines, The Law Society of Western Australia, 2019 (p48).

- All legal practitioners in NSW have a **duty not to disclose any information that is confidential** to a client unless otherwise permitted by the Legal Profession Uniform Law Australian Solicitors' Conduct Rules (the Conduct Rules).

  Data and Cyber Security for Law Practices, Fact Sheet, The Law Society of New South Wales

- See *'The (Cyber) Threat is Real'*, Law Society of the ACT, Ethos, Issue 261, Spring 2021 (among other guidance).

When things go wrong …

Professional Standards Compliant vs. Privacy Compliant

Threshold Issues

- Can you resolve the complaint and/or mitigate the risks?
- Is the complaint conflating privacy & professional standards?
- Rule 43 – duty to be open and frank in dealings with the regulatory authority
- Dealing with more than one regulator

Privacy Complaints

- Free and informal privacy complaints process
- A person must complain to the APP entity first, then to OAIC
- If OAIC investigates, outcomes might include:
  - apology;
  - compensation for financial and non-financial loss
  - 'novel' non-financial settlements
  - the entity training its staff or changing practices & procedures.
- Enforceable undertakings
- Compensation (Cmr Determination)

How is a data breach different?

- Data breaches
  - sub-set of cyber incidents
  - **unauthorised access or disclosure, or loss** of, personal information (incl tax file numbers)
- Some data breaches must be notified
  - Part IIIC of Privacy Act (**NDB Scheme**)
  - compliance can be enforced by OAIC

What is the NDB Scheme?

- **Part IIIC** of Privacy Act 1988 (Cth)
  - mandatory notification of "***eligible data breaches***"
- **Likely** result in "***serious***" harm to individuals
  - factors to consider seriousness, not defined
  - harm can be **physical, financial, reputational, emotional**
- Must have reasonable grounds to "***believe***"
  - notify **as soon as practicable**
  - if only "***suspect***" – expeditious assessment (**30 days**)

What and who do I notify?

- Notify **as soon as practicable**
  - Office of the Australian Information Commissioner (**OAIC**)
  - **directly** – individuals harmed, individuals info relates
  - **publicly** – if necessary, publish on website, social media
- **Notification statement**
  - identity and contact details of organisation
  - description of data breach
  - **kinds of personal information** involved
  - **recommended steps** to avoid potential harm

How is a data breach managed in real life?

- **Crisis management situation**
  - urgent response, but not panic
  - good communication is key!!!
  - defined tasks and timelines
  - make smart informed decisions, not rushed

- **Incident response team** working together
  - **Lawyer** (breach coach), Insurer
  - **IT Forensics** (investigation, ransom negotiation)
  - Crisis Management/PR, Data Review (e.discovery)
  - ID Theft/Credit Monitoring, Call Centre (notification)
  - Forensic Accounting (loss quantification/business interruption)

Why should I comply?

- **OAIC's powers** to enforce compliance
  - investigations (own, referral or complaint)
  - determinations (specified steps to take)
  - Federal Court **civil penalty orders**
    - incl for **serious or repeated interference with privacy** (s 13G)
    - $2.5M for individuals
    - $50M, 3 x value of benefit, 30% turnover for corporates
  - failing to comply with NDB Scheme = interference with privacy
  - enforceable undertakings (address issues)
  - injunctions (stop activities)
  - directions (prepare statement, notify)

Why should I comply?

- **OAIC's new powers** to enforce compliance
  - if reason to believe entity has information regarding **actual or suspected data breach**
    - issue notice requiring **production of documents or answer questions**
    - any entity that can assist
  - failure to comply → infringement notice
    - **civil penalty** ($13,320 individuals, $66,600 corporates)
  - multiple contraventions → **criminal offence**
    - penalty ($13,320 individuals, $66,600 corporates)
  - investigate **ability to comply** with NDB Scheme
  - extension of **extra-territorial reach** of Privacy Act

What is an incident response plan?

- **Thing you grab** when you suffer a cyber incident!
  - may become mandatory, arguably is now
- Not complicated, **clear, effective** document
  - only contains the essentials you need to know in crisis
  - how the cyber event is **escalated and then managed**
- **Contact details** of key personnel and stakeholders
  - **one page** document is best
  - IR members, core team, decision makers only
- **Print it out!**
  - assume no access to computer or mobile

Why are the recent data breaches a big deal?

