REPORT TO THE FEDERAL COURT OF AUSTRALIA

Report of an Independent Review of action taken by the Federal Court following a data breach contrary to section 91X of the *Migration Act 1958*

Professor John McMillan AO

August 2020

Table of Contents

EXECUTIVE SUMMARY **3**

Recommendations 4

THIS REVIEW **6**

Background to the Review 6

Scope of the Review 7

How the Review was conducted 8

CONSIDERATION OF MATTERS EXAMINED IN THE REVIEW **9**

1. Whether the Court's response to the data breach was timely and appropriate 9
2. The nature, extent and cause of the data breach 17
3. The adequacy of steps taken by the Court to identify individual proceedings or parties that may be affected by the data breach 20
4. The adequacy of steps taken by the Court to identify the cause of the data breach . 21
5. The adequacy of steps taken by the Court to – 22

   □ ensure that the circumstances giving rise to the data breach have been rectified and that proscribed data exposure will not occur 22
   □ implement suitable risk control and oversight mechanisms to prevent proscribed data exposure, and ensure timely identification and response to any data breach that contravenes s 91X 22

6. The adequacy of steps taken by the Court to ensure that staff and officers of the Federal Court and Federal Circuit Court are properly aware of the *Migration Act 1958* s 91X, and of necessary measures to ensure compliance with that section 25
7. The adequacy of steps taken by the Court to consider the application of the *Privacy Act 1988* to the data breach and to the Court's response 26
8. The adequacy of steps taken by the Court to notify and consult the Attorney-General, Attorney-General's Department and other relevant Australian Government agencies about the data breach 29
9. The adequacy of steps taken by the Court to respond to persons (or their legal representatives) who were concerned about whether they may have been adversely affected by the data breach 31
10. Any other matter the Review considers relevant to the Review 34

APPENDIX A **36**

Terms of Reference for this Review 36

APPENDIX B **38**

External Consultations for this Review 38

EXECUTIVE SUMMARY

Section 91X of the *Migration Act 1958* (Cth) provides that a federal court must not publish (in electronic form or otherwise) the name of a person relating to their application for a protection visa or related bridging visa, or to the cancellation of such a visa. To comply with s 91X the Federal Court assigns a pseudonym to protection visa litigants. More than 35,000 pseudonyms have been issued in migration visa proceedings in the Federal Court and Federal Circuit Court since 2001.

The Federal Court became aware in March 2020 that the names of some protection visa litigants who had been assigned a pseudonym could be accessed on the Commonwealth Courts Portal through Federal Law Search (called a 'data breach' in this report).

The Court commissioned this independent review of the circumstances relating to the data breach and the Court's response. The Review was provided with Terms of Reference (Appendix A) and consulted with a range of external parties. Those consulted included professional legal associations, migration legal support services, government agencies, legal practitioners and users of the Court website.

The main findings of this Review are:

- The Court responded to the data breach in a timely and appropriate way. The actions taken included containing and rectifying the data breach, assessing the causes and impact of the data breach, notifying affected individuals and government and non-government bodies, reviewing and changing Court practices and procedures to prevent any future data breach, and making public statements about the data breach and this independent review.

- The actions the Court took in responding to the data breach substantively accorded with its own Data Breach Response Plan and best-practice guidance from the Office of the Australian Information Commissioner (OAIC). Nevertheless, in light of concerns that have been raised about how people first became aware of the data breach, Recommendation 1 proposes that both Courts review their Data Breach Response Plan to include a separate section on notifying affected individuals, stakeholder organisations and the public. The Plan should emphasise that the public announcement of a data breach should be timely, direct and explicit.

- The Court has undertaken numerous projects, and gone to considerable lengths, to identify 1,037 individuals whose names could potentially have been exposed through Federal Law Search contrary to s 91X. Notification letters have been sent to the 1,037 individuals and their legal representatives.

- The Court is confident that it has identified the numerous different ways that a protection visa litigant's name could potentially have been exposed through the Commonwealth Courts Portal in breach of s 91X. The Court has prevented any further data exposure by revising national court practices and procedures for applying pseudonyms and restricting online access to matters in which a pseudonym has been applied. The Court's actions accord with legislative principles and OAIC guidance on securing personal information.

- While recognising an initial need to restrict online access to court information in light of the data breach, the Court acted promptly to restore online access to the extent possible consistently with s 91X. This was done in recognition of the important role of online access in an open justice system, and the practical importance of online access for litigants,

practitioners, government agencies and legal aid and support services. Recommendation 2 encourages the Court to continue managing this issue in a transparent manner.

- The Court has implemented adequate training and other measures to ensure that Court staff and officers are properly aware of the actions required to comply with s 91X.

- The Court has adequately considered the application of the *Privacy Act 1988* (Cth) to the data breach and has responded to an enquiry from the OAIC. The Court has reached a sound view that the Notifiable Data Breach scheme in the Privacy Act did not apply to this data breach, as the activities in question were not of an administrative nature. Although the Court had no statutory obligation to notify the OAIC of this data breach, there can be benefit in voluntarily doing so and the Court's Data Breach Response Plan should be revised to advise of this option (Recommendation 1).

- The Court took adequate steps to notify the data breach and subsequent developments to the Attorney-General and Department, and to consult other government and non-government bodies.

- The Court has been proactive and transparent in notifying the data breach and subsequent developments to legal professional associations and legal representatives. Some practitioners have commented that it would have been better had the Court engaged in prior external consultation about the content of the notification letters and the means of notification. This comment is taken up in Recommendation 1.

- A lingering concern is that it was not the practice of the Court to record the Internet Protocol addresses from which online searches of the Commonwealth Courts Portal were conducted. Consequently, the Court cannot advise any of the 1,037 affected individuals whether their online Court file was in fact accessed. Recommendation 3 recommends that the Court examine the feasibility of implementing a practice of recording that information.

Recommendations

Recommendation 1

The Federal Court and Federal Circuit Court each review their Data Breach Response Plan to include a separate section on notifying a data breach to affected individuals, stakeholder organisations and the public. Matters to be noted include that:

- a public announcement of a data breach should be timely, direct and explicit
- consideration should be given to voluntarily notifying a data breach to the Office of the Australian Information Commissioner, notwithstanding that it is not an eligible data breach under the Data Breach Notification scheme in the *Privacy Act 1988* (Cth)
- consideration should be given to consulting external bodies as to the way that persons potentially affected by a data breach should be notified.

The Privacy Policy of each Court should cross-refer to the Data Breach Response Plan and notification principles.

Recommendation 2

The Federal Court continue to be as transparent as possible in considering the options for restoring public access to migration and appeal matters through Federal Law Search.

Recommendation 3

The Federal Court consider implementing a practice of recording the Internet Protocol addresses from which the Federal Law Search function is used to access documents relating to migration and appeal proceedings in the Federal Court and Federal Circuit Court. The limited purpose for recording that information would be to better enable the Court to assess the potential impact of any data breach relating to that information that occurs contrary to section 91X of the *Migration Act 1958* (Cth).

THIS REVIEW

Background to the Review

This review was commissioned by the Federal Court of Australia (**the Court**) in April 2020 after the Court became aware that personal information may have been accessible from the Federal Court website in circumstances that would constitute a breach of s 91X of the *Migration Act 1958* (Cth).

Section 91X provides that a federal court must not publish (in electronic form or otherwise) the name of a person in a proceeding relating either to their application for a protection visa or related bridging visa, or to the cancellation of such a visa (called a **protection visa proceeding** in this report). The central purpose of s 91X, which was enacted in 2001,[1] is to mitigate the risk that a person who has applied for a protection visa in Australia may face adverse consequences in another country (particularly their country of citizenship) if the fact of their Australian asylum application becomes known. Others, such as family members or associates of a protection visa applicant, may face similar risks if the applicant's identity is known.

The means adopted by the Court to comply with s 91X is to assign a pseudonym to a protection visa litigant (for example, 'AWK16'). The use of the pseudonym means that the Court can disclose and publish information relating to protection visa proceedings instituted in the Court, consistently with the public interest in open justice.[2]

One mechanism adopted by the Court to enable parties and the public generally to access documents relating to proceedings in the Court is to make documents accessible on the Commonwealth Courts Portal (**CCP**) through Federal Law Search. For example, documents relating to a specific protection visa proceeding in the Federal Court or the Federal Circuit Court could be accessed by entering the applicant's pseudonym in Federal Law Search.

It was brought to the Court's notice by a journalist in March 2020 that in at least some instances Federal Law Search could be used to link a pseudonym to the name of a protection visa litigant in either court. This could be done by entering a surname in Federal Law Search that, in some instances, would link to a protection visa proceeding that had been assigned a pseudonym.

The Court took swift action the same day to examine and verify that claim. By close of business the Court disabled online access to information about individual court proceedings while the cause and scope of the issue was examined.

Analysis undertaken within the Court since the initial notification has established that the names of 1,037 individuals who were parties to matters before the Federal Court and the Federal Circuit Court between 2001-20 were potentially accessible through Federal Law Search (described as '**affected individuals**' in this report). Pseudonyms have been assigned to over 35,000 parties in migration protection visa proceedings since 2001.

The online access that could potentially be gained to the names of parties contrary to s 91X is described in this report as a '**data breach**'. Whether the online search functions were in fact used to access the names of parties is not fully known. The CCP did not record online access transactions, and in particular did not record the unique internet protocol (**IP**) addresses from which particular files were accessed.

---

[1] Migration Legislation Amendment Act (No 6) 2001 (Cth).

[2] *Federal Court of Australia 1976* (Cth) s 37AE: 'a primary objective of the administration of justice is to safeguard the public interest in open justice'.

Limited and modified online access and search functions through Federal Law Search have progressively been restored by the Court through March-June. Online access remains disabled for matters with a pseudonym.[3]

The data breach was brought to the attention of the Chief Justices and Chief Executive Officers of both courts on the day the Federal Court learnt of it. Others who were advised in the following days were other Judges, the Attorney-General, the Attorney-General's Department, the Audit Committee of the Federal Court, the Law Council, and the Presidents of the Bar Associations and Law Societies.

