

1 February 2012

## Privacy Law e-alert

# Through the looking glass – notes on privacy

## Never think your personal information is safe

The Australian Information Commissioner recently released case notes on investigations concerning privacy related complaints that illustrate the application of the Privacy Act in new circumstances, industries and subject areas.

“Case 1: Parking services organisation pursues debt” on page 2

“Case 2: No ID, No entry” on page 3

“Case 3: Investigation of alleged fraud leads to disclosure of personal information” on page 4

“Case 4: Disclosure of personal information during debt recovery process” on page 4

“Case 5: Law firm in covert operation to gather evidence” on page 5

“Case 6: Student asks for answers to exam” on page 5

“Case 7: Retailer records telephone calls with customers” on page 6

“Case 8: Dude, is that my personal information?” on page 7

“Case 9: Telco denies access to personal information” on page 7

If you have any questions about the issues raised in these cases or their impact on your business, please contact:

John Kell, Sydney (City)	+61 2 9391 3163	<a href="mailto:jkell@hunthunt.com.au">jkell@hunthunt.com.au</a>
Mark Byers (North Ryde)	+61 2 9804 5777	<a href="mailto:mbyers@hunthunt.com.au">mbyers@hunthunt.com.au</a>
David Thompson, Melbourne	+61 3 8602 9252	<a href="mailto:dthompson@hunthunt.com.au">dthompson@hunthunt.com.au</a>
Rachel Drew, Brisbane	+61 7 3292 9717	<a href="mailto:rdrew@macrossans.com.au">rdrew@macrossans.com.au</a>
Brenton James, Adelaide	+61 8 8414 3347	<a href="mailto:bjames@hunthunt.com.au">bjames@hunthunt.com.au</a>

Disclaimer: The information contained in this e-alert is not advice and should not be relied upon as legal advice. Hunt & Hunt recommends that if you have a matter that is legal, or has legal implications, you consult with your legal adviser. If you no longer wish to receive this e-alert or any other publication from Hunt & Hunt, please email us at [unsubscribe@hunthunt.com.au](mailto:unsubscribe@hunthunt.com.au).

1 February 2012

## Case 1: Parking services organisation pursues debt

This case was about:

- » **NPP 1.1:** Organisations can only collect personal information if the information is necessary for one or more of their functions or activities.
- » **NPP 1.2:** Organisations must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
- » **NPP 4.2:** Organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed.

A parking services organisation had a short business relationship with the complainant and was of the belief that the complainant owed it money. To pursue the debt the parking services organisation obtained a court subpoena for records held by a state government department.

The complainant alleged there was a mistake and it was not indebted to the parking services organisation and therefore did not want the parking services organisation to hold personal information about it.

After the parking services organisation had obtained the complainant's personal information with the court subpoena it realised there had been an administrative error and the complainant did not owe it any money. However, the parking services organisation said it still required to retain the complainant's personal information to allow it to meet obligations with other laws, including taxation and corporations law.

The Commissioner noted that:

- » the parking services organisation did not need the complainant's consent before it collected the personal information; and
- » the collection of the personal information was necessary for its activities and was collected by lawful means and not unreasonably intrusive.

The Commissioner was satisfied that the organisation's reason to keep the complainant's personal information to meet obligations with other laws, including taxation and corporations law was a legitimate reason for retaining the complainant's personal information.

The case demonstrates that:

- » the fact that an organisation's method of collecting personal information about an individual may seem heavy-handed to that individual does not mean that the method is not lawful and fair; and
- » an organisation may have a legitimate need to retain personal information even though the original purpose for collecting that personal information no longer exists.

[\*<< back to main page\*](#)

1 February 2012

## Case 2: No ID, No entry

This case was about:

- » **NPP 1.1:** Organisations can only collect personal information if the information is necessary for one or more of their functions or activities.
- » **NPP 1.3:** Organisations must take reasonable steps to ensure that individuals are aware of certain things when the organisation collects personal information about them including the purposes for which the information is collected.
- » **NPP 4.2:** Organisations must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed.

Under section 31 of the *Registered Clubs Act 1976*, registered clubs are required to retain certain information for 5 years. That information comprises the name and address of every visitor to the club and the date they entered the registered club as a visitor and is personal information for the purposes of the *Privacy Act*.

To meet this obligation the registered club that was the subject of this complaint had adopted a practice of scanning the identification of every visitor to the club. This enabled them to record the information required by section 31.

This complaint arose because the complainant noted that in scanning their driver's licence the club also collected information that was not required under the *Registered Clubs Act*. That information included the complainant's date of birth, driver's licence number, driver's licence type and photograph.

The complainant also expressed concerns that the registered club's notice and security procedures were insufficient.

The Commissioner commenced an investigation of the matter and also attempted to conciliate the matter.

As part of the conciliation process the complainant accepted the club's offer to delete their personal information from its database if the complainant would provide the club with a statutory declaration containing the information required to comply with section 31.

