PRIVACY CASE STUDIES

▶ 'WP' and Secretary to the Department of Home Affairs (Privacy) [2021] AICmr 2 (11 January 2021) – AIC's first representative complaint determination

IPP 4 – data security failure (breach) – IPP 11 – unauthorised disclosure (breach)

Remedy: *Compensation awarded – manner in which the amount of compensation payable to class members is to be calculated – process for determining dispute regarding the entitlement of a class member to the payment*

On 10 February 2014, the respondent inadvertently published the personal information of 9258 individuals who were in migration detention at that time. The information was contained in a word document that had an excel spreadsheet embedded within it which included the names, gender, citizenship, date of birth, detention location and arrival details of the individuals. The respondent was notified about the data beach by a journalist some 8 days later, and removed the report. The respondent also identified that the report was available on Archive.org and wrote to that website seeking removal, which occurred 16 days after the initial publication.

A representative complaint was submitted to the OAIC. The class members sought a declaration that they were entitled to an apology, as well as compensation for economic and non-economic loss and aggravated damages.

An Own Motion Report dated 12 November 2014 concluded that the respondent failed to put in place reasonable security safeguards to protect the personal information that it held against loss, unauthorised access, use, modification or disclosure and against other misuse. It also found that the publication of the personal information of the listed individuals was an unauthorised disclosure.

Apology given: As an apology was previously given to the class, no determination was made requiring a further apology.

Change of protection visa status not within power: The Commissioner declined to make a declaration that the respondent must reconsider the rejected protection visa applications of class members, noting that protection claims are assessed through a separate administrative decision-making process under the *Migration Act 1958* (Cth), and the Commissioner did not have the power to reconsider decisions made under a separate statutory scheme.

Compensation for economic and non-economic loss: The Commissioner determined that the participating class members are to be paid compensation for economic and non-economic loss, and directed the respondent to assign a quantum of damages for each participating class member, with reference to a Table provided as an addendum to the determination. The Commissioner declared that if, after a preliminary assessment, the respondent and class member are in agreement, compensation is to be paid as resolution of the matter within a reasonable timeframe. The Commissioner set out a process for reassessment, including the

possibility of referring the matter for assessment by an expert, with the respondent to bear the costs for resolving cases where agreement is not reached.

The table at Addendum A to the determination sets out a system of categorising non-economic loss, with Category 1 being 'general anxiousness, trepidation, concern or embarrassment' resulting from the breach, with a quantum range of $500–$4000, up to Category 5 being for 'extreme loss or damage' from the breach, and indicating a quantum of $20,000 or more would be appropriate. The table provides useful guidance to ranges of compensation depending on the degree of non-economic loss.

▶ 'WQ' and Commissioner of Taxation (Privacy) [2021] AICmr 4 (11 February 2021)

APP 6 (no breach) — APP 10 (no breach) — APP 11 (no breach)

Remedy: *None*

The complainant was advised by an ATO officer to apply for a release from his tax debt instead of pursuing a payment plan. Nearly two months later, the ATO provided the complainant's personal information to a Mercantile Agent for debt collection. The complainant then received a letter of demand from the Mercantile Agent, and contacted the ATO regarding that letter on the same day. The ATO advised the complainant that it had not received any release application from him. The ATO processed the complainant's application for a release from his tax debt a day later.

The ATO denied it had interfered with the complainant's privacy and the disclosure to the Mercantile Agent was necessary for its debt collection activities.

While WQ alleged that automation of the referral process was a breach of APPs 6, 10 and 11, the Commissioner found that the requirements of these principles were met.

The Commissioner found that the ATO did not breach APP 6 in providing access to the complainant's entire taxation file, as the data file and general information related to the specific function of debt collection, being the primary purpose under APP 6. The Commissioner found that information used for the secondary purpose fell within exceptions in APP 6.2(a).

The Commissioner found that given the range of duties required of the Mercantile Agent's staff, the ATO took reasonable steps to ensure protection of the complainant's personal information and there was no breach APP 10 or 11.