The data breach was the subject of a couple of media articles in late March 2020. That was followed by a letter to the Court from the Office of the Australian Information Commissioner (**OAIC**), which has responsibility for administering the *Privacy Act 1988* (Cth). The OAIC letter sought preliminary information about the data breach and how the Court was responding.

The Court also published a notice about the data breach on its website,[4] and responded to some enquiries from legal representatives and advocacy groups.

In late May 2020 the Court commenced writing to the 1,037 affected individuals and legal representatives to notify them of the data breach and steps that might be taken. The providers of legal aid in migration legal matters were also notified.

In April 2020 I was commissioned by the Court to conduct an independent review of the circumstances relating to the data breach and the Court's response. Terms of Reference for the Review were developed and published on the Court's website[5] and are at Appendix A.

Scope of the Review

The Terms of Reference list nine topics that are used later in this report as headings to frame the analysis of the data breach and the Court's response. The topics canvass the nature and cause of the data breach, the notification of the breach to interested parties and government agencies, actions taken by the Court to correct the breach and prevent a recurrence, and privacy law considerations.

I will note two matters that intersect with the data breach but do not fall within the Terms of Reference for this Review.

The impact of a s 91X data breach on a protection visa claim

The s 91X data breach can potentially be raised by an affected individual in proceedings in the Federal Court or the Federal Circuit Court in which the person is challenging the validity of a decision denying them a protection visa. Section 91X and similar privacy considerations have occasionally been raised in Court proceedings (some cases are noted below). However, it principally falls within the judicial function of the courts to deal with matters that are raised in judicial proceedings.

While that aspect of the operation of s 91X is outside the Terms of Reference for this Review, it was nevertheless open to the Review to take notice of this other dimension of the operation of s 91X. For example, this report notes that a step taken by the Court in responding to the data breach was to identify the current proceedings in which affected individuals are parties,

[3] 'Return of Public Search for Migration and Appeal Matters', www.fedcourt.gov.au, News & Events, 20 July 2020.
[4] 'Migration Matters in Federal Law Search', www.fedcourt.gov.au, News & Events, 31 March 2020.
[5] 'S 91X Migration Act Independent Review', www.fedcourt.gov.au, News & Events, 8 May 2020.

and to bring this to the attention of the presiding judicial officers and the Administrative and Constitutional Law and Human Rights National Practice Area of the Court.

The potential relevance of the s 91X data breach to current proceedings in the Court was also a matter raised by practitioners during the consultations for this Review. They stressed the importance of knowing as early as possible whether a party is an affected individual so that consideration can be given to raising the data breach in the proceedings.

The public search function in the Commonwealth Courts Portal

Another matter that is beyond the Terms of Reference is the practices adopted by the Court to enable litigants, the legal profession and the public to access information about Court proceedings through web-based services provided by the Court. Specifically, it is not part of this Review to examine whether online services that were partially disabled following the data breach should be fully or conditionally restored by the Court.

The focus of this Review is only upon whether the Court has taken adequate steps to ensure that online search functions do not result in a breach of s 91X. That issue nevertheless has to be considered in a context that acknowledges the importance of the online search function in the work of the Court. For example, the Federal Law Search link has been accessed on the Court website over 150,000 times in the last 12 months by interested parties that include practitioners, litigants, government and non-government organisations, researchers and journalists. The Court has reported that online access has reduced calls to the Registry by 90%.

The Court is also required by statute to facilitate public searches of court records in two areas:

- The *Admiralty Rules 1988* (Cth), rule 83, requires the Court to provide public access to two registers that it maintains under those Rules – the Register of Caveats Against Arrest (rule 14(1)) and the Register of Admiralty Proceedings (rule 79).

- The *Federal Court (Bankruptcy) Rules 2016,* rule 4.04 (and comparable Federal Circuit Court Rules), requires that a creditor's petition founded on an act of bankruptcy must be accompanied by an affidavit verifying that the records of both courts have been searched to ascertain any prior application in the matter.

How the Review was conducted

The Court provided this Review with a comprehensive range of documents that addressed each of the topics in the Terms of Reference. The documents included project reports, minutes of meetings, internal email correspondence and correspondence with external parties. Direct liaison was maintained with the Court's Privacy Officer/Acting Deputy Principal Registrar, who responded to all questions.

As anticipated in the Terms of Reference, a range of external parties were invited to consult with the Review:[6]

- The Presidents of the Law Council of Australia and the Bar Associations and Law Societies in each Australian jurisdiction. The Law Council and the Law Institute of Victoria both arranged panel discussions with officers and members; and some associations responded that they did not have anything specific to contribute to the Review

[6] The people consulted are listed in Appendix B to the report provided to the Court. I advised the Court of my view that this Appendix not be published as all consultations were private and not part of a public consultation process.

- Commonwealth agencies – the Attorney-General's Department, Department of Home Affairs, Office of the Australian Information Commissioner and Australian Financial Security Authority

- Two refugee support services, and two legal practitioners

- A non-government organisation that is a regular user of the Federal Law Search function.

CONSIDERATION OF MATTERS EXAMINED IN THE REVIEW

This part of the report comprises ten topics:

- Topic 1 sketches the chronology of the Court being notified of the data breach and the Court's immediate and ongoing response. This topic relates specifically to the opening words of item 2 of the Terms of Reference which require the Review to consider whether the Court responded in a timely and appropriate way upon becoming aware of the data breach.

- Topic 2 relates to item 1 of the Terms of Reference which requires the Review to consider the nature, extent and cause of the data breach. This section primarily provides a background explanation of the data breach rather than an analysis of the Court's response.

- Topics 3-9 match the topics that are separately listed in item 2 of the Terms of Reference regarding the adequacy of the Court's response across a number of fields upon becoming aware of the data breach. The headings are in different order to the topics in the Terms of Reference, and two topics have been combined in Heading 5.

- Topic 10 makes some concluding observations, drawn from the stakeholder consultation for this Review, in line with the instruction to the Review to consider any other matter that may be relevant to the purpose or subject matter of the Review.

1. Whether the Court's response to the data breach was timely and appropriate

The Terms of Reference suitably raise 'whether the Federal Court responded in a timely and appropriate way upon becoming aware of the data breach'. This issue is partly discussed under this heading and also under other headings. The discussion commences with a brief chronology that lists the main events in the Court being notified and responding.

Brief chronology of the Court being notified of the data breach and responding

- *20 March* (Friday): the Director of Public Information at the Court received an email at 11.44AM from an ABC journalist advising that he was able to access the names of some protection visa litigants through the Commonwealth Courts Portal. The matter was examined during the day within the Court and discussed with the Court's software vendor. At 4.45PM the matter was brought to the attention of senior officers of the Court, including the Chief Justice, the Acting Chief Executive Officer and Principal Registrar and the

Privacy Officer. Shortly after 5.00PM the Commonwealth Courts Portal and Federal Law Search were taken offline.[7]

- *21-22 March* (Saturday-Sunday): Staff from the Court and the software vendor worked over the weekend to identify the cause of the data breach, the affected files and remedial options. This work continued in following weeks. The Commonwealth Courts Portal was brought back online, and Federal Law Search was modified to prevent the same data breach occurring by removing files with an application type of 'migration' from the name search function.[8]

- *24 March* (Tuesday): the Attorney-General and the Department were informed of the data breach in a forwarded message headed 'Covid-19 update' that had been sent the previous day to all Judges of the Federal Court. On 31 March the Court sent a fuller explanation of the data breach to the Attorney and the Department. The Chief Justice of the Federal Court had earlier and informally notified the Attorney-General of the data breach on 21 March.

- *27 March* (Friday): the Court provided a statement to the ABC, noting there had been 'a major systemic failure'.

- *27 March*: the Court advised the Australian Bar Association, the Law Council of Australia and the Bar Associations and Law Societies in each State and Territory, of the data breach in an email update that was being sent regularly on COVID-19 developments. The data breach was also noted in updates on 31 March and 1 April.

- *31 March* (Tuesday): the ABC published an online article headed 'Federal Court data breach sees names of protection visa applicants made public'.[9] The article referred to a 'catastrophic data breach that potentially puts asylum seekers at risk of harm' and a 'major systemic failure'. The article quoted a migration lawyer who said that he had repeatedly raised the issue with the Court, with varying levels of success. The data breach was also the subject of another online article on 2 April in CSO online[10] that queried whether the Court had adequately complied with privacy requirements.

- *31 March*: later the same day the Court published a notice on its website advising of the data breach, headed 'Migration Matters in Federal Law Search'.

- *1 April*: the OAIC wrote to the Court making preliminary enquiries about the data breach under s 42(2) of the Privacy Act. The Court acknowledged the OAIC's enquiry on 8 April, and responded substantively on 17 April advising that in the Court's view the Data Breach Notification scheme in the Privacy Act did not apply to this particular data breach.

---

[7] Described in internal Federal Court report, titled: *Project Report PR-1: Preventing any further immediate disclosure.*

[8] Described in *Project Report IT-10: Commonwealth Courts Portal change to exclude Migration Files from Federal Law Search.*

[9] https://www.abc.net.au/news/2020-03-31/federal-court-in-protection-visa-data-breach-published-names/12102536

[10] '"Major systemic failure" on privacy – again – by Federal Court of Australia', https://www.csoonline.com/article/3535589/major-systemic-failure-on-privacy-again-by-federal-court-of-australia.html

- *1-3 April*: the Court made additional restrictions and modifications to the public search functions on Federal Law Search to exclude Appeal matters, and to disable the name search feature for non-registered users.[11]

- *3 April*: the first regular meeting was held of a Court-established '91X Non-Compliance Working Group'.

- *8 April*: a paper on the data breach was presented to a meeting of the Audit Committee of the Court; and again at a subsequent meeting on 17 June.

- *27 April*: I was appointed by the Court to conduct an independent review of the data breach and the Court's response.