- **"Wake up call"** for Australia
  - front page news, still is
  - Government and community **expectations regarding privacy** has rapidly increased
- Triggered **significant reform** in privacy/cyber space
  - new max. penalties, expanded powers of OAIC
  - **Privacy Act Review Report** proposals
  - other **Federal Government** actions
- **New litigious environment**
  - multiple **class actions** commenced
  - potential new **direct right of action**

Privacy/cyber reform

- *Privacy Legislation Amendment (Enforcement and Other Measures) Act* 2022 (Cth)
  - amended *Privacy Act,* commenced **13 December 2022**
  - only addressed **"*most-pressing issues*"**
- **Privacy Act Review Report** released by A-G
  - 110 proposals (30 categories), open until **31 March 2023**
  - removal of **small business exemption** (<$3M revenue)
  - **direct right of action** for interference with privacy
  - **statutory tort** for serious invasion of privacy
  - **notification** of eligible data breaches **within 72 hours**
  - require reasonable **data breach practices and procedures**
  - **tiers of civil penalty** provisions (new low, mid tier)

Other Government action

- **New Expert Advisory Board**
  - develop **new Australian Cyber Security Strategy 2023-2030**
- **New International Counter Ransomware Task Force**
  - drive international cooperation to combat ransomware
- **New National Office for Cyber Security (Dept of Home Affairs)**
  - supports new Coordinator for Cyber Security
- **Discussion paper** released by Expert Advisory Board
  - series of questions, open until **15 April 2023**
  - **core policy areas**
    - harmonising regulatory frameworks, strengthening international strategy on cybersecurity, securing government systems
  - areas for **potential action**
    - incl supporting cybersecurity workforce, national response to cyber incidents

Data breach class actions & cyber litigation

- **Optus/Medibank** changed the environment
  - Plaintiff firms were previously hesitant, no direct right of action through courts
  - OAIC awards very small (up to approx. $20,000)
  - Needed ‘perfect large data breach’ to run test case
- **Medibank class actions**
  - Representative complaint (Maurice Blackburn, Bannister Law, Centennial Lawyers)
  - Federal Court class action (Baker McKenzie, funded by Omni Bridgeway)
- OAIC’s own investigations
  - Optus and Medibank
- **Other litigation** will follow
  - Courts will get comfortable with cyber area over time (ASIC v RI Advice)
  - If direct right of action introduced into Privacy Act – game changer!

Cyber insurance

- Has a **bad reputation**
  - what does it actually cover?
  - isn't PI insurance enough?
- Cyber insurance is a **unique product specially designed** to help you through a cyber event
  - from the moment you discover a cyber incident
  - through the event and any third party claims
  - to when it is over and you have counted your business losses

Cyber insurance

- **First party cover**
  - **Incident response** costs (legal, forensics, PR, credit monitoring, data review)
  - **Business interruption** loss (forensic accounting)
  - Data asset recovery costs (lost data or software)
  - 'Bricking' and betterment costs (physical equipment damage)
  - Extortion costs (ransom demands, negotiation costs)
  - **Social engineering fraud** loss (monies transferred)
- **Third party cover**
  - **Liability claims** arising from data breach (incl defence costs)
  - **Regulatory fines and penalties** (if insurable at law) (incl defence costs)
  - Network security and multimedia related liability claims

Melbourne | Sydney | Brisbane | Canberra | Perth

Your cyber cover

- **LPLC**
  - Contract for Professional Indemnity Insurance for Solicitors (with defence costs exclusive/inclusive excess) 2022/2023
  - https://lplc.com.au/insurance/solicitors/solicitor-policies
- **Lawcover**
  - Tokio Marine Kiln/Lawcover LST Cyber Risk Policy
  - https://www.lawcover.com.au/about-cyber-risk-insurance/

Your cyber cover

- **LPLC**
  - **PII Policy** for Solicitors (not Cyber Policy)
  - only provides **third party cover** (civil liability, defence costs)
  - **claim made** in connection with the Firm's legal practice
  - cl 7(c) effectively provides that:
    - claim can arise from any "***cyber act***" and/or "***data breach***"
    - cyber act is unauthorised, malicious or criminal act involving any computer system
    - data breach is unauthorised acquisition, use, or disclosure of confidential or personal information involving any computer system
    - claim is a demand for compensation in connection with the Firm's legal practice
  - 19.15 **excludes** civil penalties and fines
  - **Sum Insured** is **$2,000,000**