▶ 'WL' and Secretary to the Department of Defence [2020] AICmr 69 (22 December 2020)

APP 3.1 (breach)

Remedy: *Declaration of interference with privacy – Apology.*

WL posted Australian Defence Force (ADF) equipment for sale on a website. Under the *Defence Force Discipline Act 1982* (DFD), unlawful sale of Commonwealth property is an offence.

Defence obtained details of the user from the website, which it matched with other data to identify WL as a former reservist. As Defence's activities extend only to investigating suspected unlawful activity by serving members and reservists, it referred the matter to Victoria Police.

WL claimed the collection, use and disclosure of their information breached APPs 3 and 6. WL also claimed that the sharing of information internally led to his details being posted on an unauthorised Facebook page in breach of APPs 6 and APP 11.

The Commissioner found that Defence interfered with WL's privacy by over-collecting their personal information. In addition to information that was reasonably necessary to collect, Defence had collected information from the website about WL's website feedback score, password, billing and user ID history. The Commissioner found collection was not reasonably necessary or directly related to the function to investigate service offences and a breach of APP 3.1.

The Commissioner found that the disclosure to Victoria Police, after Defence determined it no longer had jurisdiction to investigation the potential offence, occurred for a secondary purpose that a reasonable person would expect, which was authorised under APP 6.2(a). The Commissioner was not satisfied that the acts of individual members posting on the Facebook page could be attributed to the respondent.

The Commissioner made a declaration that Defence interfered with the privacy of WL and should make an apology. Damages were not considered appropriate as there was no evident connection between the additional information provided in the response and the complainant's emotional distress. The Commissioner found aggravated damages were unwarranted.

▶ 'WG' and AustralianSuper Pty Ltd (Privacy) [2020] AICmr 64 (16 December 2020)

APP 5, APP 6, APP 10, APP 11 (breach)

Remedy: Compensation awarded for non-economic loss — No aggravated damages

During November 2014, the complainant submitted a claim to the respondent for payment under income protection and total and permanent disablement insurance policies with the respondent. At different times during the assessment of the insurance claim, the complainant engaged the services of two different law firms (Law Firm 1 and Law Firm 2) to assist with their claim.

Prior to the date the respondent made a payment to the complainant in respect of the insurance claim, WG terminated the engagement of each of the law firms and notified the respondent that they had revoked authority for the firms to act. Despite the revocations, the respondent made contact with the firms regarding the insurance claim.

The complainant made a range of claims, including that the assessment of their claim was done by the administrator, not the insurer, and that this had not been made clear to them (claim 1), disclosure of their personal information to Law Firm 1 (claim 2) and Law

Firm 2 (claim 3) was unauthorised in circumstances where they had revoked authority, and disclosure to Law Firm 1 that they had received a payment (claim 4) was unauthorised.

The Acting Commissioner found that claims 1 and 4 were not substantiated. However, she was satisfied that claims 2 and 3 were substantiated, finding that:

- the respondent breached APP 6 when it disclosed the personal information of the complainant to the complainant's previous legal representatives after the complainant withdrew their consent for the respondent to do so
- the respondent breached APP 10 by failing to take reasonable steps to ensure that the complainant's previous authorisation to communicate with the law firms, was accurate and up-to-date,
- the information was disclosed in a way that amounted to a breach of APP 11 as there were additional reasonable steps the respondent could have taken in the circumstances to protect the information from an unauthorised disclosure.

The complainant considered the alleged breaches of the Privacy Act by the respondent were willful and caused a deterioration in the complainant's psychological health. The complainant sought compensation of $20,000 by way of damages for this alleged deterioration (damages claim).

Apology be provided: The Acting Commissioner declared that a written apology be provided by the respondent to the complainant within 7 days of the determination.

Compensation for non-economic loss: The Acting Commissioner was satisfied by evidence from the complainant's psychologist and mother that the complainant had experienced some pain and suffering arising from the privacy breaches of the respondent. The Commissioner considered that an amount of $4,500 was appropriate to compensate the complainant for non-economic loss but aggravated damages were not warranted.

Audit required: The Commissioner decided that an audit was required to ensure the respondent does not repeat the conduct underpinning the breaches of APP 10 and APP 11. Her declaration includes 6 steps and specific timeframes for an audit process for procedures and changes for updating changes to authorities to act.