- *18 May*: the public search function in Federal Law Search was re-enabled for Bankruptcy, Admiralty and Native Title matters; an announcement was placed on the Court website.[12]

- *22 May*: the Court commenced notification of affected individuals and legal representatives; this project was completed by 11 June.

- *25 May*: the public search function in Federal Law Search was re-enabled for all areas except Migration and Appeals.[13]

- *20 July:* the public search function in Federal Law Search was re-enabled for Migration and Appeals except those with a pseudonym.[14]

Assessment and commentary

The importance of a timely and appropriate response to a data breach is spelt out in the Federal Court's 'Data Breach Response Plan' (**Response Plan**), adopted in June 2018 and published on the Court website.[15] The Response Plan observes that a data breach can result in serious harm to individuals and can damage the reputation of the Court. (The Plan also notes the Notifiable Data Breach (**NDB**) scheme in Part IIIC of the Privacy Act, discussed below.)

The main elements of the Response Plan as it applies to this data breach are:

- A Court staff member who is aware of an unauthorised disclosure of personal information held by the Court should immediately report this to a supervisor and prepare and forward a 'Data Breach or Suspected Data Breach Incident Report' to the Privacy Officer of the Court.
- Any immediate step that can be taken to contain the data breach and limit further unauthorised disclosure of personal information should be taken, consistently with not compromising essential Court systems or information.

---

[11] Described in *Project Report IT-11: Commonwealth Courts Portal change to exclude Appeal Files from Federal Law Search* and *Project Report IT-12: Commonwealth Courts Portal change to further restrict search feature to parties to a file.*

[12] 'Return of public search for Bankruptcy, Admiralty and Native Title', News & Events, 18 May 2020.

[13] 'Return of Public Search for all Matters excluding Migration and Appeals', News & Events, 25 May 2020.

[14] 'Return of Public Search for Migration and Appeal Matters', www.fedcourt.gov.au, News & Events, 20 July 2020.

[15] The Federal Circuit Court adopted an identical Data Breach Response Plan in June 2018.

- The Privacy Officer, upon receiving the Incident Report, must inform the Data Breach Response Team, which comprises senior Court administrative officers.
- The Privacy Officer must undertake an expeditious assessment of the data breach and prepare a draft report that takes account of the circumstances of the data breach, personal information that may be affected, the nature of the harm to affected individuals, remedial action that can be taken to remove the harm, whether notification to affected individuals is required or desirable, and any recommendations regarding personal information handling within the Court.
- The Response Team, as part of undertaking a thorough review of the data breach, is to consider and finalise the draft report prepared by the Privacy Officer and provide it to the Chief Executive Officer/Principal Registrar of the Court.

Even though Privacy Act requirements may not apply to this particular data breach (discussed under Heading 7 below), the NDB scheme in the Privacy Act and the OAIC supplementary guidance are nevertheless a helpful backdrop in independently assessing the adequacy of the Court's Response Plan and actions.

The NDB Scheme has a limited application to 'eligible data breaches' occurring in entities to which the Privacy Act applies. An eligible data breach includes the loss or unauthorised access to or disclosure of personal information that could result in 'serious harm' to an individual (Privacy Act, s 26WE). A data breach of that kind must be notified as soon as practicable to the OAIC and to each individual who is at risk, providing information about steps that could be taken in response (ss 26WL, 26WK). The data breach is to be notified on an entity's website if it is not practicable to notify each relevant individual.

An OAIC guidance publication, *Data Breach Preparation and Response* (2019), spells out principles to be observed both in the NDB Scheme and in other circumstances. A key message is that there is no single way of responding to a data breach; each breach should be dealt with on a case-by-case basis and tailored to the risks posed by the breach (p 18). Generally, four steps should be followed in responding to a data breach:

- containing the data breach to prevent further compromise of personal information
- assessing all aspects of the data breach, including causes, risks, potential damage and remedial options
- notifying individuals and the OAIC
- reviewing the incident, to prevent further data breaches and improve the organisation's personal information security and handling practices.

The OAIC guide explains that notification to the OAIC and individuals is an important mitigation strategy that can serve many purposes (p 21). Notification can explain how the organisation is handling the data breach; instil reassurance that the organisation takes privacy protection seriously; and assist individuals to take protective action. Overall, the OAIC expectation is that a notification statement 'will include sufficient information about the data breach to allow affected individuals the opportunity to properly assess the possible consequences of the data breach for them, and to take protective action in response' (p 52).

Another privacy framework document that applies to some functions of the Federal Court is the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, made by the Australian Information Commissioner. The Code does not contain any specific guidance on handling data breaches.

The actions the Federal Court took following notification of the data breach did not conform precisely to the steps outlined in the Court's Response Plan. The explanation appears to lie

in early recognition within the Court of the potential scale and significance of this data breach and the need for an urgent and tailored response. This is consistent with the OAIC's best practice guidance.

The actions the Court took appear to have met the substance of the requirements of the Response Plan and general principles relating to data breach notification. Among the actions the Court took were:

- The notification received from an ABC journalist was promptly shared among several Court staff (including the Chief Information Officer) who examined the potential breach, discussed it with the Court software vendor and notified the Privacy Officer and other senior personnel later the same day.
- The Court's online services that allowed the data breach to occur were disabled approximately 15 minutes after the report to the Privacy Officer.
- A deep analysis of the cause and extent of the data breach commenced the following morning (a Saturday) and has continued for many weeks. A large number of Registry staff around Australia have participated in analysing the impact of the data breach. The analysis has been fully documented in several Project Reports. There has been regular reporting on the matter to senior personnel, including the Chief Justice and the CEO/Principal Registrar.
- There was external notification of the data breach in various ways that included a notice being posted on the Court website, and emails being sent to the Attorney-General and the Department, and to legal professional associations. The notice on the Court's website gave helpful information about the nature and scale of the data breach, how it was caused, and the remedial action both already taken by the Court and underway.
- The Court responded to a few direct queries it received from the media and legal practitioners and bodies.
- Online search functions have gradually been restored, but with some modifications and limitations to prevent the same data breach occurring.
- The Court has identified as many as 1,037 people who were potentially affected by the data breach, and has sent letters to those people and their legal representatives with information about the data breach and steps they might consider taking.
- Consideration is being given within the Court to action that might mitigate potential adversity to affected persons, such as assigning new pseudonyms and case numbers to those persons. Judges of the Court have been advised of affected individuals who are parties in current matters listed before them.

A few aspects of the Court's response warrant discussion.

Internal notification of the data breach: On the day the Court was notified of the data breach there was a five hour delay in notifying the Privacy Officer and other senior personnel. It appears that this delay was understandable in context, as the time was spent interrogating the online Court systems, consulting the Court's software vendor, exploring the scope of the issue, ascertaining if previous reports had been logged, and exploring options for preventing ongoing disclosure consistent with maintaining the functionality of the Court's online functions.[16] The officers were then well-placed to provide a fuller internal briefing. This led to the Court's online systems being disabled within a matter of minutes of the briefing.

Public notification of the data breach: The Court's first public statement about the data breach was on Tuesday 31 March when a notice was published on the Court website in a link

[16] The steps taken on 20 March 2020 are described in *Project Report IT-1: Preliminary Investigation*.

headed ‘Migration matters in the Commonwealth Courts Portal’, that linked to a statement headed ‘Migration Matters in Federal Law Search’.

The ABC online article – ‘Federal court data breach sees names of protection visa applicants made public’ – was published earlier the same day. The ABC article followed a journalist’s enquiry to the Court on Friday 20 March, and a Court statement to the ABC on 27 March (that was briefly noted in the ABC article).

Most of the people to whom I spoke about the data breach said they learnt about it from the ABC article. The OAIC letter to the Court on 1 April making preliminary enquiries about the breach was triggered by the ABC article. So, too, were a couple of the enquiry letters the Court received from refugee advocacy services.

The Court has been transparent about the data breach, and took early action to respond to the ABC enquiry and to bring the data breach to the attention of others. This was done at a time when the scale of the problem was still unresolved internally.

It is probable that a newspaper story about a data breach is more likely to be noticed publicly than, for example, a statement on an agency website. Nevertheless, an agency will be better placed to reassure others that it is committed to privacy protection if it can point to action that was earlier taken to publicly disclose the data breach. A central purpose of proactive data breach notification by an agency is to alert those who are potentially affected so that they can consider whether pre-emptive action is necessary to safeguard their interests.

Viewed in that light, it is unfortunate that the Court did not post its website statement earlier than the ABC article, and that the title of the statement was not explicit that a data breach had occurred. This is a relatively minor matter in the context of the potential scale and impact of this particular data breach and how the Court has responded to it. The timing of the Court’s disclosure should nevertheless be noted as a source of temporary concern to some people.

This issue is taken up in **Recommendation 1** – that the Federal Court and Federal Circuit Court each review their Data Breach Response Plan to include a separate section on notifying a data breach to affected individuals, stakeholder organisations and the public.

The Response Plans do not presently deal with notification, other than to observe that a draft assessment report prepared by the Privacy Officer on a data breach incident should consider ‘whether notification is required pursuant to the NDB scheme or is otherwise desirable’. Recommendation 1 notes that a public announcement of a data breach should be timely, direct and explicit; and that the option of voluntarily notifying the data breach to the OAIC should be considered (discussed below under Heading 7).

Recommendation 1 also notes that the Privacy Policy of each Court should cross-refer to the Response Plan.

Posting individual notification letters to affected persons: There was an eight week delay in notification letters being sent to affected individuals and their legal representatives. The generally accepted – but elastic – timeframe for notifying a data breach is that stated in the Privacy Act, namely ‘as soon as practicable’ after a statement explaining the data breach has been prepared (s 26WL(3)).

The Court’s stated intention in its early external communication about the data breach was to notify individuals much earlier than occurred. For example, the Court’s letter to the OAIC on 17 April advised that the notification of individuals who were affected by the data breach ‘will commence this week’. When that forecast was made the Court expected that fewer than 500 people would be notified (as the Court had advised the legal profession in an email on 31

March). The number of affected individuals later grew to 1,037. That explains in part why a delay occurred. Another contributing factor to the delay was the need to ascertain the addresses for notifying either a litigant or their legal representative. The large number of notification letters were mostly sent simultaneously.