Melbourne | Sydney | Brisbane | Canberra | Perth

Your cyber cover

- **Lawcover**
  - **Cyber Risk Policy** sits adjacent to PII Policy (no added cost)
    - Group policy purchased by Lawcover from **Tokio Marine Kiln** (London)
    - described as "*foundational cyber risk insurance*"
    - Law practices are encouraged to consider whether it is sufficient
  - **first party cover**
    - Cyber Costs and Expenses, Crisis Management Costs, Customer Notification Expenses, Cyber Extortion Monies, Loss of Business Income
  - **third party cover**
    - Cyber Liability, Regulatory Defence Costs and Penalties
  - **excludes** liability arising from Professional Services, except Claim alleging Breach of Privacy
  - **Limit** of indemnity is **$50,000** (any one claim, in aggregate)
  - **Excess** is determined by fee income (**$0-$25,000**)
  - **Notification** condition requires contacting CBP

Where do I start?

- **C.H.E.C.K.** your cyber risk and insurance position
  - **Challenge** your cybersecurity through penetration testing
  - **Have** an incident response plan and test it
  - **Evaluate** your cyber resilience against ASIC's expectations
  - **Contact** your cyber insurer or broker
  - **Know** your team that will face the crisis

- Where to start?
  - A **simulation exercise** with team and experts
  - Arrange **penetration testing** of cybersecurity

Do you use strong passwords?

How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

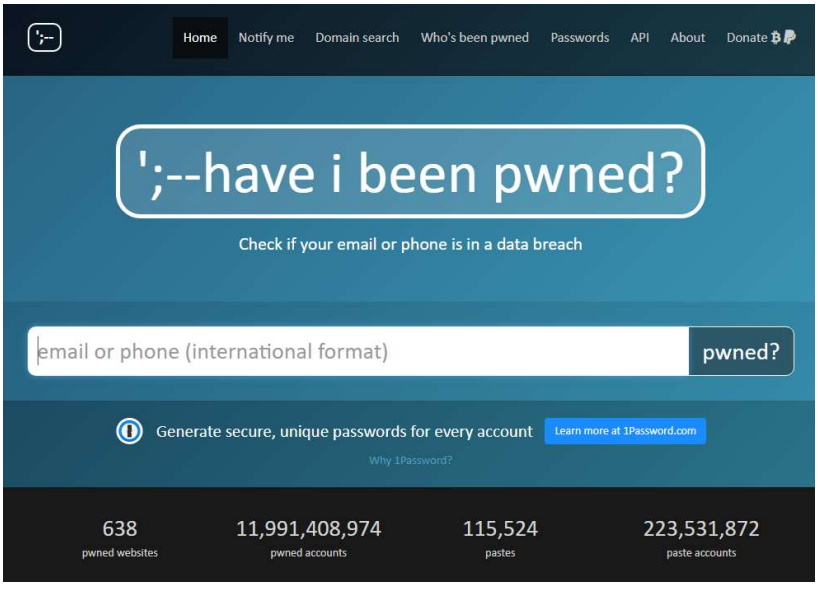
Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

statista

Melbourne | Sydney | Brisbane | Canberra | Perth

Have you been compromised?



Melbourne | Sydney | Brisbane | Canberra | Perth

Questions?

Sources / References

Legislation

- *Privacy Act 1988* (Cth)
- *Information Privacy Act 2014* (ACT)
- *Legal Professional Act 2006* (ACT)

Guidelines

- OAIC, APP Guidelines
  https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines
- OAIC, Guide to securing personal information:
  https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information
- Australian Government Information Security Manual (ISM):
  https://www.cyber.gov.au/acsc/view-all-content/ism
- Protective Security Policy Framework (PSPF)
  https://www.protectivesecurity.gov.au/about