However, the club explained that because the scanning practice allowed it to comply with its obligations under section 31 it would not agree to stop or vary that practice. It had procedures in place to ensure that information was deleted after the requisite 5 year period. The registered club also offered patrons the option of manually completing and signing the register. In response to the complaint, the club also offered to give patrons the option of changing their mind after their identification had been scanned and deleting any information not required by section 31 provided that the club had sufficient information to comply with its obligations under that section.

In response to the complaint about the lack of notice about the club's privacy practices, the club responded that there was a statement displayed at the entrance to the club and again at the terminal where visitors' identification was scanned. That statement referred patrons to the club's privacy policy.

Finally, the club conceded that it had been retaining the personal information collected from patrons for 7 years rather than the 5 years required by section 31 and agreed that it would destroy that information after 5 years.

The Commissioner considered the registered club's proposal and believed it adequately dealt with the collection and notice issues that were of concern to the complainant.

This case illustrates the sometimes complicated relationship between legislation that requires an organisation to collect and retain personal information and the organisation's obligations under the *Privacy Act*. In this case, by scanning patrons' identification cards the club was collecting more information than was strictly necessary. However, the scanning practice presumably also facilitated easy entry to the club. Because patrons had the option of manually completing and signing the register, by agreeing to have their identification scanned patrons consented to the collection of that additional information.

[<< back to main page](#)

1 February 2012

## Case 3: Investigation of alleged fraud leads to disclosure of personal information

This case was about:

- » **NPP 3:** Organisations must take reasonable steps to make sure that the personal information they collect, use or disclose is accurate, complete and up-to-date.

The complainant was a loss assessor in the insurance industry. An insurance company collected the complainant's personal information from a third party insurance industry database while investigating an alleged fraud.

The complainant accessed their file on the industry database and discovered that the insurance company had made multiple enquiry listings about them and had inaccurately listed the purpose for the enquiries such as the complainant was a 'witness', 'insured'; and 'third party claimant'.

The insurance company made multiple enquiries as it had not included an enquiry reference number (which was not mandatory) when disclosing the complainant's personal information to the insurance industry database. This resulted in multiple enquiries being recorded when only one enquiry should have been listed. In addition, the insurance company was

not able to update its records when the complainant advised it that its records were inaccurate as its systems did not have the capability to do so.

In order to resolve the complaint, the insurance company:

- » put in place procedures to ensure its staff used a unique reference number for enquiries it makes on the insurance industry database;
- » retrained staff on the appropriate descriptors to be attached to enquiries made with the database;
- » amended the complainant's insurance database so it was accurate; and
- » offered the complainant an unconditional apology.

This case emphasises the importance of ensuring that organisations have in place systems and processes to ensure that any personal information they deal with is accurate, complete and up-to-date but, if it is not, that they are able to correct it.

[<< back to main page](#)

---

## Case 4: Disclosure of personal information during debt recovery process

This case was about:

- » **NPP 2.1:** Organisations must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection, unless an exception in NPP 2.1(a) to (h) applies.
- » **NPP 2.1(a):** An organisation is permitted to use or disclose personal information for a secondary purpose where that purpose is related to the primary purpose of collection, and the individual would reasonably expect the disclosure.

A utility service provider engaged a law firm to recover a debt owed by the complainant. The complainant subsequently settled the debt and was advised that debt recovery action would cease.

The utility service provider was unable to notify the law firm to cease the debt recovery action before the law firm had sent correspondence to the complainant's neighbour enquiring as to the complainant's whereabouts. This revealed that the complainant had an outstanding debt.

As part of recovering the debt, the law firm said it sought information from third parties that it believed could assist in their investigation and debt recovery activity.

As a result of its investigations the Commissioner considered that the information disclosed was that the law firm wished to contact the complainant, not any specific information relating to the debt.

The Commissioner was of the view that the individual would reasonably expect that an organisation would disclose its name and the complainant's name to contact a third party in the circumstances.

While there was no breach of NPP 2, the Commissioner referred the debt collection practices to the Australian Competition and Consumer Commission to confirm whether they were consistent with its debt collection guidelines.

[<< back to main page](#)

1 February 2012

## Case 5: Law firm in covert operation to gather evidence

This case was about:

- » **NPP 1.2:** Organisations must collect personal information only by lawful and fair means and not in an unreasonably intrusive way;
- » **NPP 10.1:** Organisation must not collect sensitive information about an individual unless one of the exceptions at NPP 10.1 (a) to (e) applies;
- » **NPP 10.1(e):** An organisations is allowed to collect sensitive information if the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

A law firm was acting for an insurer when it launched a covert surveillance operation in an effort to collect the complainant's personal information, including their health information which was used during court proceedings. The complainant alleged that the law firm interfered with their privacy by improperly collecting the personal information.

The Commissioner agreed that generally the collection of personal information covertly would not be considered as 'fair' under NPP 1.2.

However, in this instance the Commissioner disagreed with the complainant and was of the view that:

- » the law firm's collection of personal information was by fair means and not in an unreasonably intrusive way as it was part of defending a claim where it was suspected that the individual may have misrepresented their claim; and
- » collection of the health information was necessary for the defence of a legal claim.

