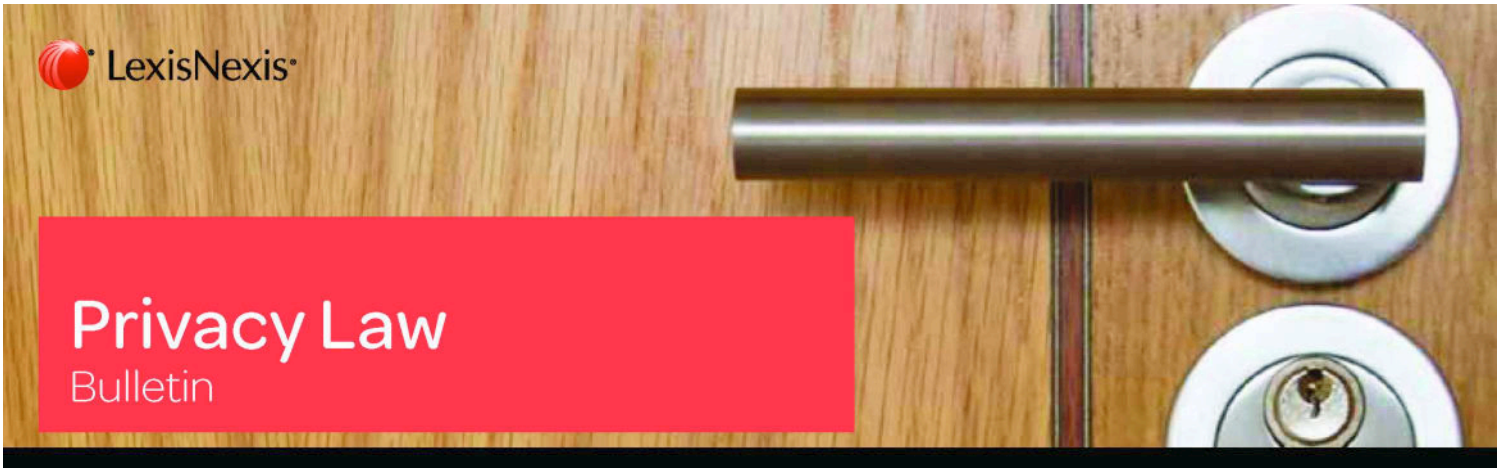

Privacy Law Bulletin

2024 . Vol 20 No 10

Contents

Information contained in this newsletter is current as at February 2024

Privacy Law
Bulletin

Privacy obligations and the insolvency practitioner — Part 2

Deidre Missingham *and* ***Penelope Pengilley*** *KEYPOINT LAW*

This second of two articles considering privacy obligations in relation to ordinary sale or other disposal of a business examines in detail the rights and obligations of the insolvency practitioner.

Key takeaway points for privacy lawyers in insolvency practice

- Insolvency firms and the entities they oversee may be subject to privacy obligations under the Privacy Act 1988 (Cth).
- Australian Privacy Principle (APP) entities, including insolvency practitioners' firms, must only collect personal information when reasonably necessary for their functions or activities.
- When insolvency practitioners' activities are authorised by legislation like the Corporations Act 2001 (Cth) (CA), the disclosure of personal information is permitted under the "required or authorised by or under law" exception to APP 6.
- The scope of disclosure under the APP 6 exception must be limited to what is necessary.
- Privacy considerations in insolvency practice involve additional mechanisms and factors.

Introduction

The first of our two articles considering privacy obligations in relation to sale or other disposal of a business by an insolvency practitioner, considered what personal information may be held by businesses and outlined privacy watchpoints in relation to an ordinary sale. We then asked the following:

- Do insolvency practitioners face different privacy hazards from those of the ordinary business buyer of a company?
- What are the pitfalls?

before introducing particular privacy hazards for insolvency practitioners and examining how the Australian Restructuring Insolvency & Turnaround Association (ARITA) Code of Ethics[1] and Inspector-General Practice Guideline 2 address protection and use of information. However, our main focus is corporate insolvency.

Many of the actions and practices of insolvency practitioners who are APP entities would constitute interferences with the privacy of individuals under the APPs were it not for the CA legislation whereby the exception under APP 6.2 is engaged; that is, use or disclosure of personal information about an individual is permitted if "(b) the use or disclosure of the personal information is required or authorised by or under an Australian law or a court/tribunal order."

We now examine insolvency practitioners' work in depth through a privacy lens. First, we consider the range of roles within insolvency practice and their legislated powers in relation to information, then what information access rights creditors have and issues associated with information obtained by means of coercive powers.

Finally, we list some privacy hazards for the assistance of insolvency practitioners.

As an Appendix, we consider two privacy determinations in the insolvency context.

What data do insolvency practitioners collect and disclose?

Under Sch 2 of the CA (the Insolvency Practice Schedule (Corporations)), only a registered liquidator can perform certain roles, such as that of the receiver of the property of a corporation, the administrator of a company or of a deed of company arrangement, the restructuring practitioner for a company or for a restructuring plan, or the liquidator of a company. The specific role the insolvency practitioner is performing in an engagement will determine what legislated powers it has in relation to the distressed company and its information holdings.

Receivers

The CA provides receivers with extensive powers. Depending on the terms of their instrument of appointment and the extent of the property they are appointed

over, receivers may:

- carry on the business of the company (s 420(2)(h)) and then subject to approvals, during a winding up (s 420C(1))
- dispose of property of the company (s 420(2)(b)) and convert property of the company into money (s 420(2)(g))
- engage or discharge employees of the company (s 420(2)(o))
- where the security interest respecting which the receiver was appointed includes security over uncalled share capital, make a call for that capital (s 420(2)(s)) and enforce payment (s 420(2)(t)) and
- bring or defend proceedings on behalf of the company (s 420(2)(k)) and where a debt or liability is owed to the company, make a claim for that debt in a bankruptcy, liquidation or winding up (s 420(2)(r))

These activities all require the receiver to have access to and deal with the subject company's collection of personal information. For this reason, receivers are given power to inspect the books of the company[2] that relate to the subject property that they are appointed over, at any reasonable time (s 431 of the CA).

Voluntary administrators

The appointment of a voluntary administrator marks the ceding of control of the subject company's affairs. During the administration, the administrator has power under the CA to:

- control and carry on the company's business, property and affairs (s 437A(1)(a) and (b)) and
- may terminate or dispose of all or part of that business and dispose of any or all of that property (s 437A(1)(c))

Further, as soon as practicable after commencement, administrators are required under the CA to investigate the company's business, property, affairs and financial circumstances to enable them to advise the creditors. This advice addresses whether it would be in the creditors' interests for the company to execute a deed of company arrangement, for the administration to end or for the company to go into liquidation (s 438A). These matters must be considered by creditors at a so-called "second creditors' meeting", called pursuant to s 439A.

To enable administrators to carry out these functions, as soon as practicable after commencement, each director must deliver to the administrator all books in that director's possession (s 438A(1)) and within 5 business days after commencement, provide the administrator with a report as to the affairs of the company (s 438B(2)). Failure to provide access is an offence (s 438B(4) and (5)). In addition, the CA gives administrators rights to the books as against third parties (s 438C).

Further, for the second creditors' meeting, the Insolvency Practice (IP) Rules[3] 75-225 require that the creditors be provided with a report as to the company's business, property, affairs and financial circumstances and contain the administrator's recommendations regarding the future of the company. Reports to creditors generally include creditor lists, because these are material to a company's financial circumstances and therefore likely return to creditors and to voting at the meeting if a poll is called (IP Rules 75-115).