Sources / References

Other Resources

- The Importance of Cyber Security for Practitioners and Legal Practice, The Law Society of South Australia: https://www.lawsocietysa.asn.au/Public/Publications/Resources/CyberSecurity.aspx (Accessed 26/2/23)
- Cybersecurity FAQs, The Law Institute of Victoria: https://www.liv.asn.au/Web/Resource_Knowledge_Centre/Practice_Support_Resources/Cybersecurity/Web/Content/Resource_Knowledge_Centre/Practice_Support_Resources/Cyber-security/Cyber-Security.aspx?hkey=aeb5005f-7366-4f5c-bea1-a4df9de014eb (Accessed 26/2/23)
- Ethical and Practice Guidelines, The Law Society of Western Australia, 2019 (p48): https://www.lawsocietywa.asn.au/wp-content/uploads/1970/01/ethical-practice-guidelines-25-august-2015.pdf (Accessed 26/2/23)
- Data and Cyber Security for Law Practices, Fact Sheet, The Law Society of New South Wales https://www.lawsociety.com.au/sites/default/files/2022-12/LS3808_PSD_DataBreach_2022-12-8a.pdf (Accessed 26/2/23)
- *'The (Cyber) Threat is Real'*, Law Society of the ACT, Ethos, Issue 261, Spring 2021. https://issuu.com/act.law.society/docs/ethos_261_spring_2021_print/56?fr=sMTVhNTQzNDI1OTU (Accessed 26/2/23)

Professional obligations

Legal Profession (Solicitors) Conduct Rules 2015 (ACT)

Rule 9 - Confidentiality

9.1 ***A solicitor must not disclose*** any information which is confidential to a client and acquired by the solicitor during the client's engagement to any person who is not:

- 9.1.1 a solicitor who is a partner, principal, director, or employee of the solicitor's law practice; or
- 9.1.2 a barrister or an employee of, or person otherwise engaged by, the solicitor's law practice or by an associated entity for the purposes of delivering or administering legal services in relation to the client,

9.2 A solicitor may disclose information which is confidential to a client if:

- 9.2.1 the client expressly or impliedly authorises disclosure;
- 9.2.2 the solicitor is permitted or is compelled by law to disclose;
- 9.2.3 the solicitor discloses the information in a confidential setting, for the sole purpose of obtaining advice in connection with the solicitor's legal or ethical obligations;
- 9.2.4 the solicitor discloses the information for the sole purpose of avoiding the probable commission of a serious criminal offence;
- 9.2.5 the solicitor discloses the information for the purpose of preventing imminent serious physical harm to the client or to another person; or
- 9.2.6 the information is disclosed to the insurer of the solicitor, law practice or associated entity.

Professional obligations

Legal Profession (Solicitors) Conduct Rules 2015 (ACT)

Rule 30 Another Solicitor's or Other Person's Error

30.1 A solicitor must not take unfair advantage of the obvious error of another solicitor or other person, if to do so would obtain for a client a benefit which has no supportable foundation in law or fact

Rule 31 Inadvertent Disclosure

A solicitor to whom material known or reasonably suspected to be confidential is disclosed by another solicitor, or by some other person and who is aware that the disclosure was inadvertent must not use the material and must:

31.1.1 return, destroy or delete the material (as appropriate) immediately upon becoming aware that disclosure was inadvertent; and

31.1.2 notify the other solicitor or the other person of the disclosure and the steps taken to prevent inappropriate misuse of the material.

MILLS OAKLEY

Melbourne

Level 6
530 Collins Street
Melbourne VIC 3000
T: +61 3 9670 9111
F: +61 3 9605 0933

Sydney

Level 7
151 Clarence Street
Sydney NSW 2000
T: +61 2 8289 5800
F: +61 2 9247 1315

Brisbane

Level 23
66 Eagle Street
Brisbane QLD 4000
T: +61 7 3228 0400
F: +61 7 3012 8777

Canberra

Level 1
121 Marcus Clarke Street
Canberra ACT 2601
T: +61 2 6196 5200
F: +61 2 6196 5298

Perth

Level 24
240 St Georges Terrace
Perth WA 6000
T: +61 8 6167 9800
F: +61 8 6167 9898

actlawsociety

the law society of the australian capital territory
a member of the law council of australia
ABN 60 181 327 029
02 6274 0300 | mail@actlawsociety.asn.au
www.actlawsociety.asn.au