▶ 'WC' and Chief of Defence Force (Privacy) [2020] AICmr 60 (27 November 2020)

Spent convictions

Remedy: *Declaration ADF engaged in unlawful conduct – non-economic loss: $6,000; reasonably incurred expenses: $4,850.*

This matter was the first determination made by the Commissioner in relation to spent convictions.

WC claimed that the Australian Defence Force (ADF) had breached s 85ZW(b)(ii) of the *Crimes Act 1914* by taking into account convictions that were 'spent' (s 85ZV(2)), or subject to a right of non-disclosure (s 85ZV(3)) in its decision to terminate his appointment.

While the Commissioner was not satisfied the convictions were spent, a right of non-disclosure existed under Queensland law. Although the ADF argued it considered only the conduct underlying the convictions in making its termination decision, the Commissioner found the ADF had taken into account the convictions.

The respondent argued that the exception in s 85ZZH(g) applied as the disclosure was for the purpose of 'assessing appointees or prospective appointees to a designated position'. The Commissioner did not accept the submission as she found no formal determination had been made designating the position for the purposes of the Crimes Act 1914, and the information was used to terminate WC's service, not assess suitability for appointment to, or removal from, the relevant position.

The Commissioner concluded that the ADF had breached s 85ZW(b)(ii).

The Commissioner did not make a declaration requiring the reappointment of WC as she was not satisfied the breach of s 85ZW(b)(ii) caused the termination decision.

The Commissioner made declarations that the ADF pay WC:

- $6,000 for non-economic loss as a result of harm caused by the breach (relevantly feelings of distress, anxiousness and upset)
- $4,850 for reasonable expenses, comprising the full amount of fees incurred to engage a lawyer to review documents and draft a submission in response to the Commissioner's preliminary view.

▶ Flight Centre Travel Group (Privacy) [2020] AICmr 57 (25 November 2020)

APP 1.2 (breach), APP 6.1 (breach), APP 11.1 (breach)

Remedy: *Declarations that the respondent had engaged in conduct interfering with privacy of approximately 6,918 individuals; that the respondent must not repeat that conduct; and that it would be inappropriate for further action to be taken.*

The respondent organised a 'design jam' to create new technologies for travel agents. The respondent provided participants with a dataset that mistakenly included credit card details and passport information of approximately 7,000 customers.

This is the first matter to be determined by the Commissioner arising from an investigation made on the Commissioner's own initiative under s 40(2) of the Privacy Act (with other determinations arising from complaints from affected individuals).

The Commissioner found that the respondent had unlawfully disclosed its customers' personal information to participants, having failed to retain effective control over that information. Notably, participants did not sign non-disclosure agreements and arrangements for the deletion of data post-event were inadequate.

The Commissioner found that the personal information had been disclosed for a purpose other than the primary purpose for which it had been collected (the provision of travel advice and services). The Commissioner did not accept the respondent's submission that it could infer customer consent to the disclosure from the mere provision of a privacy policy.

In any case, consent could not be obtained through the policy because it was insufficiently specific and bundled with other uses and disclosures.

The Commissioner found that the respondent had not taken reasonable steps to protect the information. While the respondent had reviewed samples of the data to check for sensitive information, that review had been insufficient and the dataset inadequately cleansed. Further, she did not accept the respondent's submission that the adequacy of its privacy safeguards was irrelevant as they did not cause the breach. The Commissioner found that the respondent should have implemented better training, compliance checks, assurance processes, and technical controls, and that the privacy protections in place, which should have been 'multi-layered and multi-faceted', fell short of the standard required.

The Commissioner found that the practices/procedures/systems the respondent had adopted to comply with the APPs were not reasonable in the circumstances.

The Commissioner made a declaration acknowledging the breach in view of factors including the seriousness of the incident and the specific and general educational, deterrent or precedential value in making a determination. However, she did not require the respondent to take further steps and noted the respondent's conduct after the breach in voluntarily notifying affected individuals, cooperating with the OAIC investigation, making payment of $68,500 to replace passports, and promptly improving its practices to mitigate against future breaches.