However, although creditors as a body or individually can seek further information about the company's affairs from an administrator, access may be denied where requests are unreasonable (see further below under "What information access rights does a creditor have?")

In addition, material debts owed to the company may also be separately listed. This list may contain personal information where debtors are individuals. Unless individuals were officers of the company, any listing would probably be limited to name and amount of debt or indebtedness. However, in the case of company officers, the nature and extent of information provided will depend on whether any breaches of duty have been identified, and if so, whether there could be claims, and then, prospects of recovery should a claim be made, and that information may include references to personal assets. It could also include information about the transfer of assets to family members, if such transfers could be overturned, another layer of personal information.

Deed administrators

Insolvency practitioners often become deed administrators as a follow on from their appointment as voluntary administrator, in which case they already have access to extensive information including personal information.

Further, because they are responsible for administering and therefore making payments pursuant to any deed of company arrangement, deed administrators must maintain creditor lists. In addition, where the transfer of shares is contemplated by the deed pursuant to s 444GA (which permits a deed administrator to transfer shares with the consent of the shareholder or by leave of the court), it will be necessary for the deed administrator to access the company's share register.

Liquidators

Under the CA, liquidators, like administrators, may carry on the business of a company (s 477(1)(a)) and sell

or otherwise dispose of all or any part of the property of the company (s 477(2)(c)). They are also entitled to inspect the books of the company at any reasonable time (s 447(3)), with refusal an offence.

If there is a prospect of paying a dividend in the liquidation, they too may be required to settle creditor lists. Of course, liquidators are obliged to get in the assets of the company, including any outstanding debts, respecting which personal information may be held.

Further, liquidators are required to settle a list of contributories where the share capital is not fully paid, and contribution is required to meet liabilities in the winding up or where there will be a surplus available for distribution or there is a need to adjust rights as between contributories (s 478).

Liquidators and other external controllers of companies also have powers to summons people for examination regarding the company's affairs. These powers are discussed below.

Other external appointments

The CA also recognises other external appointments such as restructuring practitioners (s 453B) and empowers restructuring practitioners to access company books (s 453F(1)(c) and s 453G).

What information access rights does a creditor have?

The CA gives creditors rights to inspect the books kept by external administrators at all reasonable times (Sch 2 70-10).

Further, creditors can request information or a document by resolution (Sch 2 70-40(1)). However, the external administrator may refuse if:

- the information is not relevant to the external administration (Sch 2 70-40(2)(a)) — which may well be the case with personal information or
- it would be a breach of duty to comply (Sch 2 70-40(2)(b)) or
- it would otherwise be unreasonable (Sch 2 70-40(2)(c))

Unreasonableness is dealt with in the Insolvency Practice Rules Div 70 — Information. So, it may be unreasonable to comply with a creditor's request where:

- the information could prejudice another creditor (IP Rules 70-10(2)(a))
- disclosure could found an action in breach of confidence (IP Rules 70-1(2)(c)) or
- the request is vexatious (IP Rules 70-10(2)(g))

Individual creditors can request information or a document (Sch 2 70-45(1)) with the same bases for refusal as for requests by creditor resolution (Sch 2 70-45(2)).

Practitioners' coercive powers and information access

Liquidators' examinations

The external administration provisions of the CA are intended to assist in the administration of the affairs of distressed companies where assets available to creditors may be:

- non-existent
- limited proportionate to claims or
- dependent on successful claims brought against directors, officers, preferred creditors and other persons with involvement in or, in some cases, knowledge of challengeable activities

Sometimes liquidators cannot gain a complete picture of a company's affairs from its books, so they and other external controllers of companies are empowered to summons people for examination regarding the company's affairs. Examinations are conducted before officers of the court and are open to the public. Creditors or officers of the company can inspect transcripts without fee, although anyone else must pay (s 597(14A)).

Directors and officers may be summoned as of right. Others may be summoned with leave of the court where the court is satisfied the proposed examinee took part or was concerned in examinable affairs of the company and had been or may be guilty of misconduct respecting the company, or may be able to give information about the examinable affairs of the company (s 596B). Persons summoned for examination may also be required to produce documents that may be in their possession that relate to the company or any of its examinable affairs (s 596D(2)).

Compelling attendance at an examination is an exercise of the coercive power of the state and examinees cannot avoid answering questions on the basis of tendency to incriminate (s 597(12)).[4] However, if at the time of answering the examinee states that the answer may incriminate, then the answer cannot later be used against the examinee in a criminal or penalty proceeding, save respecting a proceeding for perjury in the examination (s 597(12A)). Therefore, the power to compel attendance and provision of information is a powerful tool in the hands of liquidators.

The courts have acknowledged the tension between the importance of gathering information for the purposes of a winding up and the inconvenience and intrusion into the privacy of an examinee — especially an examinee who is not a director or officer of the company. This is the reason why leave to examine must be given. In striking this balance, the court has said:

> [T]he exercise of the power can involve tension between two important public interests. The first is the public interest[5] in a liquidator obtaining necessary information to

> properly discharge the function of liquidator in the winding up of the company for the benefit of the creditors. The second is the right of the individual to privacy in regard to his or her affairs, documents and papers.
> . . .
> The relevant test as to the sufficiency of the relationship between the person against whom the examination was sought and the affairs of the company in liquidation was whether, in the opinion of the court, that person was, or may be, able to give information relevant to increasing or protecting the assets available in the winding up.[6]

The cases make it clear that examinable affairs can extend to the existence of insurance policies and assets held by an examinee — personal information — as these matters go to whether the examinee can satisfy a judgment should proceedings be brought.[7] Accordingly, there is a real likelihood that the personal information of examinees may be made available to the public.

Nevertheless, courts may exercise a protective discretion in relation to individuals' privacy in that they have power to give directions regarding the examination process, including respecting:

- whether, by reason of special circumstances, parts should be in private (s 597(4)) and if so, who may be present (s 596F(1))
- that someone may be excluded even if the examination is conducted in public (s 596F(1)(d))
- access to records of the examination (s 596F(1)(e))
- the publication or communication of information about the examination including questions asked and answers given (s 596F(1)(f))
- the destruction of documents that relate to and were created at the examination (s 496F(1)(g))

Orders for private examinations are not lightly made, given the purposes of liquidators' examinations. Adverse publicity alone is not considered a "special circumstance". The prejudice suffered through publication must outweigh the publicity contemplated by the legislation.[8] However, a pending criminal prosecution may justify a private examination in light of the potential to expose lines of defence and also, if there is publicity, to affect potential jurors.[9]

We note that where insolvency issues are dealt with by the Federal and Supreme Courts in their oversight jurisdiction, these courts and practitioners before them generally follow practices that minimise exposure of third-party personal information where that information is not material to the facts and matters supporting the reasons for judgment.

So, for example, in making orders adjusting or declaring rights as between parties, and the assessment of amounts, the subject of such orders, which are based or rely upon other individuals' personal information, affidavits or other documents disclosing that information to the court can be ordered to be treated as confidential. This means they will be inaccessible on the court file saved for further court order or if information has to be disclosed as a necessary part of the order, identifying numbers or initials only may be used, with identifying lists kept confidential.

Use of documents obtained via the exercise of coercive powers

In our first article, we cited cl 5.17 of the ARITA Code of Ethics and the limitations it imposes on use of information obtained during the course of an insolvency appointment.