In the circumstances, I believe the Court has posted the individual notification letters within a reasonable timeframe. Public notification of the data breach had occurred much earlier when a notice was published on the Court website on 31 March and emails were sent to legal professional associations on 27 and 31 March and 1 April.

The content of the Court's website notification: The statement published on the Court's website on 31 March explained several matters:

- the nature of the data breach – 'a major systemic failure' had occurred whereby the names of some parties who had been assigned a pseudonym could be seen in the Federal Law Search section of the Commonwealth Court's Portal if a user entered a common family name and clicked the 'migration' category
- the multiple causes of the data breach – these were registry process issues stemming from how documents are described at the time of filing
- the number of cases affected – approximately 400, with work underway to identify other possible cases
- the Court's response – online search functions had been disabled while work was underway to modify search functions and registry processing procedures
- further notification – 'To the extent possible, parties known to be affected by the breach (and their lawyers where relevant) will be informed by the Court of the breach'.

As that summary indicates, the Court's statement gave specific and helpful information about the data breach. (I have commented above that the heading on the statement did not explicitly alert people to the fact that it was a statement about a data breach.)

The essential requirements for an effective data breach announcement were also met if viewed in the context of the notification requirements in the NDB Scheme in the Privacy Act. The Act requires an entity that is aware of a data breach to which the Act applies to prepare a statement setting out the name of the entity, a description of the data breach, the kinds of information concerned, and recommendations that individuals could take in response to the data breach. The statement is to be provided to the OAIC (s 26WK) and, if practicable, to each individual who is at risk from the data breach (s 26WL).

The OAIC supplementary guidance on that requirement explains that the recommended steps for individuals may include an explanation of the protective steps already taken by the entity.[17]

The content of the Court's notification to individuals: The letter of notification that the Court sent to 1,037 individuals potentially affected by the data breach is discussed below under Heading 9. The discussion notes that the notification was informative, but has attracted some criticism from legal representatives to whom I spoke.

Realisation within the Court of the data breach: The Court's public announcement of the data breach on 31 March commented that it 'recently became aware of a major systemic failure'. The implicit reference in that statement is to the email the Court received from an ABC journalist on 20 March. A similar comment about 'recently becoming aware' was also made by the Court in other information and notification statements.

[17] OAIC, *Data Breach Preparation and Response* (2019) at p 50.

A question arising is whether the Court was earlier made aware of circumstances that put it on notice of the data breach but had failed to act on that knowledge. For example, the ABC online news article on 31 March referred to a migration lawyer to whom the ABC had spoken and said: 'he has repeatedly drawn the attention of the court to the data breach in individual cases, but the Federal Court failed to grasp the systemic nature of the problem and, as [a] consequence, did not act to fix the problem'. Similarly, a couple of respondents to a Law Council survey (discussed below under Heading 9) commented that disclosure of information identifying protection visa litigants was known for some years to be a problem with the Court's website.

This is an important matter, but more for noting than for extended exploration as part of this investigation. The Court is now better apprised of the matter, having identified a few instances in which s 91X issues had earlier been raised but not treated at the time as pointing to a 'systemic weakness' in court processes. For example, in three cases in February 2020:

- A legal representative contacted a Judge's Associate and a Legal Case Manager to advise that his client's name was accessible in relation to an appeal currently before the Judge. The cause of the error was identified and corrected the same day. The issue exposed in this case was taken up again after the data breach was notified on 20 March.

- A Judge advised the Registrar that a party had sought an adjournment on the basis of their name being accessible from the Electronic Court Portal. The National Registrar Migration followed up on 12 March by sending an email to other registrars, headed 'Compliance with s 91X of the Migration Act'. The email advised that a s 91X breach had been detected in a few recent cases in which litigants in appeal cases had wrongly entered their actual name in eLodgment. In each of those cases, Registry staff had checked and corrected the file title but not the cause of action title, which could be viewed through the Commonwealth Courts Portal. The National Registrar's email provided advice on managing pseudonyms and on checks and corrective action required of Registry staff to ensure there were no inadvertent breaches of s 91X. The email was raised with or forwarded to Registry staff around Australia on the same day.

- A legal representative wrote to the Court seeking a suppression order on the basis that an applicant's date of birth had been disclosed in two consent orders made a couple of years earlier by a Registrar. The representative was advised to apply for an interlocutory order in the current proceedings.

In none of those instances did the Court ignore the concern that was raised about disclosure of identifying information of a protection visa litigant. On the other hand, one or other of those instances, if assessed differently or discussed more broadly at the time within the Court, might reasonably have alerted the Court to the systemic problems relating to s 91X. The systemic problems were brought to a head in the following month and have led to an extended and searching analysis of affected cases and of the steps necessary to prevent further data breaches contrary to s 91X.

There is little more that needs to be said at this stage other than that examples of this kind illustrate in hindsight that individual problems can point to larger issues. That is a particularly important perspective in relation to s 91X, as it imposes a duty on the Court not to disclose the name of a protection visa litigant. It is vital that the internal processes of the Court are attuned to that statutory duty and to the risk of s 91X being inadvertently breached by small lapses in administrative procedure. This point is further discussed below under Heading 6,

where it is noted that the Court has implemented procedures to ensure that staff are alert to the broader implications of a potential s 91X breach.

A matter to note briefly is that s 91X and related issues have also been addressed in published decisions of the Court. Several of those cases are discussed in *AVN20 v Federal Circuit Court of Australia* [2020] FCA 584.[18] The applicant in that case sought relief on the basis that the published reasons of the Federal Circuit Court contained an extract from a document filed in the proceedings that included a party's name. In refusing relief, the Federal Court noted that the s 91X breach in the Federal Circuit Court did not constitute jurisdictional error by that Court. Kenny J observed (at para 108):

> Section 91X creates a duty of imperfect obligation. Courts to which the prohibition is directed are under a duty not to publish the names of certain persons in relation to the proceedings to which the prohibition applies. The statutory obligation in s 91X does not support the conclusion that the Parliament intended that a court's failure to comply with the prohibition in the provision would invalidate the judgment of the court. Section 91X does not withdraw jurisdiction from the court on account of a breach on its part of the prohibition in s 91X.

Her Honour noted other avenues that may be available to a person who is affected by a breach of s 91X – for example, applying to the Minister under s 48B of the Migration Act for permission to make a fresh protection visa application (see also *WZAUP v Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs* [2020] FCA 116, and the discussion below under Heading 8).

Three other aspects of s 91X that have been dealt with in decisions of the Court include:

- The Court may make a suppression or non-publication order under s 39AF of the *Federal Court of Australia Act 1976* (Cth) to prevent a breach of s 91X or the publication of personally identifying information (*AWU15 v Minister for Immigration and Border Protection (No 2)* [2019] FCA 2132).

- Section 91X applies only to the publication of a person's name and not other personally identifying information (*EAU17 v Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs* [2019] FCA 2086).[19]

- In preparing reasons for decision in cases to which s 91X applies, courts should be careful not to include details that might identify a person and therefore frustrate the purpose of s 91X (*MZABP v Minister for Immigration and Border Protection* [2016] FCAFC 110 at [5]).

2. The nature, extent and cause of the data breach

This section gives a background explanation of the data breach. The Court's response is discussed later in this Report.

The position in summary is that the Court's understanding of the nature, cause and extent of the data breach has changed during the course of the Court's investigation. The Court has, progressively, identified multiple ways that the name of a person assigned a pseudonym could

[18] See also *BBE15 v Federal Circuit Court of Australia* [2020] FCA 965.

[19] Cf Migration Act s 48B(4) which provides that a statement tabled by the Minister in Parliament under that section 'is not to include: (a) the name of the non-citizen; or (b) any information that may identify the non-citizen'; and s 431 which provides that a statement of reasons by the Administrative Appeals Tribunal in a migration review proceeding must not 'identify an applicant or any relative or other dependant of an applicant'.

potentially be visible through Federal Law Search. Correspondingly, more names were potentially accessible than initially thought.

The starting point for explaining the data breach is that the Court maintains a National Pseudonym Register for protection visa proceedings commenced in both the Federal Court and the Federal Circuit Court.

A pseudonym will be assigned to a case to which s 91X applies if the initiating application is filed over the counter or by facsimile. Most proceedings are in fact commenced and managed by registered users through eLodgment, which is the online document filing service. Parties are advised to obtain a pseudonym from the Court before eLodging. The pseudonym assigned to a matter is then to be used on all documents subsequently filed in the same matter. eLodgment automatically populates data from documents that are accepted for filing into CaseTrack and the electronic court file (**ECF**).

Documents that are lodged over the counter – for example, by litigants in person – can be entered into eLodgment by the Registry. The pseudonym procedures are followed before this is done.

The ECF contains several fields in which the name (or pseudonym) of a party will be visible through a Federal Law Search on the CCP. This includes the *File title, Cause of Action* level, and *Parties for this Action* section. Procedures were in place to ensure that the pseudonym would be recorded or pre-populated in those fields in matters to which s 91X applies. Correspondingly, a Federal Law Search for a particular matter that had been assigned a pseudonym would reveal only that identifier.

Different arrangements existed for online access searches through the CCP for registered users and members of the public. A registered user who was a party to a proceeding could access all documents in that proceeding, unless the document was confidential or access was restricted. A member of the public – which may include interested parties such as advice and support services, government agencies and legal practitioners who are not representatives in the proceeding – could obtain information about court events, a list of documents filed by the parties, the names of parties and lawyers, orders of the Court and links to judgments

The Court has ascertained several different ways in which a breakdown in the pseudonym procedures could result in a protection visa litigant's name being left in a visible section of the ECF and being exposed through Federal Law Search. Exposure would occur if the searcher entered a surname, selected the 'migration' application type, and the search returned names that included the name of a protection visa litigant who had been assigned a pseudonym.

