



DEIDRE MISSINGHAM
Consulting Principal,
Keypoint Law



PENELOPE PENGILLEY
RITP
Consulting Principal,
Keypoint Law

legal update

DISCLOSURE OF PERSONAL INFORMATION

How to chart a safe course through statutory obligations and the Australian Privacy Principles.

Natural metaphors sprang to mind as Keypoint Law privacy and insolvency specialists were privileged to present at ARITA's Small Practice Conference in June this year.¹ Our topic then was 'In the Interests of Full Disclosure: When do statutory obligations override the privacy principles?', but robust discussion prior and questions after – on issues including regulation of sale of personal information and the Privacy Act's penalty regime – carried our talk into waters less charted. This article recaps and expands on that presentation.²

KEY PRIVACY ACT OBLIGATION AND PENALTIES

An overarching obligation under s 15 of the *Privacy Act 1988* (Cth) (Privacy Act) states that:

An APP entity must not do an act, or engage in a practice, that breaches the Australian Privacy Principles.

Despite these clear words, in the past some Australian Privacy Principles (APP) entities – including insolvency practitioners – may have felt comfortable carrying on their businesses while paying scant attention to privacy obligations. For liquidators and the like, there was also the widespread view that practitioners enjoyed special protections.

However, from 2022, the penalties under the Privacy Act for breaching an APP increased substantially. Now a "serious" or "repeated" interference with privacy can attract a fine of the greater of:

- \$50 million
- three times the value of any benefit obtained through the misuse of the information, or

- 30% of the organisation's annual turnover when the breach occurred (if the court cannot determine the value of the benefit).

In addition, Privacy Act reforms set to be introduced from August this year are likely to include a suite of new 'administrative fines' that have been agreed on by the government. At the current penalty rate value, once legislated, these could cost organisations up to \$126,000 for simply not having complied with the APPs, and up to \$626,000 for medium-level breaches. Importantly, individual insolvency practitioners who are officers of a corporation may be subject to these fines. These penalties have certainly been designed to encourage organisational accountability and focus the corporate mind.

In light of this expanded penalty regime, insolvency practitioners and their firms have no time to lose in ensuring that they understand and act in accordance with their privacy obligations under the Privacy Act, as well as under other legislation and standards governing their professional practice.

APPS, APP ENTITIES AND 'PERSONAL INFORMATION'

Before we sail further into disclosure issues, practitioners may be assisted by a brief recap on some of the Privacy Act fundamentals that will help chart a course towards compliance.

The 13 APPs set out in Sch 1 of the Privacy Act are legally binding principles that are the cornerstone of the Privacy Act's privacy protection framework. They set out standards, rights and obligations in relation to collecting, handling, holding, accessing and correcting personal information.

¹ The Keypoint Law Consulting Principals who presented were Deidre Missingham and Mark Addison RITP. Special thanks are extended to Mark Addison for his contribution to the presentation and discussions leading to this article. ² This article is current as at 19 July 2024.

The private and public sector organisations to which the APPs apply are collectively called "APP entities". A private sector organisation is defined as:

- an individual (including a sole trader)
- a body corporate
- a partnership
- any other unincorporated association, or
- a trust.

Therefore, both an insolvency practitioner and their practice (or an entity a practitioner is appointed over) may be caught by the APPs, unless an exemption applies. Importantly, the current 'small business exemption' available to most organisations with an annual turnover of \$3,000,000 or less, may be modified or removed in the (at the time of writing) forthcoming Privacy Act reforms. Organisations are not considered small business operators for the purpose of this exemption if they are undertaking higher-risk activity, including trading in personal information, pursuant to s 6D of the Privacy Act.

Personal information is defined in s 6 of the Privacy Act as:

Information or an opinion about an identifiable individual, or an individual who is reasonably identifiable:

- a) Whether the information or opinion is true or not; and
- b) Whether the information or opinion is recorded in a material form or not.

In the course of their duties under the *Corporations Act 2001* (Cth) (Corporations Act), insolvency practitioners commonly collect a wide range of personal information contained in:

- client lists
- creditor lists
- customer and supplier lists
- CRM (customer relationship management) software content, including the Notes section
- patients' or clients' records, and
- shareholder information and staff and contractor details.

DISCLOSURE

Disclosure of personal information contrary to the provisions of APP 6 (Use and Disclosure) is prohibited. But what does "disclosure" mean here? The Privacy Act does not define disclosure, but an APP entity discloses personal information when it makes it accessible or visible to others outside the

“Practitioners and their firms have no time to lose in ensuring they understand and act in accordance with their privacy obligations.”

entity and releases the handling of the information from its effective control.

Insolvency practitioners might relevantly disclose personal information in situations such as:

- selling a business or selling a business's assets, including information³
- enabling due diligence and data rooms
- reporting to creditors
- filing an affidavit in proceedings, or
- dealing with employees, a FEG Scheme or trade unions.