In addition, we noted that where documents or information are obtained in a court process then the *Harman v Home Department State Security*[10] (*Harman*) undertaking will arise. The *Harman* undertaking protects the interests of parties who are required by the coercive power of the courts to disclose their confidential and personal information. It has been described by the High Court as follows:

> Where one party to litigation is compelled, either by reason of a rule of court, or by reason of a specific order of the court, or otherwise, to disclose documents or information, the party obtaining the disclosure cannot, without the leave of the court, use it for any purpose other than that for which it was given unless it is received into evidence.[11]

Breach of the *Harman* undertaking is a contempt of court, so in cases of doubt, prudence dictates that insolvency practitioners will seek leave of the court to use the information or documents.[12] This is because the undertaking can be released only by a court.

The courts have made it clear that liquidators are not excused from the reach of the *Harman* undertaking, however documents produced to the court in response to a liquidator's summons are produced for the purposes of the liquidation so using them in the liquidation is not a breach of the undertaking.[13] More difficult questions arise where litigation funding may be in prospect or consideration is being given to assigning a company's claims.[14]

Further, cl 5.17 of the Code would apply to all documents obtained via the coercive power granted by the CA.

Privacy hazards for insolvency practitioners

Our brief review shows that privacy issues arise in a variety of contexts in insolvency administration, with obligations upon insolvency practitioners not limited to the CA. Accordingly, in our view insolvency practitioners could benefit if a single source designed to assist them to navigate between their legislated information-handling powers and responsibilities and the principles

of privacy best practice were available. Such a compilation and summary would touch upon not only general privacy issues and how they pertain to insolvency, but also factors specific to individual appointments and the order in which privacy issues may arise, as follows:

- whether their firms or the entities they are appointed over are subject to the Privacy Act. That will enable them to determine the scope of their obligations under privacy legislation
- how their powers and obligations under the CA interact with their privacy obligations
- whether the entity they are appointed over is subject to other privacy, confidentiality or information management obligations by reason of the nature of its business for example, in the legal or health sectors
- upon appointment, whether the information could be or has been subject to cyber compromise or other data breach and what cyber risk minimisation steps should be followed
- where a business or business assets may be sold, how privacy issues should be managed during the sale process
- whether by reason of previous or current litigation, the entity holds materials subject to the *Harman* undertaking and if so, whether leave to use the information should be sought
- in discharging their reporting obligations, how they balance privacy concerns with creditor entitlement to information regarding the affairs of the company both respecting the content of their reports and accessibility (for example, ensuring online access is password protected or similar)
- where creditors seek access to the company's books and records, whether any issues arise that could create an exception to the general statutory right of access or whether a special confidentiality regime should be put in place
- where personal information has to be disclosed in any court documents, whether individuals can be deidentified with names and other details protected by confidentiality orders
- where information has been obtained via a liquidator summons or similar, what information management practices should be adopted during the administration given the impact of the *Harman* undertaking, whether leave to use the information may need to be sought in particular cases and then how the information should be dealt with once the appointment has been concluded

Conclusion

The Office of the Australian Information Commissioner (OAIC)'s 2023 Australian Community Attitude to Privacy Survey (ACAPS)[15] found that 3 in 5 (62%) Australians see the protection of their personal information as a major concern in their life. Commissioner Angelene Falk noted in her foreword that recent events and factors such as high-profile data breaches and the speed of tech innovation have intensified individuals' focus on privacy in relation to their sense of control and autonomy, human dignity and other key values.

Insolvency administrators wanting to meet their compliance obligations and play their part in building trust in today's business environment should not forget the OAIC's top three recommended actions to protect personal information:

- Only collect it when it's necessary.
- Take proactive steps to protect it.
- Delete it when it's no longer needed.

Appendix

Privacy determinations in the insolvency context

On two occasions, both now historic, a Privacy Commissioner has made determinations on issues relating to insolvency, and both cases contain some useful learnings.

Complainant J v Statutory Entity[16] concerned the production of documents upon service of a s 530B notice, which compels production of the company's books to the liquidator. The notice had been served upon a statutory entity that licensed certain trade activities. The complainant had a legal dispute with the company and had sent numerous unsolicited letters to the statutory entity regarding the company's conduct. A close associate of the company director had also sent unsolicited letters to the statutory entity about the company, the complainant and several other customers of the company.

Given the "delicate nature of the letters", the statutory entity sought clarification from the liquidator as to whether the notice extended to the unsolicited correspondence and was advised that it did. The statutory entity then sought and obtained written undertakings of confidentiality, limitation of use and return of the documents before providing the documents.

The complainant was also in discussions with the liquidator and became aware that the liquidator had received the correspondence that contained damaging assertions about him and complained first to the statutory entity and then to the Victorian Privacy Commissioner.

The Privacy Commissioner determined that the matter would turn on the ambit of s 530B and whether

"company books" meant books belonging to the company and not merely documents relating to it and concluded that that would be a matter for Victorian Civil and Administrative Tribunal (VCAT) if the matter was not conciliated. Conciliation was successful.

This determination raises an interesting question as to whether VCAT has jurisdiction over a liquidator's powers under s 530B, however arguably if the correspondence was not within power, the liquidator would not be protected. That said, if the correspondence had been part of the company books, the liquidator may obtain access by some other means.

The determination also illustrated the point that liquidators must take care with how they use documents obtained through the coercive powers given under the CA, especially where due to their "delicate nature" they may contain defamatory material.

In this instance, the interests of both the complainant and the other correspondent to the statutory entity may need protection. Contrast the putting of potentially damaging and possibly defamatory correspondence to an examinee in the course of a liquidator's examinations where the proceeding is under court supervision and directions regarding confidentiality can be made. It is another to do it privately in interviews not overseen by the court. Further, without proper protections in place, the liquidator could also be liable for damages in defamation through republication.

Own Motion Investigation v Bankruptcy Trustee Firm[17] concerned information about a bankrupt estate published on the bankruptcy trustee's firm website. The information included financial details and the firm's opinion as to whether certain persons had breached the requirements of the Bankruptcy Act 1966 (Cth).

The matter had been drawn to the Commonwealth Privacy Commissioner's attention by a member of the public and the Commissioner decided to conduct an "own motion" investigation. The firm argued that the trustee had obligations to lodge certain information to the Insolvency and Trustee Service of Australia that maintained the National Personal Insolvency index that was publicly available, and that some but not all of the information on the firm's website had been available there.

The Commissioner concluded that by allowing the information to be generally available on the internet, rather than placing limitations on access, the firm had interfered with the privacy of the bankrupt and had failed to comply with (then) National Privacy Principle 4.1 that requires an organisation to take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. Therefore, the Commissioner recommended password protection.

On-line reporting is now widely used by insolvency practitioners and the ARITA Code of Conduct provides that where websites are used to communicate with creditors, they should comply with privacy laws. Further, if appropriate, access should be restricted to those with an entitlement to access, say through password protections (6.12).

The Commissioner also recommended that the trustee's opinion on whether bankrupts had breached the Bankruptcy Act be removed from the file made available to creditors.

As to opinions on possible breaches of the law, unfortunately the reported findings do not provide insight into the Commissioner's understanding of the requirements of the Bankruptcy Act. Nevertheless, prudent insolvency practitioners will ensure that they do not exceed their reporting obligations.