Following are the several different ways identified by the Court that could lead to a protection visa litigant's being entered in a field that would be visible through a search of that nature:

- If the Registry identified that a pseudonym was required for a matter initiated in the name of an applicant, a change was required at the File Title and Cause of Action levels. If a change was made only at the Cause of Action level, a Federal Law Search using the applicant's name would reveal that name at the File Title level.

- If the Registry end-dated rather than deleted a name that was used in an initiating application, a Federal Law Search would reveal that name at the File Title and Cause of Action levels.

- Although a matter may be listed under a pseudonym, supplementary documents lodged by a party during the course of the proceeding may name the applicant or a new party.

These documents were placed in a special queue in eLodgment that identified that a new party had been added to a matter. If a document was accepted without amendment, the party's name would be revealed during a Federal Law Search of the matter.

- The name of a party may have been wrongly listed in the field for entering the name of the party's legal representative.

- The relevance of s 91X (and the need for a pseudonym for a party) may have emerged during the course of a proceeding, yet no order was made for a pseudonym to be applied.

- A file created in error may have been voided, but a party's name exposed in the meantime.

- A record may have been amended to substitute a pseudonym for the name of a party, but the party's name may have been exposed in the meantime.

- The name of a party may have appeared in an order that was available through Federal Law Search.

- A matter that requires a pseudonym may have been commenced in the name of an applicant. All matters are scrutinised by the Registry before they are accepted for lodgment to check if a pseudonym is required. The Court has identified a few instances in which the need for a pseudonym was overlooked or the pseudonym was not applied correctly.

Four themes run through those various breakdown points in the Court's procedures:

- there are various pathways through which information (including a person's name) can be entered into the ECF, by either a party or the Court Registry or during the course of proceedings
- the CaseTrack system is complex, including for amending entries in the ECF
- there can be disparate regional practices in applying the Court procedures
- it is clear in the great majority of cases if a matter requires a pseudonym (notably applications for judicial review of protection visa decisions of the Immigration Assessment Authority and the Administrative Appeals Tribunal), but it is not readily apparent in some other cases (for example, judicial review of a refusal or cancellation of a protection visa on character grounds, or of a decision on an application for Ministerial intervention under s 417 of the Migration Act).

The Court has applied pseudonyms in more than 35,000 migration visa proceedings since 2001. The Court has ascertained that a party's name is visible in the ECF and could potentially have been exposed through Federal Law Search in 1,037 instances. Individual notification letters have been sent to each of those parties or their legal representatives.

The Court's initial analysis on 21-22 March identified 428 files in which a protection visa litigant's name could appear in the Federal Law Search result (78 files in Federal Court matters, and 350 in Federal Circuit Court matters). These were the numbers the Court cited in its early external communications about the data breach. The Court's subsequent work has identified the numerous different ways that a protection visa litigant's name could be exposed. This has led to the increased number of affected individuals.

3. The adequacy of steps taken by the Court to identify individual proceedings or parties that may be affected by the data breach

Actions taken by the Court

The Court has undertaken several projects to identify files in which a protection visa litigant's name could be exposed during a Federal Law Search:

- Over the weekend of 20-21 March, a joint project by the (internal) IT Business Applications and the (external) Datacom Incident team developed and ran search query scripts to identify electronic court files (among the more than 35,000 pseudonym matters) in which a protection visa litigant's name could appear in the Federal Law Search result.[20] The project identified 428 files, of which 360 had data issues that were manually rectified that weekend. The project also resolved that further scripts would need to be developed to capture other possible cases.

- A project was conducted the following week (23-30 March) using different scripts to identify proceedings at the File Level between 2015-2020 that were potentially affected by the data error.[21] This identified 187 files in which the name of a party was exposed on 215 occasions, and a further 41 files in which it was potentially exposed on 42 occasions. The project generated a spreadsheet list of files to be checked by Registry staff for potential exposures and rectification.

- A supplementary project was conducted on 31 March to identify files at the Cause of Action Level between 2015-2020 that were potentially affected by the data error and to generate a spreadsheet list of matters to be checked and rectified by Registry staff.[22] The project identified that there were records which had never had a pseudonym applied but which could not be identified through a technical search.

- A project conducted on 8-9 April applied the same search functions as in the previous two projects to identify files at the File Level and Cause of Action Level for the period 2004-14 that were potentially affected by the data error. The project generated spreadsheets for Registry checking and rectification.[23] This project also identified that there were records which had never had a pseudonym applied but which could not be identified through a technical search.

- A project conducted on 14 April was the same as the preceding project, for files in the period 1996-2003.[24]

- Commencing on 31 March, Registry staff have manually checked the matters listed in the spreadsheets generated by the preceding projects, to identify if a file exposed the name

[20] Described in *Project Report IT-2: Issue Investigation and Root Cause Analysis*, and *Project Report IT-3: Scripts run to identify potential exposures at File Level.*
[21] Described in *Project Report IT-4: Scripts run to identify affected proceedings at File Level 2015-2020.*
[22] Described in *Project Report IT-5: Scripts run to identify potential exposures at Cause of Action (COA) level 2015-2020.*
[23] Described in *Project Report IT-6: Scripts run to identify potential exposures for the years 2004 to 2014 for combined File and Cause of Action (COA) checks.*
[24] Described in *Project Report IT-7: Scripts run at File and Cause of Action level to identify potential exposures for the years 1996-2003*.

of a litigant and required rectification.[25] The spreadsheets listed 6,553 matters to be checked (with some duplication of matters). This project was undertaken by experienced Registry staff who were given special training for the project, to ensure consistency of results and because of the complexity of CaseTrack. The matters that were identified as requiring rectification were checked by Team Leaders and experienced client service officers. An added complexity in the project, relating to pre-2015 records, was that a name listed as a legal representative had to be checked to ensure that the person was not also the pseudonym applicant. A similar confirmatory check had to be made relating to respondents (eg, a Tribunal member) who appeared on multiple files.

- A supplementary project was established to review the judgments and orders in the 35,000 matters to which a pseudonym had been assigned to identify whether the protection visa litigant's name was exposed, and if so how an amendment could be made.

- Three quality assurance projects commenced in March/April. One aimed to identify if there were any integrity issues with the Pseudonym Register. Another aimed to rectify all data errors in CaseTrack. A third, which is ongoing, is a daily quality assurance check on all data entered into CaseTrack in respect of Migration matters, in particular to ensure that a protection visa litigant's name is not exposed.[26]

Assessment and commentary

On the information provided, it appears the Court has adequately examined its existing records to identify those in which the name of a protection visa litigant could potentially have been exposed during a Federal Law Search – that is, to identify the names of affected individuals.

The Court has undertaken numerous projects, using various search methods, to examine the electronic court files for all proceedings commenced between 1996 and 2020 in which a pseudonym was applied, to check if the name of a protection visa litigant was exposed. The search has gone beyond the original parameters of the data breach to check if a name was exposed as a consequence of other events or actions in the Court. Files have been rectified when necessary to ensure there is no continuing breach of s 91X.

This work was undertaken by experienced Registry staff who received specific training for the task. For example, the training included screenshots of the multiple actions that may be required in CaseTrack to ensure that only a pseudonym and not a party's name is exposed in the ECF.

4. The adequacy of steps taken by the Court to identify the cause of the data breach

Actions taken by the Court

The specific activities and projects the Court has initiated to identify the cause of the data breach are discussed under other headings in this Report. Common features of those specific measures include the following:

- There has been close involvement and collaboration from 20 March onwards between the (internal) IT Business Application Support Team and the (external) Datacom Incident Team.

[25] Described in *Project Report R-1: Identification of affected proceedings and rectification*.
[26] Described in *Project Report IT-8: Script to check files with Pseudonyms for COA Tile and File Title Check*, and *Project Report IT-9: Export of Pseudonym Register for Data Integrity Checks*.

- The Court established a s 91X Non-Compliance Working Group that is convened by the CEO/Principal Registrar of the Court and includes other senior officers responsible for registry, corporate, financial, legal and court and tribunal services. The Working Group commenced meeting on 3 April and has since met regularly, holding 11 meetings in the following 12 weeks.

- The Working Group has oversighted several projects that are separately recorded in Project Reports that identify the objective and scope of each project, how and by whom the project is to be undertaken, and the outcome (many of the project reports are referenced in footnotes in this report).

- Numerous electronic and manual search and checking methods were used to identify affected individuals among more than 35,000 files. This has involved double checking many files, at both operational and supervisory levels in the Court. The potential breach incidents have been examined by senior Registry officers within the National Migration Team to identify underlying causes and systemic issues.

- The Judicial Registrars are advised each day of matters that are newly filed and whether any data entry errors occurred.

Assessment and commentary

The Court is confident that it has identified the numerous different ways that a protection visa litigant's name could potentially be exposed through the CCP in breach of s 91X. The initial understanding of how a data breach could occur has given way to a more comprehensive and penetrating understanding of potential causal elements for data breaches. On the information provided, it appears this matter has been adequately handled by the Court.

The Court has prevented any further data exposure by revising national court practices and procedures for applying pseudonyms and by restricting access through the CCP to migration and appeals matters in which a pseudonym has been assigned. A project is underway in the Court to examine the options for re-enabling public access in a way that does not compromise compliance with s 91X.

5. The adequacy of steps taken by the Court to –

- **ensure that the circumstances giving rise to the data breach have been rectified and that proscribed data exposure will not occur**

- **implement suitable risk control and oversight mechanisms to prevent proscribed data exposure, and ensure timely identification and response to any data breach that contravenes s 91X**

Actions taken by the Court

The Court has implemented a range of projects, covering different functional areas, to ensure current and future compliance with s 91X. Many of the projects have been coordinated by the 91X Non-Compliance Working Group.

Projects undertaken within the Court that are specifically relevant to both Terms of Reference include the following:

- Federal Law Search was disabled on 20 March when the Court was notified of the data breach. By 25 May, all public search functions were progressively re-enabled with the exception of migration matters and appeals – which covers all matters to which s 91X applies and in which a pseudonym is used. Registered users have access to all documents in proceedings in which they are a party (other than confidential and restricted files).