Provision of personal information to a contractor that the APP entity has engaged also generally constitutes disclosure, which could include provision to agents for sale, managers in a trade-on or professional stock takers.

Unfortunately, human error can also cause relevant disclosure, for example:

- accidental or unauthorised release of information to a third party in response to a request
- accidental posting of information on a website, or
- negligent handling or loss of information, devices or an unencrypted USB drive.

³ The sale of a whole business is not "trading in personal information", but selling personal information including customer lists is and requires the consent of each affected individual or to be otherwise required or authorised by law: see <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/trading-in-personal-information>. The ACCC also regulates data collection, use and disclosure. On 21 May 2024, the ACCC released the eighth interim report for the Digital Platform Services Inquiry, which considered potential competition and consumer issues in the supply of data products and services by data firms in Australia.

Deliberate but unauthorised disclosure could include:

- a practitioner's disclosure of information to themselves in a different capacity (e.g. in their capacity as a director of another entity) (though disclosure of other than sensitive information to a related body corporate is permitted under s 13B(1)(b)), and
- where information shared by a practitioner exceeds any legal requirements or authorisations.

Under APP 6, an APP entity that holds personal information about an individual *can only use or disclose that information for a particular purpose for which it was collected (known as the 'primary purpose' of collection, unless (as mentioned above) an exception applies. If there is an applicable exception the entity may use or disclose personal information for another purpose (known as the "secondary purpose").*

For insolvency practitioners, relevant exceptions may include:

- the individual consented to a secondary use or disclosure (APP 6.1(a))
- the individual would reasonably expect the secondary use or disclosure, and it is related to the primary purpose of collection or, in the case of sensitive information as defined, directly related to the primary purpose (APP 6.2(a)), and
- the secondary use or disclosure of the personal information is required or authorised by or under an Australian law or a court/tribunal order (APP 6.2(b)).

Of these, if it is applicable, APP 6.2(b) presents the fewest obstacles to lawful disclosure, since it can be difficult or impractical for insolvency practitioners to obtain the valid consent required for APP 6.1(a) to apply, and they may lack the time or resources needed to ascertain the required "reasonable expectation" of each individual whose personal information is held for APP 6.2(a).

Accordingly, some acts and practices of insolvency practitioners who are APP entities, which would otherwise constitute interference with the privacy of individuals under the APPs, are permitted by reason of provisions of the Corporations Act (an 'Australian law') whereby the key exception (APP 6.2(b)) is engaged (see above). However, practitioners should also note that the Privacy Act itself is 'an Australian law' containing specific privacy requirements outside the APPs, notably concerning tax file numbers (TFNs).⁴

CORPORATIONS ACT DISCLOSURE REQUIREMENTS AND AUTHORISATIONS

Practitioners will be well aware that under Sch 2 of the Corporations Act (the Insolvency Practice Schedule (Corporations)), only a registered liquidator can perform certain roles, such as:

- receiver of the property of a corporation
- administrator of a company or of a deed of company arrangement
- restructuring practitioner for a company or for a restructuring plan, or
- the liquidator of a company.

The specific role being performed will generally determine what legislated powers the practitioner has in relation to the distressed company and its information holdings.

As an example, we consider here the requirements under Disclosures by Administrators to Creditors and others.

The Insolvency Practice Rules (IPR) 75-225 made under s 105-1 of Sch 2 to the Corporations Act (IPS) require that for the "second creditors' meeting" called under Corporations Act s 439A, the creditors must 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 are required to include creditor lists for a variety of policy reasons, including because they are material to a company's financial affairs, and enabling creditors to identify other creditors may assist them in enforcing their rights.

We note in particular the requirement under s 497(1)(a)(ii) of the Corporations Act to provide to all creditors in a CVL a list of creditors' names, addresses and estimated amounts owing. These creditors may include identified individuals, such as employees or customers/consumers who have pre-paid for goods.

Insofar as a creditor list contains legislatively specified information that is personal information, the provision of the report may be a relevant disclosure that is permitted under APP 6.2(b). However, the amount of personal information included in the creditor list should be kept to a minimum when reporting to creditors – inclusion of superfluous information (for example individuals' telephone numbers) is neither "required" nor "authorised".

⁴ See s 17 Rules relating to tax file number information and s 18 File number recipients to comply with rules.

Minimisation is also recommended for responses to creditors who, as a body or individually, can seek further information about the company's affairs from an administrator:

- creditors have rights to inspect the books kept by external administrators at all reasonable times (IPS 2 70-10), and
- creditors can request information or a document by resolution (IPS 2 70-40(1)).

The external administrator may refuse to provide access if:

- the information is not relevant to the external administration (IPS 2 70-40 (2)(a)) (likely to be personal information, and unlikely to satisfy APP 6.2)
- it would be a breach of duty to comply (IPS 70-40(2)(b)), or
- it would otherwise be unreasonable (IPS 70-40 (2)(c)).