General Editor's note

This article is the second instalment in a series of two, focusing on privacy obligations in the context of insolvency practice. The first article explored privacy concerns related to the ordinary sale or disposal of a business, while this second article delves into the specific rights and responsibilities of insolvency practitioners in managing personal information. Both articles consider the complexity of privacy issues faced by insolvency practitioners.

Deidre Missingham
Consulting Principal
Keypoint Law
deidre.missingham@keypointlaw.com.au
www.keypointlaw.com.au

Penelope Pengilley
Consulting Principal
Keypoint Law
penelope.pengilley@keypointlaw.com.au
www.keypointlaw.com.au

Footnotes

1. Collectively, an Introduction, the Code of Ethics, Code of Professional Practice: Insolvency Services (COPP: Insolvency Services) and Code of Professional Practice: Advisory Services (COPP: Advisory Services) form the ARITA Code. The ARITA Code is supported by Practice Statements which provide detailed explanations to support the ARITA Code but do not form part of the ARITA Code. Rather, the Practice Statements provide guidance to assist Members.

2. The meaning of "the books of the company" is considered in *Complainant J v Statutory Entity* [2004] VPrivCmr 4.
3. Made under s 105-1 of Sch 2 to the Corporations Act 2001 (Cth) (CA).
4. A related issue was recently the subject of *Re Deane, MSB Capital Holdings Pty Ltd (in liq)* [2023] FCA 919; BC202310960. It concerned a summons to produce books under s 596B of the CA. The examinee claimed privilege against exposure to penalty in respect of certain documents.
5. The courts have also recognised a secondary public interest element in examinations in that they assist in the regulation of companies by providing a public forum for the examination of examinable company officers: *Bazzo v Kirman* [2020] WASCA 43; BC202002646 at [54]–[64].
6. *Grosvenor Hill (Qld) Pty Ltd v Barber* (1994) 48 FCR 301; 120 ALR 262; 12 ACLC 176; BC9406580 at 269 and 308
7. Above; *Re McEachern, Gladstone Civil Pty Ltd v Pleash (Liquidator)* [2014] FCA 1364; BC201410658; *Tolric Pty Ltd v Taylor* [2015] FCA 1051; BC201509282 at [51]–[54].
8. *Friedrich v Herald and Weekly Times Ltd* [1990] VR 995 per Kaye, Fullagar and Ormiston JJ applied in *Re New Tel*, op cit at [91].
9. *Re Plutus Payroll Australia Pty Ltd (in liq) and Companies Listed in Sch 4 to Amended Originating Process* (2020) 143 ACSR 234; [2020] NSWSC 46; BC202000546 at [10]–[14] per Gleeson J.
10. *Harman v Home Department State Security* [1983] 1 AC 280.
11. *Hearne v Street* (2008) 235 CLR 125; 82 ALJR 1259; [2008] HCA 36; BC200806976 at [96] per Hayne, Heydon and Crennan JJ.
12. In *Re Southern Equities Corp Ltd (in liq); Bond and Caboche v England* (1997) 25 ACSR 394; BC9705389: the Full Court of the Supreme Court of South Australia said that the undertaking covered documents produced to the court in response to an examination summons. However, using the documents in the liquidation, including in any proceeding brought to get in the assets of the company, falls within the purpose for which the documents were sought (Lander J at 437, Cox and Bleby JJ agreeing) so no contempt arises.
13. Above.
14. See *Re LCM Operations Pty Ltd, 316 Group Pty Ltd (in liq)* [2021] FCA 324; BC202102384 where the assignee of a claim was given leave to use documents produced under compulsion.
15. See www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023.
16. Above n 2.
17. *Own Motion Investigation v Bankruptcy Trustee Firm* [2007] PrivCmrA 5.

Prompt action following a data breach is critical

Susan Kantor *and* ***Jaimie Wolbers*** *MINTERELLISON*

Two recent decisions of the Privacy Commissioner have emphasised the need for organisations to undertake an expeditious assessment of data breaches to determine whether an "eligible data breach" has occurred, and issue notices in a timely manner. These decisions reflect broader comments made by the Privacy Commissioner in the most recent half-yearly Notifiable Data Breach Report, as well as a general trend towards increased enforcement action for privacy breaches.

Determining an eligible data breach

Following a suspected data breach, organisations that are subject to Pt IIIC of the Privacy Act 1988 (Cth) are required to take a reasonable and expeditious assessment as to whether an eligible data breach has occurred.[1] Specifically, an organisation's assessment should consider whether:

- there has been unauthorised access to, or disclosure of, personal information (or loss of personal information that is likely to result in unauthorised access to, or disclosure of, personal information) and
- a reasonable person would conclude that the access or disclosure of such personal information would likely result in serious harm to any of the individuals to whom the information relates

Organisations are required to take all reasonable steps to ensure that their assessment is completed within 30 days of becoming aware of the incident.[2] However, given that a key purpose of the notifiable data breach scheme is to inform affected individuals of a data breach so that they can take measures to protect themselves and mitigate any harm that might arise, the 30 day timeframe should be considered the upper limit. If possible, organisations should complete this assessment much sooner.

Indeed, organisations could soon be required by law to complete their assessments within a much shorter timeframe. The proposed reforms to the Privacy Act, as outlined in the Attorney-General Department's *Privacy Act Review Report*,[3] proposed that the time for notifying the Privacy Commissioner of eligible data breaches should be significantly reduced to 72 hours from the time of becoming aware of an incident. The government has indicated that it 'agreed in principle' to this proposal in its *Government Response to the Privacy Act Review Report*.[4] If enacted, this change would align Australian privacy laws with other Australian regulatory incident reporting requirements (for example, under Australian Prudential Standard CPS 234) and global privacy notification regimes, such as under the General Data Protection Regulation (GDPR) in the EU and the UK, and significantly reduce the time for organisations to complete their assessment.

Recent decisions

In *Pacific Lutheran College (Privacy)*[5] an email account of the operator of an independent private school was compromised by an unauthorised access by an unidentified third party and used to send phishing emails to over 8000 email contacts. The compromised account included personal information of a number of individuals, including financial details, tax file numbers, identity information and contact information.

It was the ordinary practice of the user of the email account to collect the following types of information in the usual course of performing their role:

- information regarding parents and guardians, including birth certificate, credit card details, Medicare card details, Centrelink customer reference number
- information regard students, including name, address, date of birth and medical information
- information regarding staff, including tax file numbers

In *Datateks Pty Ltd (Privacy)*[6] (*Datateks*) Datateks (a company involved in building, operating and maintaining communications networks and infrastructure services) identified that three email accounts (including a general email account) had been subject to unauthorised access by a third party and used to carry out a phishing campaign. It was a routine practice at Datateks to hold personal information in email accounts, including individuals' date of birth, credit card information, bank

account details, superannuation information, driver's licence, birth certificate, working with children check, Medicare details and tax file numbers.

In both of these cases, the Privacy Commissioner held that at the time each entity became aware of the events (in both cases, within 24 hours of the unauthorised access), there was sufficient information for the entities to "reasonably suspect" that:

- there had been unauthorised access to personal information and
- unauthorised access to the types of personal information held in the email accounts would likely result in serious harm to the individuals to whom the information related. The types of harm identified by the Privacy Commissioner included serious financial harm, identity theft and fraud

Section 26WH of the Privacy Act provides that where an entity "has" reasonable grounds to "suspect" that there has been an eligible data breach, but the entity "does not have" reasonable grounds to believe that the circumstances amount to an eligible data breach, the entity must undertake a reasonable and expeditious assessment of the incident to establish whether they can form the requisite belief.