- A project within the Court examined the options for re-enabling public access in migration and appeals, consistently with the principle of open justice but taking account of the statutory confidentiality requirement imposed by s 91X. The main options canvassed were:[27]
    - Permanent removal of non-party access to all appeals and migration matters through Federal Law Search; non-party access would require a file inspection request to the Court.
    - Re-instatement of public access to non-migration appeal matters; a file inspection request would be required for non-party access to all migration visa matters
    - Re-instatement of public access to all appeals and migration matters except those in which a pseudonym was assigned; re-instatement of either public or restricted access to those matters would be examined further.

  As at 20 July the Court had implemented option 3

- All open matters in the Federal Court and the Federal Circuit Court were reviewed for s 91X compliance, and in particular to identify those in which a pseudonym should have been used and to correct any errors.[28] This involved a review of more than 12,000 open matters in the Federal Circuit Court and 750 in the Federal Court. The review identified only 10 matters in the Federal Circuit Court that may have been non-compliant.

- A 'mop-up' review of all migration files was conducted to ensure that pseudonym details were correctly entered.

- A daily quality assurance check/audit is conducted of all new matters in which a pseudonym is entered into CaseTrack to ensure that data was correctly entered in compliance with s 91X. Similarly, a daily audit is conducted to identify any data inconsistencies in CaseTrack that could allow exposure of a litigant's name (such as inconsistency between the File Title name and the Cause of Action name). These audits are reported daily to the Migration Judicial Registrars to ensure that errors are rectified and that systemic issues and staff training needs are identified.

- The eLodgment portal has been enhanced to advise users of the procedures to be followed to obtain a pseudonym prior to lodgment of an originating document. This is supplemented by system-generated correspondence containing advice for protection visa litigant applications.

- A protection visa case descriptor note (or s 91X identifier) has been created for use in CaseTrack, to support special management mechanisms for protection visa matters.

[27] Described in internal paper, 'Federal Law Search – Restoration of Public Access'.
[28] Described in *Project Report: Manual and NORS Review of Open Matters for 91X Compliance.*

- A mandatory check box to identify whether a matter is a protection visa proceeding has been added to the originating forms for Federal Court and Federal Circuit Court proceedings.

- A review was undertaken of orders made in current listed matters in both courts that were potentially affected by the data breach to identify if the order contained personally identifying information in breach of s 91X. Rectification was required in 16 matters. Consideration is being given to extending this review to the judgments and orders in the more than 35,000 matters to which a pseudonym has been assigned since 2001.

- Judges of the Courts were notified of current matters listed before them that were potentially affected by the data breach.

- Parties are advised, upon request, that a new pseudonym and file number can be issued in a current proceeding by making an application to the presiding judge in the matter, who may make an appropriate order.

Other structural changes recently implemented in the Court have also been tailored to ensure that protection visa litigation is handled in compliance with s 91X.

A new Court database was already in development when the data breach occurred – the National Operations Registry Information Systems database (**NORS**). An objective of the NORS project was to introduce additional categorisation, case management and reporting tools for migration matters in the Federal Court and the Federal Circuit Court. A decision was made following the data breach to prioritise further development of the NORS database so as to better support s 91X compliance.[29]

Another change was the formation of a specialist National Migration Team, comprising the Migration Judicial Registrars and support staff, to deal exclusively with all aspects of migration matters in the Federal Court and Federal Circuit Court. One responsibility of the Registrars (noted above) is to oversight the daily audit of newly entered matters to ensure that no data processing errors have occurred.

Assessment and commentary

The Australian Privacy Principles in the Privacy Act may not directly apply to this aspect of Federal Court practice and procedure. The APPs nevertheless provide constructive guidance on the steps that organisations are expected to take to ensure that personal information is securely protected. *APP 11 – security of personal information*, provides in part that an entity 'must take such steps as are reasonable in the circumstances' to protect personal information from 'unauthorised access … or disclosure'.

The *Australian Privacy Principle* Guidelines, promulgated by the Information Commissioner, explain that the requirement to take 'reasonable steps' depends on the circumstances of each matter. Factors to be considered include: the nature, size and resources of the entity; the amount and sensitivity of the personal information that is held; the possible adverse consequences of a security breach; and the practical steps required to secure the information (para 11.7). Reasonable steps may require procedures and systems to safeguard the physical security of information, to control access, manage internal information handling, and regulate governance, culture and training (para 11.8). An OAIC

[29] Described in *Project Report: Development of Migration Applications & Reporting Tools.*

guidance publication, *Guide to Securing Personal Information* (2018), elaborates on the requirements in APP 11 and the Information Commissioner's Guidelines.

On the information provided, it appears that the Court has taken reasonable steps to secure personal information to which s 91X applies. The root cause analysis undertaken by the Court identified multiple points at which a protection visa litigant's name could potentially be exposed in breach of s 91X. The changes since made by the Court to national registry practices and procedures address those weak spots and aim to ensure that pseudonyms are properly applied in protection visa proceedings.

The changes are recorded and explained in numerous Project Reports that use a standard template. These provide an excellent record of the challenges the Court has faced in responding to the data breach to ensure compliance with s 91X.

The unresolved issue is whether online public access can be fully restored to all migration and appeal matters to which s 91X applies and in which a pseudonym was assigned. The Court recognises, in the internal papers considering this issue, that if unrestricted public access through Federal Law Search is re-instated, no information system can completely eliminate the possibility of information to which s 91X applies being inadvertently exposed to public access. On the other hand, the Court has recognised both the role that online access plays in an open justice system, and the practical importance of online access for litigants, practitioners, government agencies and legal aid and support services.

The Court appears to be dealing with this complex issue in a timely and appropriate manner. It is equally important that the Court's continuing examination of this matter occurs in a transparent manner for the information and benefit of people who may use the Federal Law Search function. This encouragement for continuing transparency is taken up in **Recommendation 2** of this Report.

6. The adequacy of steps taken by the Court to ensure that staff and officers of the Federal Court and Federal Circuit Court are properly aware of the *Migration Act 1958* s 91X, and of necessary measures to ensure compliance with that section

Actions taken by the Court

The Court had acted prior to 20 March to alert staff to the risks of non-compliance with s 91X. As discussed earlier in this Report,[30] the National Registrar emailed other registrars on 12 March after s 91X breaches had been detected in a few recent cases in which identifying information had been wrongly entered by parties during eLodgment and the error was not fully corrected by Registry staff.[31] All registry offices confirmed shortly after that this training advice on applying pseudonyms had been disseminated to registry staff and was formally discussed in meetings in some offices.

Following the data breach, the Court has implemented a more comprehensive staff training program, to be conducted both as a regular refresher course for staff and as part of induction training for new staff:[32]

[30] Heading 1, 'Realisation within the Court of the data breach'.
[31] Described in *Project Report R-2: Registry notification and update of training procedures*, and *Project Report M-4: Development of training material for Registry staff concerning pseudonyms and compliance with s 91X of the Migration Act 1958 (Cth).*
[32] Described in *Project Report M-5: Development and delivery of comprehensive induction and annual training program for Registry staff.*

- The Migration Judicial Registrars conducted face-to-face staff training between 18-22 May for all relevant Registry and Chambers staff. The topics covered included the identification both of protection visa applicants and of matters covered by s 91X, and the national procedures for applying pseudonyms to ensure s 91X compliance. This course will be run annually and will be compulsory for relevant Registry and Chambers staff.

- An eLearning training course is being developed for new and existing Registry staff, with similar content to the face-to-face course. Completion of the course will be required for new staff, and as a refresher course where required for existing staff at an interval of six months from the face-to-face course. Satisfactory completion of the course will require a pass score of 100% in an online quiz.

Assessment and commentary

The importance of complying with s 91X – as a statutory safeguard of the wellbeing of protection visa litigants – was well understood within the Court before the data breach. A comprehensive and regular staff training program has since been implemented to underpin proper compliance. That is appropriate, and is a salutary reminder that it cannot be assumed that staff are properly aware of important policies and procedures that apply to their work. It is reassuring that an element of the new training course for staff is a test to confirm that they completed and fully understood the training material.

7. The adequacy of steps taken by the Court to consider the application of the *Privacy Act 1988* to the data breach and to the Court's response

Actions taken by the Court

The Privacy Act regulates the manner in which personal information is collected, stored, secured, used, corrected and disclosed by 'APP entities' to which the Australian Privacy Principles apply.

The term 'APP entity' extends to Australian Government agencies, including 'a federal court' (s 6). However, the Act does not apply to all actions of a court, but only to 'an act done, or a practice engaged in, in respect of a matter of an administrative nature' (s 7(1)(b)). The obligations imposed by the Notifiable Data Breach scheme in the Act are similarly confined as to federal courts to acts or practices of an administrative nature (s 26WE(1)(a)). The phrase 'of an administrative nature' is not defined in the Privacy Act.

The Privacy Policy of the Court, which is published on the Court website, draws attention to this limited application of the Privacy Act. The Policy draws a distinction between matters relating to 'the management and administration of the Federal Court's registry and office resources' (to which the Act applies) and 'documents, records and other material relating to court proceedings' (that are exempt from the operation of the Act) (p 1). The Policy goes on to observe that 'the Federal Court and its Judges are sensitive to the need to protect personal information and makes arrangements that are consistent with all legal requirements and which balance appropriately the principle of open justice and interests of individual privacy' (p 2). The Policy also notes the requirement in the Migration Act that the Court cannot publish the name of a protection visa litigant (p 2).

The Court's Data Breach Response Plan is framed in general terms as applying to all Court functions, and in particular to any 'unauthorised access to or disclosure of personal information held by the Court'. The Plan notes the legal obligations imposed by the NDB scheme in the Privacy Act. It is implicit in the way the Plan is framed that all data breaches occurring within

the Court will be managed in accordance with the Plan and also – if the data breach is one to which the Privacy Act applies – in accordance with the requirements of that Act.