Unreasonableness is dealt with in the IPR Division 70 – Information. A creditor's request may be refused on the ground of unreasonableness where:

- disclosure could found an action in breach of confidence⁵ (IPR 70-10 (2)(c)) if the confidential information contains personal information.

When deciding whether or not to refuse, practitioners should also take into account, if enacted, the proposed introduction into the Privacy Act of an (overarching) requirement that the

collection, use or disclosure of personal information must be "*fair and reasonable in the circumstances*". This requirement would apply whether or not consent has been obtained.

This 'fair and reasonable test' will be objective. Factors that may be taken into account include:





- the kind, sensitivity and amount of personal information being collected, used or disclosed
- whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation, and
- whether the collection, use or disclosure is 'proportionate', including consideration of:
 - a) whether the collection, use or disclosure intrudes upon the personal affairs of the affected individual to an unreasonable extent
 - b) whether there are less intrusive means of achieving the same ends, at comparable cost and with comparable benefits, and
 - c) any actions or measures taken to mitigate the loss of privacy.

A recent Federal Court decision suggests that courts may be prepared to afford protection to creditor information (and to hard-pressed administrators) in some circumstances.

⁵ Use of the doctrine of breach of confidence to protect personal information was more common before express legislative protections were enacted, but as the IPRs demonstrate it still forms part of the protective framework today.

IPS Cloud

The future of insolvency & restructuring software

-  Access anytime, anywhere
-  Be audit ready with a complete record of all changes
-  Secure platform with automatic upgrades
-  Manage approvals on the go with our new mobile app

turnkey-ips.com
enquiries@turnkey-ips.com
Asia-Pacific: +617 2104 9050

Powered by 



On 5 February 2024, in the case *Crosbie (administrator in the matter of Godfreys Group Pty Ltd (administrators appointed))* [2024] FCA 60 (Godfreys), Justice Beach made the following order in respect of an extension of convening period sought by the administrators appointed:

5. Pursuant to s 90-15 of the IPS, in complying with *any requests for information pursuant to ss 70-40 or 70-45 of the IPS and/or in discharging any other obligation to disclose* names or contact information of any creditors or potential creditors of the Companies (including owners and lessors of property occupied by or in possession of the Companies), the first plaintiffs may:
 - a) redact from any document the names or contact information of any creditors or potential creditors of the Companies; and
 - b) withhold the names or contact information of any creditors or potential creditors of the Companies. [emphasis added]

It remains to be seen how often this approach will be taken. Justice Beach did not provide reasons for this part of his orders. However, in making the order the Court seems to have made certain assumptions about what is fair and reasonable regarding the provision of specified personal information to other creditors.

DISCLOSURES REQUIRED OR AUTHORISED BY OR UNDER ... A COURT/TRIBUNAL ORDER

Courts and tribunals may order disclosure. But because insolvency practitioners have extensive coercive powers under the Corporations Act (such as summoning directors and officers for examination in court regarding the distressed company’s affairs, or requiring other persons to produce documents), courts may also exercise a protective discretion: especially for third-party personal information.

For example, in appropriate cases, courts may order:

- private examinations, or give directions regarding the examination process, or
- that documents containing certain information including personal information be treated as confidential or have names and other details redacted, as in *Godfreys*.

The orders in the *Godfreys* case demonstrate an awareness of the issue and willingness to take a practical approach to privacy protection.

CROSS-BORDER DISCLOSURES


Disclosure of personal information outside Australia, even when permitted under APP 6, carries additional obligations. APP 8 together with s 16C of the Privacy Act (Acts and practices of overseas recipients of personal information) creates a framework for this cross-border disclosure.

The framework generally requires an APP entity to take reasonable steps to ensure that an overseas recipient will handle an individual’s personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information.⁶

By way of example:

- a permitted disclosure would include an APP entity disclosing personal information to the government of a foreign country under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), and
- a disclosure that may be in breach would include an APP entity disclosing personal information by publishing it on the internet, whether intentionally or not, and the information is accessible to an overseas recipient not authorised to see it. Uploading of personal information to a cloud service provider may be characterised as “use” for the limited purpose of storing rather than “disclosure”, but uploading it to an overseas-based public generative AI site such as ChatGPT is also likely to constitute a disclosure breach under APPs 6 and 8.

KEY TAKEAWAYS FOR SMOOTH SAILING

1. Organisations must comply with the APPs unless an exception or exemption applies in the circumstance of the organisation’s handling of personal information.
2. Statutory obligations in other legislation affecting the handling of personal information, notably in the Corporations Act, will apply in any circumstances where the APPs (including the Commissioner’s Guidelines) are silent or may provide a relevant exception or exemption.
3. Remember that the Privacy Act also contains statutory obligations outside the APPs that may also apply, e.g. for TFN recipients or under the Notifiable Data Breaches scheme. 

⁶ We recommend that insolvency practitioners pay particular attention to the relevant terms in any enforceable contracts with overseas third-party service providers and monitor compliance (e.g. by auditing).