Critically, s 26WH(2)(b) states that the entity must take "all reasonable steps" to ensure the assessment is completed within 30 days of forming the suspicion (ie within 30 days of becoming aware of the incident). Once the entity has formed a reasonable belief that an eligible data breach has occurred, it must as soon as practicable, notify the Privacy Commissioner (by way of a statement that complies with the requirements of s 26WK(3)(d) of the Privacy Act). The Privacy Commissioner found that neither of these steps had been complied with in either of these matters.

In the *Pacific Lutheran College* matter, there was a delay in engaging solicitors and a forensic investigator — a lengthy period of time for the forensic investigator to complete their assessment of the incident (which initially focussed on the technical nature of the breach, not whether personal information was affected and the likely risk of serious harm to the individuals) — and a further delay, after a reasonable belief had been formed, in notifying the Privacy Commissioner. In total, 200 days elapsed between the college first becoming aware of the incident and lodging the required notice with the Privacy Commissioner.

In the *Datateks* matter, there were also delays in engaging cybersecurity experts to undertake an investigation — a failure of the preliminary investigation to identify what personal information had been compromised and the risk of serious harm to individuals — and a further delay once a reasonable belief in making the required notification to the Privacy Commissioner. In total, 206 days elapsed between Datateks becoming aware of the incident and lodging the required notice with the Privacy Commissioner.

In both matters, the Privacy Commissioner determined the respondents had:

- failed to conduct an assessment of the incidents in an expeditious manner and to take all reasonable steps to complete the assessment within 30 days, in breach of s 26WH(2) and
- failed to notify the Privacy Commissioner as soon as reasonably practicable that an eligible data breach had occurred, in breach of s 26WK(2)

and made declarations under s 52 of the Privacy Act, that, amongst other things, require Pacific Lutheran and Datateks to engage in specific steps to ensure that the same conduct is not repeated or continued in the future.

Notably, the Privacy Commissioner also made declarations requiring both Pacific Lutheran College and Datateks to develop privacy data breach response plans (specifying the matters to be included in the plans), as well as a range of improvements to their existing IT security arrangements, to ensure compliance with Australian Privacy Principle 11 (relating to the security of personal information).

In line with guidance issued by the Office of the Australian Information Commissioner (OAIC), the Privacy Commissioner required the data breach response plans to include a minimum range of matters. These requirements serve as a useful guide to other organisations who are preparing or reviewing their own data breach response plans. The matters include the following:

- a clear explanation of what constitutes a data breach
- an overview of the roles and responsibilities of personnel when there is a data breach, or suspected data breach
- clear guidance as to the respondent's capacity to investigate a suspected data breach, and the circumstances in which an external provider would need to be engaged to conduct an investigation
- details of the respondent's insurance coverage, including the extent of the coverage and the contact details of the insurer
- a process for engaging an external provider to investigate a suspected data breach where necessary, including details of the information that should be given to the provider, such as deadlines and guidance as to the level of analysis the respondent will require

- clear advice about the need for an investigation to be conducted expeditiously, and for all reasonable steps to be taken to conclude an investigation within 30 days
- a communication strategy that allows for notification of data breaches, where required by the Privacy Act and within the time limits required by the Privacy Act, to affected individuals and other relevant entities

A robust approach to investigating data breaches

The decisions discussed above reflect the views expressed by the Privacy Commissioner in her most recent half-yearly report on notifiable data breaches regarding delays in reporting breaches. According to the Privacy Commissioner:

> The NDB Scheme is now a mature model and the OAIC expects entities to have strong practices in place to protect personal information. Entities are also expected to have processes to ensure a timely response and compliance with the requirements of the scheme should a data breach occur.[7]

In the previous half-yearly Notifiable Data Breach Report for breaches notified in the period July to December 2022, the Privacy Commissioner acknowledged that organisations may not have all facts to hand at the time of suspecting that an eligible data breach has occurred. However, given the objective of notifying individuals of a data breach in a timely manner, this should not be considered a reason for delaying in issuing notifications. According to the Commissioner, where an eligible data breach is unfolding, organisations may wish to consider:

- Including in their data breach response plan a strategy for when and how to communicate information about data breaches to individuals. This can assist with making decisions on notification when an incident occurs.
- When notifying individuals directly as well as providing information on their website, seeking to ensure consistent information is provided and updates are communicated clearly.
- Where an entity is unable to complete its assessment promptly and within 30 days, and there are grounds to suspect an eligible data breach may have occurred, consider erring on the side of caution and notifying affected individuals and the OAIC.[8]

Further, while there may be delays in a forensic investigation identifying precisely what data might have been access or compromised by malicious threat actors, in recent half-yearly reports, the Commissioner has advised that organisations that suffer a cyber incident should assume a data breach has occurred, even if it is not possible to conclusively determine from forensic investigations whether personal information has been accessed or exfiltrated.

Enforcement trends

These recent decisions are also reflective of broader enforcement action being taken by the Privacy Commissioner. On 3 November 2023, the OAIC announced it had commenced legal proceedings against another entity, Australian Clinical Labs Ltd, seeking civil penalties in relation to similar alleged failures (ie, a failure to carry out a reasonable assessment as to whether a breach was an eligible data breach, and failing to notify the Privacy Commissioner as soon as practicable), amongst other alleged interferences with the security of personal information it held. This has clearly become a critical area of focus for the OAIC.

Conclusion

These decisions highlight that an organisation's response to a data breach is important. Both entities became aware of the incidents within 24 hours, yet substantial delays occurred in assessing the breaches and notifying the Privacy Commissioner, with a significant amount of time passing before the required notices were lodged. These delays highlight the critical importance of swift and efficient data breach response, as emphasised by the Privacy Commissioner.

The decisions serve as an important reminder for organisations to ensure they have prepared, updated and tested a robust data breach response plan, so they can act expeditiously in the event of a data breach. It is important to ensure that any response meets the requirements to contain a breach from a technical perspective as well as to ensure that regulatory obligations, including those arising under the Privacy Act are met. In setting themselves up in this way, organisations will also be better placed to address the impending privacy reforms.

Takeaway tips

- Recent rulings by the Privacy Commissioner highlight the importance of swift data breach response.
- Organisations should review and rehearse their data breach response plans, so they are ready to respond to a data breach.
- If privacy reforms proceed as proposed, organisations will have only 72 hours to assess and report a data breach in future.

Susan Kantor
Special Counsel
MinterEllison
susan.kantor@minterellison.com
www.minterellison.com

Jaimie Wolbers
Senior Associate
MinterEllison
jaimie.wolbers@minterellison.com
www.minterellison.com

Footnotes

1. Privacy Act 1988 (Cth), s 26WH(2)(a).
2. Above, s 26WH(2)(b).
3. Attorney-General's Department *Privacy Act Review Report* (2022) 15 (proposal 28.2(a)) www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.
4. Australian Government *Government Response to Privacy Act Review Report* (2023) www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF.
5. *Pacific Lutheran College (Privacy)* [2023] AICmr 98.
6. *Datateks Pty Ltd (Privacy)* [2023] AICmr 97.
7. Office of the Australian Information Commissioner (OAIC), Notifiable Data Breaches Report: January to June 2023, September 2023, accessed 5 February 2024 www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2023#_exsum.
8. OAIC, Notifiable Data Breaches Report: July to December 2022, March 2023, accessed 5 February 2024 www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2022.