[\*<< back to main page\*](#)

---

## Case 6: Student asks for answers to exam

This case was about:

- » **NPP 6.1:** Organisations that hold personal information about an individual must provide the individual with access to the information on request unless one of the exceptions listed in NPP 6.1(a) to (k) applies;
- » **NPP 6.2:** Where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

The complainant undertook an exam through a professional association and sought access to their completed and marked exam paper, associated documents which were used to mark and rate their performance along with the application for special consideration and all relevant documentation used in assessment of that application.

In response to the complainant's request, the professional association provided the complainant with a copy of the front page of the exam paper, the multiple choice sheet that contained their personal information as well as a copy of their application for special consideration. The professional association refused to provide the complainant with access to the rest of the documents they had requested and provided an explanation to the complainant through a detailed 'personal analysis letter'.

The Commissioner formed the view that providing the complainant with access to the documents used to assess the exam and the application for special consideration would reveal evaluative information generated in connection with the commercially sensitive decision making process for the Professional Association.

This case provides useful guidance as to what constitutes a commercially sensitive decision-making process.

[\*<< back to main page\*](#)

1 February 2012

## Case 7: Retailer records telephone calls with customers

This case was about:

- » **NPP 1.1:** Organisations can only collect personal information if the information is necessary for one or more of their functions or activities;
- » **NPP 1.2:** Organisations must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

It was alleged that a retail company recorded outbound calls it made to the complainant without providing notification that it was recording the calls and without notifying or asking for the complainant's consent to record the calls.

The retail company argued that they had notified the complainant that inbound calls were recorded. On this basis, the retail company argued that the complainant was aware that outbound calls were also being recorded and consent to the collection of such information could be implied.

The retail company said the purpose for recording the calls was for training, coaching and monitoring purposes including to process orders and action enquiries. The Commissioner agreed that this was the purpose of the recording the calls. However, the Commissioner did not agree with the retail company's argument that the calls received by the complainant were a continuation of the original incoming call where notification had been provided.

The retail company claimed that its privacy policy outlines that as part of its terms and conditions that a customer agrees to the collection of personal information in ways the retail company considers appropriate including for a purpose to which an individual consents (express or inferred consent). The Commissioner reviewed the privacy policy and formed the view that it did not provide sufficient notification that the collection of information via call recording would occur.

Having considered that the complainant was not notified that the retail company was recording outbound calls and the retail company's general privacy obligations, the Commissioner formed the view that collection of personal information during the calls was unlawful and unfair.

This resulted in the retail company changing its procedures for recording calls. It also implemented a standard script read by relevant staff making outbound calls advising the individual that their call is being monitored and recorded for training purposes.

This case demonstrates the difficulty of an organisation relying on implied consent when the information given to the individual whose personal information is collected is inadequate.

[\*<< back to main page\*](#)

1 February 2012

## Case 8: Dude, is that my personal information?

This case was about:

- » **NPP 2.1:** Organisations must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection, unless an exception in NPP 2.1(a) to (h) applies.

A complainant agreed to sell their car to a prospective buyer, which was under finance to a financial institution. The financial institution held an interest in the car as security for the complainant's loan.

The prospective buyer had been advised by the financial institution that the car had been under finance. The financial institution then sent a letter to the prospective buyer confirming the complainant had paid out the loan and that it would release its security interest in the vehicle in ten working days.

The financial institution denied that it disclosed the complainant's personal information because the letter it sent to the prospective buyer only contained details about the complainant's vehicle, but not the complainant's name, date of birth, address or account number.

Even though the letter from the financial institution only related to the complainant's account and the prospective buyer was aware that the vehicle was under finance, the Commissioner was of the view that the financial institution had breached its obligations under the Privacy Act and disclosed the complainant's personal information to the prospective buyer as the prospective buyer could reasonably ascertain that the details related to the complainant's account.

The financial institution did not agree with the Commissioner's findings. Despite this, the financial institution agreed to immediately cease its practice of sending such letters to the third parties without the written consent of the account holder.

The finance company conciliated with the complainant and offered an apology and a goodwill payment.

On the face of it, it is difficult to agree with this decision as the buyer was aware that the car they were buying was under finance which was information that should have been publicly available. It is not surprising that a reasonable buyer in these circumstances would not seek confirmation that the finance had been paid out before completing their purchase and would seek that confirmation from the financial institution.

[<< back to main page](#)

---

## Case 9: Telco denies access to personal information

This case was about:

- » **NPP 6.1(j):** Organisations that hold personal information about an individual must provide the individual with access to the information on request unless providing access would be likely to prejudice activities carried out by, or on behalf of an enforcement body;
- » **NPP 6.7:** An organisation must provide reasons for denial of access or a refusal to correct personal information.

A complainant tried to gain access to their personal information held by a telecommunication company that they believed included correspondence to a law enforcement agency.

The telecommunication company denied the complainant access to the personal information relying on its internal privacy policy and claimed access would reveal strategy and procedures employed in law enforcement.

The Commissioner found that the telecommunication company could rely on the defence that access to the information would reveal strategy and procedures employed in law enforcement and subsequently was not obligated to reveal whether it possessed records from a law enforcement agency.

This case illustrates that it is not only enforcement bodies that can rely on the exception in NPP 6.1(j).

[<< back to main page](#)