An APP entity that is aware of a data breach to which the NDB scheme applies is to prepare a statement that is to be given to the Information Commissioner as soon as practicable (s 26WK). I was informed that the Privacy Officer turned his mind to this issue immediately upon being notified internally of the data breach on 20 March.[33] He decided that the Privacy Act did not apply to this Court function (for reasons discussed below) and did not notify the OAIC. The OAIC has also confirmed, in consultation with this Review, that it first became aware of the data breach on or around 31 March as a result of the ABC report.

The ABC report triggered the OAIC's letter to the Court the following day (1 April) making preliminary inquiries under s 42(2) of the Privacy Act. The OAIC letter to the Court had a list of detailed questions about the reported data breach to which the OAIC requested a response by 8 April. The Court responded on that day with a message of reassurance that it was taking the matter extremely seriously, and requesting a further week so that a comprehensive and meaningful response could be prepared.

The Court responded substantively to the OAIC's preliminary inquiry letter on 17 April. The Court did not respond specifically to each of the questions the OAIC had asked, but explained the nature and cause of the data breach, that internal and independent investigations would be conducted and that affected individuals would soon be notified. The Court's letter ended:

> The Court is of the view that the acquisition and management of the information was integrally connected with the Court's judicial function and was not an act done or practice engaged in, in respect of a *matter* of an administrative nature for the purpose of subparagraph 7(1)(b) of the Privacy Act.

The view expressed by the Court that the Privacy Act did not apply to this particular data breach was based on a careful consideration within the Court in preceding days of the provisions of the Privacy Act. I note that I have seen the key documents that reflect the Court's consideration of the issue.

There has been no further communication between the Court and the OAIC about the data breach. I understand that the OAIC may await the finalisation of this report before deciding whether to follow up on the earlier preliminary inquiry.

Assessment and commentary

On the core issue posed in the Terms of Reference – did the Court take adequate steps to consider the application of the Privacy Act? – my opinion is that the Court did so. I note two actions in particular.

First, the Court gave serious consideration to the application of the Privacy Act after receiving the OAIC letter on 1 April. There is a sound basis for the view that the Court reached, namely, that the Court activities that gave rise to the data breach related to the Court's judicial functions and were not of an administrative nature.

I shall not discuss this matter at length, other than to draw attention to the decision of the High Court in *Kline v Official Secretary to the Governor-General* (2013) 249 CLR 645. That case concerned the operation of a similar phrase in the *Freedom of Information Act 1982* (Cth) s 6A(1) – whether a document held by the Official Secretary to the Governor-General 'relates to

[33] Described in *Project Report PR-2: Assessing whether there had been an eligible data breach.*

matters of an administrative nature'. The FOI Act applies to documents that meet that description, but not to other documents held by the Official Secretary.

Their Honours defined the scope of that phrase in the following way: 'the management and administration of office resources'; 'relating to the office "apparatus"' to support the exercise of substantive powers and functions'; and 'providing logistical support (or infrastructure or physical necessities or resources or platforms) for the exercise or performance of … substantive powers or functions to be able to occur'.[34]

The High Court noted that the application of the FOI Act to federal courts rests on the same distinction – that is, the Act applies only to documents held by a court relating to matters of an administrative nature. The joint judgment observed that the phrase refers to 'documents relating to the management and administration of registry and office resources'.[35]

Applying those distinctions in this instance, there is in my view a sound basis for the Court to decide that, consistently with s 91X of the Migration Act, the way that proceedings are titled, documents are lodged, and litigants' names are kept confidential, are matters relating to the discharge of the Court's substantive judicial functions. This approach is consistent with conventional understanding that separate arrangements are maintained within government for oversighting the conduct, respectively, of administrative/executive functions and judicial functions.

Secondly, although the Court proceeded on the basis that the Privacy Act did not apply to the data breach, the Court has handled the breach in a manner consistent with the principles and requirements of the Privacy Act. In particular, the Court acted promptly to contain the breach, it made a public statement about the breach, it notified affected individuals, and it has examined options for ensuring that no further breach occurs.

I have noted earlier[36] that the Court has published both a Privacy Policy and a Data Breach Response Plan that explain how the Court manages personal information and data breaches. The actions the Court took in responding to this data breach are consistent with those guidelines.

A final matter to which I draw attention was the option open to the Court of voluntarily notifying the data breach to the OAIC prior to the data breach being published in the ABC online article.

I raised this issue with the OAIC and it advised that, since the NDB scheme commenced on 22 February 2018, the OAIC has received 32 voluntary notifications from Australian Government agencies. A small number of those data breaches were ones to which the NDB scheme did not apply, while others were data breaches that failed to meet the threshold requirements of the NDB scheme (that is, they were not 'eligible data breaches').

A benefit of voluntary notification is that it puts the OAIC on notice of a breach without having to enquire further. This may be important if, for example, the OAIC receives media enquiries or complaints about the data breach (none were in fact received about this data breach). Voluntary notification can also open a dialogue with an experienced privacy regulator about assessing and managing a data breach.

That said, it was a matter for the Court to decide whether it would embark on voluntary notification when there was no legal obligation to do so. I nevertheless recommend in

[34] Respectively, joint judgment at 662 [41] and Gageler J at 670-1 [74].
[35] Joint judgment at 664 [47[.
[36] Heading 1, 'Assessment and commentary'.

Recommendation 1 that the Court review its Data Breach Response Plan and consider including a reference to the option of voluntary notification.

8. The adequacy of steps taken by the Court to notify and consult the Attorney-General, Attorney-General's Department and other relevant Australian Government agencies about the data breach

Actions taken by the Court

Several Australian Government agencies had a directly relevant interest in the data breach and the Court's response to it.

Attorney-General's Department: Under the *Administrative Arrangements Order* the Attorney-General and the Attorney-General's Department deal with matters relating to courts and the legislation that constitutes courts. It was therefore to be expected that the Court would notify the Attorney-General and the Department of the data breach and subsequent developments.

The Attorney was informally notified of the data breach by the Chief Justice on 21 March, and the Attorney and the Department were notified more formally by the Court on Tuesday 24 March when it forwarded the 'Covid-19 update' that had been sent the previous day to all Judges of the Federal Court. Further updates (in the same style) were provided during the week. A fuller and more direct explanation was provided in emails sent on 31 March by the Chief Justice to the Attorney and by the Court's Privacy Officer to the Department (headed 'Report on s 91X Compliance Issue'). The emails enclosed an internal Court report to the Chief Justice that explained the data breach and the steps taken in response and included internal Court emails and correspondence between the Court and the ABC journalist who had notified the breach.

There has been subsequent discussion and emails between the Court and the Department, covering matters such as the OAIC preliminary inquiry to the Court, the Court's notification of the data breach to the profession and to affected individuals, the contact between the Court and the Department of Home Affairs, and the Court's suspension and restoration of online search services through the CCP.

In consultation with this Review, the Department explained that the information and briefings it received from the Court were timely and enabled the Department to discharge its role of providing advice and coordination within government. The Court's subsequent direct communication with other agencies (such as the Department of Home Affairs) lessened the active coordinating role the Attorney-General's Department might otherwise have to play.

OAIC: The Court's communication with the OAIC, following a preliminary inquiry received from the OAIC on 1 April, is discussed under Heading 7. A view I express in that discussion is that the Court responded appropriately to the preliminary inquiry that it received from the OAIC, but could have earlier considered making a voluntary notification of the data breach to the OAIC.

Department of Home Affairs: As part of its responsibility to administer the *Migration Act 1958* (Cth), the Department of Home Affairs manages the consideration of protection visa applications. It falls within that domain to evaluate the implications of a data breach relating to a person's protection visa application. In particular, it was foreseeable that the Minister for Home Affairs may receive a request under s 48B of the Migration Act from an individual

potentially affected by the data breach to 'lift the bar'[37] and allow a fresh protection visa application to be made.

The Department advised this Review that, in accordance with government protocols, it initially spoke to the Attorney-General's Department about the data breach, and then liaised directly with the Court. The Court consulted the Department about the draft letter to be sent to affected individuals and gave the Department a list of those to whom it was sent. The Court has advised the Department that the CCP does not record IP addresses for online searches in Federal Law Search.

The Department was pleased that it could speak directly and constructively to the Court about the matter. Any requests that are received under s 48B of the Migration Act will be dealt with individually by the Department and the Minister as circumstances require.

Consultation with other corporate users of Court services: There is frequent use of the public search functions in Federal Law Search by many individuals and corporate bodies. I spoke to two bodies – one government, one non-government – about their interaction with the Court after the public search functions were disabled from 20 March onwards. Both bodies regularly access the online services (sometimes multiple times each week) to check on litigation developments that relate to the government agency's regulatory role and to the private sector body's member services.

Both bodies had a similar experience with online access. They became aware in April that online access was impaired, but assumed this was episodic and not caused by the function being disabled. Neither body had seen or was alerted to the online access restrictions by the Court's initial postings in the 'News and Events' section of its website (the item on 31 March was headed 'Migration Matters in the Commonwealth Courts Portal' and on 1 April, 'Federal Law Search').

Both bodies followed up directly with the Court about the access difficulties and then learnt of the data breach problem and the online access restrictions. Those restrictions caused some practical inconvenience. However, the Court has been helpful and engaged in explaining the problem and advising on ways to work-around the access problems. The non-government association conveyed its knowledge to its members in an information alert in early May.

Assessment and commentary

The Court was proactive in notifying the Attorney-General and the Attorney-General's Department of the data breach and in providing regular updates. There was full transparency in providing information to the Attorney and the Department. There has been a similar level of open engagement with the Department of Home Affairs and other government and non-government bodies.

The Court's external engagement with government agencies, non-government bodies, professional legal associations and legal practitioners has been similar as regards the information provided and the level of transparency that was practised. This was important in diminishing any risk of uncertainty or misunderstanding among different Court communities about the nature and scope of the data breach and the Court's response.