Harnessing privacy management technologies for a competitive edge and enhanced efficiency

***Kelly Henney**, **Michelle Griffin** and **Niran Garcha** KPMG AUSTRALIA*

As organisations expand into global markets which are flooded with advanced technologies and artificial intelligence, it has become critical to ensure compliance with privacy regulation is at the forefront of everyone's mind. Advanced technologies coupled with rising data breaches and increased online activities has resulted in privacy and data protection concerns becoming a top priority for several organisation boards. Statistics indicate that 93% of organisations consider privacy as a top 10 organisational risk and 36% ranked it within the top 5.[1] Organisations are now coming under greater scrutiny by both regulators and consumers for how personal data is used and protected when it comes to both maximising corporate opportunities and minimising risks. Therefore, it has become critical for organisations to firstly, assess their privacy culture and secondly, embed privacy management technology that will proactively assist with the management of privacy compliance. Privacy management technologies are tools that can assist organisations to perform several privacy management activities. This article will discuss how privacy management technologies[2] can help organisations comply with numerous privacy regulations and data protection frameworks driving up efficiency and embedding a privacy by design approach for a lasting culture that promotes accountability.

It is evident, that the pandemic in 2020 accelerated not only the shift to digitalisation and technology use, but also the use and storage of data at a rapid pace and on a global scale. Statistics indicate that by 2025, the global data creation is projected to grow to more than 180 zettabytes.[3] This has led many organisations to struggle to keep track of their corporate data, personal data and sensitive data. Without proper oversight and an in-depth understanding of their data holdings, organisations are not able to decipher what data types are subject to which regulatory requirements. Therefore, it is of paramount importance for every organisation to design a strong privacy culture which can be supported with a well-established privacy management technology, as the consequences of not having those deep insights or being noncompliant with regulatory obligations can lead to significant reputational damage and financial damage which has the ability to impact the overall performance and competitiveness of an organisation.

A good privacy culture within an organisation fosters an environment where data privacy is considered to be a shared value/responsibility of all employees. It serves as the bridge that connects how an organisation encourages its employees to change their behaviour when dealing with personal data, emphasising the significance and influence of such information. This empowers an organisation to then operationalise its privacy management processes and drive efficiency with the help of privacy management technologies.

Privacy management technologies have undergone a swift evolution since the introduction of EU's General Data Protection Regulation (GDPR) GDPR 2016/679 which is considered to be the "golden standard" when it comes to the management of personal data. All organisations regardless of their size and industry handle personal data and therefore must be aware of where the collected personal data is going and how it will be used and disclosed. Privacy management solutions can help organisations ensure compliance with privacy obligations across multiple jurisdictions by streamlining manual processes. For instance, most privacy management technologies offer tools that can automate data discovery, privacy impact assessments/data protection impact assessments, data mapping, privacy rights, privacy incident management etc. Some solutions may also assist organisations with additional security controls such as automated encryption, masking and access tools.

Incorporating such privacy management technologies into a organisations existing structure can be simple and straightforward and often involves five critical steps.

Step 1: planning

Planning is the first step towards implementing a privacy management technology within an organisation's existing technological ecosystem. This will often involve planning and completing in-depth analyses of each business function to identify which systems and processes within an organisation involve personal data. Moreover, the organisation must identify the types of

personal data held, and identify impacted data subjects. Once this initial identification is complete, this will assist in the integration of the privacy management technology and ensures that there is a complete picture of the data landscape. Once these systems have been tiered by taking into consideration the volume and categories of personal data held, then discussions should be held to determine which systems would be incorporated at the first roll-out, second roll-out, third roll-out etc.

Step 2: integration

Once a plan has been developed, the second step is to integrate the privacy management technology to work alongside the organisation's existing applications, databases or platforms. Often, this integration will occur through the use of API integrations or similar which will enable different software applications to communicate with each other. This will enable the organisation (user) to maximise the value of their data whilst simultaneously prioritising privacy and compliance.

Step 3: customisation and training

Once the privacy management technology has been integrated within the organisation's ecosystem, the next step would be to customise and tailor the technology to meet the unique needs of the organisation. Some examples include but are not limited to, customising privacy impact assessment/data protection impact assessment questionnaires, setting up risk ratings and tiering methodologies for third parties as per the organisation's risk appetite. All of this should be followed by specific and tailored privacy training coupled with ongoing support from the technical implementation partner to ensure optimal productivity and seamless collaboration occurs across the various business teams.

Step 4: roll-out

The fourth step being the roll-out phase is interlinked to the planning phase in terms of ensuring the privacy management technology is rolled out in a systematic and phased manner to ensure minimal disruptions to the organisation's day-to-day operations. The phased roll-out will enable both the organisation and the implementation partner to provide ongoing technical support and ensure a seamless integration occurs and any issues that arise are resolved quickly and effectively.

Step 5: continuous monitoring

The final step is the most critical and will determine the long-term success of the privacy management technology's implementation. Through regular monitoring, an organisation will be able to:

- drive personal data insights and undertake benchmarking reporting
- compete, comply and commercialise their personal data holdings
- understand their critical success factors
- monitor their productivity levels through continuous customisation of their privacy management technology platform

There is no doubt that privacy management technologies allow organisations to harness their personal data holdings by putting in place structures that enable them to meet their data privacy obligations and drive out meaningful insights that can add real value. All organisations handling personal data have obligations under privacy regulations globally and are accountable for ensuring these obligations are met. Organisations who can take these obligations and leverage it to gain a deeper understanding of their data landscape can gain advantages over those organisations who complete the "tick-the-box" exercise and/or meet their obligations by completing manual processes.

Introducing privacy management technologies as described in steps 1–5 above involves a level of effort to ensure that the privacy management technology is set up in a way that can maximises efficiencies. For this reason, organisations who take steps to ensure their privacy technologies are complete, accurate and tailored to their specific organisation from the beginning are the organisations who see the most benefit on an ongoing basis. Organisations should at first instance gain an understanding of their technology and system capabilities, ensuring they are utilising what is already in their environment and are looking for opportunities to enhance their technology stack before introducing potential new technology.

In order for organisations to gain a competitive advantage, it is critical for them to gain consumer trust. In today's society trust has emerged as a significant factor in how organisations can compete and distinguish themselves from their competitors. This can be achieved easily by ensuring compliance with privacy and data protection rules and regulations across all jurisdictions in which the organisation operates. Privacy management technologies coupled with technical data privacy capabilities can facilitate the proactive management of privacy obligations throughout the data privacy lifecycle. This provides organisations with an agile, proactive and efficient way to meet the growing needs and demands of data privacy. It also supports organisations with the

ability to consistently demonstrate data privacy compliance, which at present is a rapidly changing landscape as it aims to meet the needs of society in the continuously modernising era.

Disclaimer
The views contained in this article are those of the authors alone and do not represent the views of any organisation.

About the authors
Kelly Henney is a Partner and National Leader at KPMG. Kelly is a legal practitioner with over 18 years' experience e across the corporate sector in government regulation. Kelly brings a wealth of experience managing data privacy risk in complex and sensitive transactions, data breach response and complex regulatory investigations throughout Asia Pacific. Kelly has also led multiple high-profile litigations and Regulatory Taskforces and advised on proceedings before the High Court of Australia.

Michelle Griffin is a Manager at KPMG. Michelle has over 6 years' experience in Privacy. She has worked as a data subject matter expert within KPMG Ireland and KPMG Australia in the risk and regulatory consulting department. Michelle has worked extensively on General Data Protection Regulation Data Privacy Programmes, in addition to compliance, remediation, risk and internal audit projects.

Niran Garcha is a Senior Consultant at KPMG. Niran is a legal practitioner with over 6 years of professional experience on the interpretation and implementation of privacy obligations, industry standards and best practice principles predominantly in privacy governance, risk and compliance for a broad range of sectors.

Kelly Henney
Partner and National Leader
KPMG Australia
khenney@kpmg.com.au
www.kpmg.com

Michelle Griffin
Manager
KPMG Australia
mgriffin7@kpmg.com.au
www.kpmg.com

Niran Garcha
Senior Consultant
KPMG Australia
ngarcha@kpmg.com.au
www.kpmg.com

Footnotes

1. B LaLonde, S Kanthasamy and S K Kingsmill "Privacy Risk Study 2023 — Executive Summary" *IAPP* June 2023 https://iapp.org/resources/article/privacy-risk-study-summary/.
2. Privacy management technologies in this context refers to technologies that assist organisations in managing their data privacy activities.
3. Statista, Volume of data/information created, captured, copies, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025, November 2023, accessed 5 February 2024 www.statista.com/statistics/871513/worldwide-data-created/.

Privacy Law
Bulletin

Expansion of data-subject-access-request (DSAR) rights under the privacy reforms

David John Mesman *SYNERGY LAW*

Takeaway tips for lawyers

- Lawyers need to understand that the proposed Commonwealth privacy reforms will significantly enhance data-subject-access-request rights (DSARs). Mirroring aspects of the EU's General Data Protection Regulation (GDPR), data subjects will have broad access rights to their personal information (PI), including rights to confirm whether an entity holds PI about them, details on how PI has been handled, used and shared, along with rights to delete or erase PI upon request.
- Lawyers with clients subject to the Australian Privacy Principles (APPs) will need to provide detailed explanations about their use of PI, demonstrate compliance with the Privacy Act 1988 (Cth) and outline reasons for refusing a DSAR request.
- The reforms suggest that APP clients, especially those with little experience in managing DSARs, will need to review and possibly enhance their access determination processes.
- Lawyers may need to guide their APP clients in utilising legislative tools and administrative processes, such as the substantial and unreasonable diversion of resources (SUDR) provisions drawn from Freedom of Information (FOI) law. This includes developing clear criteria for SUDRs or practical refusal reasons under the new privacy regime, ensuring accurate estimates of processing times and investing in staffing and technology to handle increased workloads.

Overview of changes

The Commonwealth Government's planned reforms to the Privacy Act 1988 (Cth) will enable Australians to exert much more control over the use and handling of their PI. This is reflected in the *Government Response to the Privacy Act Review Report*[1] (Cth Privacy Response) and its agreement-in-principle to significantly enhanced DSAR rights.

Modelled on the EU's GDPR, Australia's reforms will give data subjects very broad access rights under an expanded set of APPs. These new DSARs will include a right to confirm whether an APP entity holds PI about an individual, how an entity has handled, used and shared PI, along with rights to delete or erase PI upon request.

These reforms will also mandate that APP entities provide explanations about their use of PI, justify that their practices comply with the Act and outline their reasons for refusing a DSAR request. One new refusal ground has particular relevance for lawyers with APP Clients — and that is the proposal to expand APP 12.3(c), enabling them to refuse DSARs that are "frivolous, vexatious or unreasonable".

Implications for legal practice — managing DSAR volumes

When the privacy reforms come into force, the term "unreasonable" will likely play a critical and practical role for APP entities in their efforts to manage DSARs. Why? It is a near-certainty that APP entities will witness a significant uptick or surge in DSARs. That would mirror experiences in the UK, where organisations saw a sharp increase in DSARs following the GDPR coming into force in 2018.[2] Since the GDPR's enactment, many other sources have indicated that DSAR numbers in the EU have not only increased in volume, but also in terms of processing costs.

It follows that APP entities will need to rely on legislative tools and administrative processes to ensure that they are not overwhelmed by the requirement to process this uptick in DSARs. This is particularly the case with complex or vexatious applicants, who tend to monopolise the time, resources and energies of legal teams, HR groups and other business units. Similar issues surround DSARs involving "internals" using access requests as an adjunct to an employment or workplace dispute.

How will lawyers and their APP clients manage this surge in DSARs? They may need to look no further than s 24AA of the Freedom of Information Act 1982 (Cth). Section 24AA and its related provisions enable Commonwealth agencies to issue a practical refusal decision on the basis that it is a SUDR. Arguably, the SUDR principle could be applied — with relative ease, to the privacy reforms' new (unreasonable) refusal ground

under APP 12.3(c). The more difficult question for practitioners is how to define or establish a SUDR?

What's a SUDR — is time a sufficient measure?

Cianfrano v Director General, Premier's Department[3] (*Cianfrano* case) is generally considered to be a leading authority in FOI SUDR determinations — and particularly those related to complex or vexatious applicants. The *Cianfrano* case identified a series of factors that may give rise to a SUDR, including a finding that 40 hours of processing work would tend to be on the upper end of a reasonable request. However, many subsequent cases have treated the 40-hour benchmark in the *Cianfrano* case with caution. This is reinforced by the Office of the Australian Information Commissioner (OAIC)'s *FOI Guidelines*,[4] which provide a detailed summary of key SUDR cases and principles to apply in making a finding of unreasonableness:

> Whether a practical refusal reason exists will be a question of fact in the individual case . . . Agencies should not adopt a "ceiling" in relation to processing times . . . Rather, each case should be assessed on its own merits . . .[5]

While Commonwealth organisations cannot apply a processing time ceiling in making a SUDR finding, these FOI cases should not be interpreted as a ban on considering processing-time as a benchmark. Rather, processing-time should be considered a key indicator of unreasonableness in a SUDR determination. As to the specific number of processing-time hours, that would very much depend on the organisation, its structure, budget and staffing levels. What does seem clear is that the 40-hour "standard" flagged in the *Cianfrano* case is insufficient. More importantly, processing-time estimates cannot be considered as the "only" factor in making a SUDR determination.

That begs the question — how would we apply FOI and SUDR principles to a practical refusal under APP 12.3(c)? Again, this would depend on the APP entity, its structure, volumes of PI handled and other factors. However, APP entities could and, arguably, should use processing-time as a benchmark in making a determination that a given DSAR is "unreasonable". That is the common thread that weaves its way through all of the "practical, compliance strategies" outlined below.

Practical compliance strategies for refusing "unreasonable" DSARs

Certainty about processing time estimates

To paraphrase the reasoning in the *Cianfrano* case, an organisation's estimate of processing time should have a high level of certainty attached to it. It follows that APP entities making a practical refusal determination under the (new) APP 12.3(c) should be equally certain about their processing time estimates. Such estimates should be demonstrated through well-established and reliable record-keeping protocols.

The Cth Privacy Response picks up on that theme, by setting baseline expectations for APP entities when they handle PI, both from a business process and a technical perspective. This is reflected in Proposals 12.1 and 12.2 (Fair & Reasonable PI Handling), which requires entities to handle PI with due care. Proposals 12.1 and 12.2 also seek to establish an objective standard for what constitutes "fair-and-reasonable" standard when handling PI. In addition, Proposals 21.1, 21.2 and 21.7 (Security, Retention & Destruction) indicate that "reasonable steps" in APP 11 (Security of PI) should include technical and organisational measures, along with requirements to establish maximum and minimum retention periods. It also follows that any claim of "unreasonableness" under APP 12.3(c) would be more readily accepted by OAIC investigators if an APP entity has clear methodologies for estimating DSAR processing time — and ones that can be sense-checked against objective standards.

Staffing and resource availability

The OAIC *FOI Guidelines* and caselaw make it clear that Commonwealth agencies cannot point to their own "fault" in the form of poor records management, scarcity of resources or qualified staff to substantiate a SUDR claim. The same logic would likely apply to APP entities when refusing to process a DSAR as "unreasonable" under the (new) APP 12.3(c). The Cth Privacy Response seems to echo that reasoning in its proposals. In particular, Proposals 12.1 and 12.2 call for the establishment of an objective standard for the handling of PI.

Arguably, an objective, "fair-and-reasonable" implicitly would require APP entities to adequately invest resources in staffing and record-handling processes. Similarly, Proposals 21.1, 21.2 and 21.7 (Security, Retention & Destruction) will require APP entities to adopt baseline technical capabilities. Likewise, Proposal 15.2 (Organisational Accountability) will mandate the appointment of a senior employee as responsible for privacy matters. In other words, APP entities must appoint someone with sufficient seniority and accountability to ensure that privacy is adequately managed and resourced.

With the exponential growth of data held by APP entities, the resourcing equation is sure to involve the deployment of "smart tools" that can simplify repeatable, mundane and error-prone tasks. A prime use-case would relate to search tools that can scan most, if not all

APP entities' platforms. Other examples include privacy-by-design solutions, deploying robotic-process-automation (RPA) techniques. RPA solutions can replicate labour-intensive, manual processes required to lift-and-shift individual files, particularly those containing out-of-date and no-longer-needed PI. Considering that the Privacy Commissioner regularly urges APP entities to conduct data inventories and delete unnecessary PI, it would seem "unreasonable" not to deploy smart tools and business processes. It follows that APP entities would struggle to make a claim that a DSAR is unreasonable if they failed to invest in these "smart techniques".

Specialist expertise — and their competing priorities

This factor ties back to the need for certainty in estimating DSAR processing times. The complexity of a DSAR determines if specialists (like internal or external forensic services) are needed to locate personal information (PI) in difficult-to-access archives or ICT platforms. Engaging legal or other specialists might also be necessary to assess impacts on third-party privacy, health or safety risks, or grounds to refuse a DSAR under APP 12. For internal specialists, APP entities must review their regular duties and workload. Developing clear protocols to accurately assess the time needed for a DSAR, considering other priorities and documenting findings is crucial. Recording this in a standard format, such as 6-minute increments, offers benchmarks for comparing DSAR processing times, facilitating process improvements and efficiency gains.

Impacts on other work and the processing of other DSARs

This is a variation on the "specialist" criterion, with a twist that APP entities would be obliged to identify and measure the impact that a given DSAR would have on other workstreams — or the management of other DSARs. It would also require APP entities to consider — and record, the additional efforts and staff hours diverted from BAU activities to process a given DSAR. APP entities would need to account for the resourcing beyond their legal or governance teams normally tasked to manage and process DSARs. APP entities might also consider taking a forensic approach when accounting for these "surge" efforts and include IT staff and time, individual business units responsible for the given data set related to the DSAR, among others. However, APP entities should (arguably) refrain from including the time taken by internal or externals to brief executives or prepare stakeholder engagement and communication plans. Including such matters would likely undermine a finding that a DSAR was unreasonable — arguably, these stakeholder activities have little to do the mechanics of processing a DSAR. It would also tend to undermine the first and essential factor mentioned above, ie that there should be high level of accuracy in the APP entity's estimates.

Applicant limiting DSAR scope

It would be rare for DSAR applicants to volunteer to limit the scope of their access request — at least without guidance from an APP entity. With that in mind, APP entities should be inclined to assist DSAR applicants to refine the terms of their request to specific classes of data, such as PI held in active platforms and excluding any PI in digital-deep-freeze. It is not clear how the privacy reforms will balance the rights of an applicant requesting erasure (Recommendation 18.3 in the Cth Privacy Response) versus an APP entity's adherence to fair-and-reasonable PI handling (Recommendation 12.1). This issue will become particularly thorny when APP entities raise issues of reasonableness in the context of searching through cloud-based archive platforms, where retrieval costs can be prohibitively expensive. Accepting that this will sound like a broken record, APP entities will need to maintain excellent record-keeping protocols so they can pinpoint a specific individual's PI in the event of a DSAR. Otherwise, they will expend countless resources to complete a "reasonable search".

Level of public (or personal) interest in requested information

This factor originates with the FOI Act's public interest balancing tests — and determining whether conditionally exempt documents should be released. By its nature, PI relates to a specific individual, meaning that general public interest consideration would, arguably, be moot. However, this wouldn't be the case where DSARs arise in the context of a large data breach affecting significant numbers of Australians. Arguably, it would be in the "general public interest" for large numbers of individuals to determine whether their PI has been mishandled. In other words, it would likely be difficult for an APP organisation to argue that it would "unreasonable" to respond to a tsunami of DSARs, numbering in the hundreds-of-thousands. Similar issues would likely animate individual DSAR applications where there the applicant has a keen interest in obtaining the PI because it would assist in enforcing their legal rights — or where the applicant can demonstrate a significant impact upon their finances, reputation or other adverse consequences.

Conclusion

According to the FOI authorities, a practical refusal based on a SUDR — a substantial and unreasonable diversion of resources, is a question of fact in each-and-every individual case. That may not fill practitioners

with confidence, much less provide them with broad principles that can be applied when refusing a DSAR as "unreasonable" under the Privacy Act. However, APP entities can "get ahead of the curve" by establishing clear, data-driven protocols that accurately estimate the time needed to process a DSAR. While those efforts could appear daunting, they are likely to be much less of a burden than responding to a complaints and investigation by the Privacy Commissioner or scrambling to "reinvent the procedural wheel" with each new DSAR. And with privacy reforms, you can bank on the fact that there will be many DSARs.

David John Mesman
GAICD, FIP, CIPM, CIPT, CIPP/E, LLB/BCL, BA (Hnrs)
Senior Counsel & Executive Director
Synergy Law (Part of Synergy Group)
DMesman@synergygroup.net.au
https://synergygroup.net.au/synergy-law/

Footnotes

1. Australian Government *Government Response to the Privacy Act Review Report* (2023) 18 www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF; referencing Proposals 18.1–18.9.
2. Refer, for example, to M Lewis and others "The Rise and Challenge of DSARs, One Year on From the GDPR and the DPA 2018" *Squire Patton Boggs* May 2019 www.squirepattonboggs.com/~/media/files/insights/publications/2019/05/the-rise-and-challenge-of-dsars-one-year-on-from-the-gdpr-and-the-dpa-2018/dsar_survey_alert.pdf.
3. *Cianfrano v Director General, Premier's Department* [2006] NSWADT 137 at [62].
4. Office of the Australian Information Commissioner *FOI Guidelines* (2023) www.oaic.gov.au/__data/assets/pdf_file/0023/103595/Combined-FOI-guidelines-November-2023.pdf.
5. Above, para 3.119.

For editorial enquiries and unsolicited article proposals please contact Monica Nakhla at monica.nakhla@lexisnexis.com.au
Cite this issue as (2024) 20(10) *PRIVLB*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN 1449-8227 Print Post Approved PP 243459/00067