There was an initial lag in some government and other bodies fully understanding the nature, scope and impact of the data breach. Partly this was due to the data breach occurring at the

[37] The Migration Act s 48A provides that a non-citizen who has been refused a protection visa may not make a further application for a protection visa. The Minister may determine under s 48B that s 48A does not apply to a person.

same time as and being overshadowed by changes the Court was implementing in response to the COVID-19 crisis. Partly too it was because the Court's announcement of the data breach and its implications either was not highlighted as explicitly as it could have been or was not drawn directly to the attention of relevant parties. This is taken up in **Recommendation 1** in this Report which recommends that the Courts revise their Data Breach Response Plans to outline a clearer procedure for publicly notifying data breaches, and in particular to emphasise that a public announcement of a data breach should be timely, direct and explicit.

9. The adequacy of steps taken by the Court to respond to persons (or their legal representatives) who were concerned about whether they may have been adversely affected by the data breach

Actions taken by the Court

The Court has communicated information about the data breach to the legal profession in several ways, including:

- *Notifying professional legal associations*: The Chief Justice wrote on 27 March, 31 March and 1 April to the Australian Bar Association, the Law Council of Australia, and the Bar Associations and Law Societies in each State and Territory. The three emails were similarly headed, '**Federal Court of Australia – Coronavirus (COVID-19) – Update [12, 13, 14]**. They principally provided information about the adjustments to Court procedures in response to COVID-19, but also contained a paragraph on the data breach and the suspension of the public search facility in the Commonwealth Courts Portal.

- *Responding to individual enquiries:* Following the ABC online article, the Court received correspondence from lawyers and migration advice and advocacy groups, enquiring specifically in some instances about the identity of people affected by the data breach, and in other instances about the significance and potential damage the data breach could cause to individual litigants. The Court has responded to each communication.

- *Individually notifying persons potentially affected*: Between 22 May and 11 June, the Court wrote individually to the 1,037 affected individuals and their legal representatives.[38] Matters explained or noted in the letter were:

    - how a protection visa litigant's name could potentially be exposed through a Federal Law Search
    - steps that had been taken by the Court to ensure that only a pseudonym and not a party name would be shown through a search
    - the Courts cannot determine whether access may have been gained to individual files
    - a person who previously had a protection visa refused or cancelled may be eligible to request Ministerial intervention under s 48B of the Migration Act
    - any person with concerns about how this may affect them should seek independent legal advice
    - the Court contact details to discuss the matter further.

- *Notifying providers of legal aid:* A letter in similar terms as that sent to affected individuals was sent to the providers of legal aid, including immigration and refugee advice centres.

[38] Described in *Project – Notification of Affected Individuals*.

They were advised that they may be contacted for assistance by affected individuals. The letter was sent to 17 providers in all States and Territories.

- *Notifying judicial officers:* Judges of the Federal Circuit Court and the Federal Court were advised of matters in their current docket that were affected by the data breach.

The Department of Home Affairs was given the list of affected individuals to whom the data breach notification was sent.

The Court used several methods to select the most appropriate address(es) to send the letter of notification. An address could not be determined for only 3 people. Some notification letters were returned undelivered – 17 for postal notification, and 33 for email notification; letters were then sent to all but 8 of those 40 people using another address.

By late July the Court had received 35 enquiries from affected individuals in response to the notification. The enquiries were handled by a small group of specially-appointed staff.

Assessment and commentary

As part of this Review I wrote to the legal professional associations and to some of the lawyers and advocacy groups that contacted the Court at the time the data breach became known publicly.

The Law Council and the Law Institute Victoria accepted the invitation to consult further. The Law Institute arranged a telephone conference panel discussion with experienced migration lawyers. The Law Council undertook a survey of the members of the Federal Litigation and Dispute Resolution Section in late May; 13 members responded, of whom approximately half had clients potentially affected by the data breach.[39]

Some other professional legal associations advised that – after consultation with members – the associations had no comments to convey.

I also held three telephone conference discussions with migration lawyers and an advocacy group.

I make the following observations based on this consultation.

- The Court was complimented for the steps it was taking to inform the legal community of developments. Those consulted said it was reassuring to know that the public search function on the Court's website had initially been closed and that affected individuals and their lawyers would be contacted. It was also welcomed that people could speak to Court officers directly about any concerns or queries they had.

- Most practitioners initially became aware of the data breach from sources other than the Court, such as other colleagues or the ABC news article. The Court's website announcements were important, though not readily noticed by casual visitors to the website. The Court's subsequent communication was generally more targeted at reaching specific audiences – though, here again, there was a risk of the initial message being overlooked in the emails to the professional legal associations headed 'Coronavirus (COVID-19)'. The preferred practice for notifying a data breach is to do so directly or specifically.

[39] With the Law Council's consent, its letter and survey report have been provided separately to the Court. The survey sample was too small (as the Court noted) to have a representative value. The main points in the survey are picked up in this report.

- Some concern was expressed by practitioners that, in the early days, the Court was unresponsive to specific requests for information on whether a particular litigant fell within the cohort of affected persons. Two months elapsed before individual notification letters were sent. Practitioners understood that it may be difficult for the Court to give specific earlier advice, though it may have helped even to know the parameters for the data breach or a timeframe for action so that clients could be advised on pre-emptive steps that may be advisable to safeguard their interests.

- Some practitioners wished to emphasise the potentially serious implications of this data breach.[40] The information that may be accessible from the Court file could divulge considerable detail about a protection visa litigant's claims of persecution in another country at the hands of government officials. It was said that intelligence authorities in some countries are known to monitor Australian refugee claims and litigation. Practitioners observed that this was a more serious data breach than one in 2014 when the Department of Immigration published a statistical spreadsheet that inadvertently divulged embedded information about protection visa applicants who were in immigration detention – specifically, their names, dates of birth, nationality, gender and places of detention.[41]

- There were comments about the content of the notification letter the Court sent to affected individuals. The letter would not, it was said, have been easily understood by most protection visa litigants. Some litigants may have been unrepresented, their English proficiency may have been limited, and they may not understand or may distrust Australian Government and court processes. Some recipients rang a lawyer or immigration advice centre perplexed as to what the letter meant and what action was required. No information was given in the notification letter about access to interpreter/translator services, nor the contact details for legal advice agencies/services. The letter raised unanswered questions as to how a litigant may be affected by the data breach, and what further action (if any) the Court might be taking in individual cases.

- Practitioners gave examples of the misapprehension that a recipient may have faced on receiving the letter. One person understood the letter to be advising the recipient to discontinue their Court proceedings and instead seek Ministerial intervention under s 48B of the Migration Act. Another recipient was an affected individual in the 2014 Department of Immigration data breach and wondered whether the two data breach incidents were connected. The reference in the letter to s 48B was incomplete: s 46A also provides a pathway for some protection visa applicants to request Ministerial intervention; and s 48B does not apply if the pseudonym litigant falls under s 501 of the Migration Act.[42]

- Some practitioners would (as they requested the Court) have preferred the Court to have consulted one or more migration law services before sending the letter, and to alert them when the letter was about to be sent. For example, it was fortuitous that one law service learnt that multiple letters were sent to a website address that the service did not monitor as closely as another email address that it ordinarily used. It may equally have been beneficial to discuss with the migration law services the feasibility of different options for

[40] I have separately provided to the Court one of the submissions I received on this issue.
[41] This data breach is discussed in *Minister for Immigration and Border Protection v SZSSJ* [2016] HCA 29 (27 July 2016)
[42] I note that this part of the Court's letter was based on consultation with the Department of Home Affairs.

responding to the data breach – for example, whether a phone advice line was required, whether backup steps could be taken to substantiate if letters were received at the addresses to which they were sent, and whether the shift to remote legal services in response to COVID-19 required an adjustment to data breach mitigation strategies.

- A source of continuing unease is that the Court is unable to advise whether particular litigant files have been accessed online, and if so by whom. This, in turn, makes it difficult to know whether a person should make a request under s 48B of the Migration Act, and if so how to frame that request in a persuasive manner. The relevance of the data breach to proceedings currently underway in the Federal Circuit Court or the Federal Court would also have to be considered.

- Some practitioners observed that the data breach highlighted a problem that had been known for some time regarding exposure of protection visa litigants' names contrary to s 91X of the Migration Act.

My view – which I believe is shared by others – is that the Court went to considerable lengths to ensure that the data breach was notified both generally to the legal community and individually to affected persons and their legal representatives.

Not surprisingly, however, a data breach can have a potential and uncertain impact on many individuals. It may take some time to ascertain who is potentially affected, and how they are affected. This is borne out in the comments made to this inquiry by members of the legal community. Those comments underscore the importance of maximum transparency in notifying a data breach to affected individuals, responding to queries and consulting others about questions that may need to be addressed in notification letters.

Those points are reflected in two recommendations. **Recommendation 1** recommends that the Courts review their Data Breach Response Plans and consider including a reference to the option of consulting external bodies as to the way that persons potentially affected by a data breach should be notified. **Recommendation 3** recommends that the Court consider implementing a practice of recording the IP addresses from which the Federal Law Search function is used to access documents relating to migration and appeal proceedings in the Federal Court and Federal Circuit Court. The limited purpose for recording that information would be to better enable the Court to assess the potential impact of any data breach relating to that information that occurs contrary to section 91X.

10. Any other matter the Review considers relevant to the Review

In this section I note a few matters raised during the Review that do not squarely fall under the Terms of Reference. For the most part these matters were raised in the consultations held with professional legal associations, legal practitioners and advice and support services.

- Section 91X applies narrowly and prohibits only the publication of a protection visa litigant's name. By contrast, two other provisions in the Migration Act (noted in footnote 19 above) prohibit the publication of information that may identify a visa applicant.

  A few legal practitioners observed that s 91X does not adequately address the risks that underlie its enactment. A minor personal detail in a Court judgment may enable the security intelligence agencies of another country to identify a person referred to only by a pseudonym – such as the person's date and place of birth and date and method of arrival in Australia; or their involvement in an incident in Australia or abroad that is known to intelligence authorities or was reported in the media.

Courts are apprised of this risk and are frequently asked to make a suppression order applying to particular details in an order or judgment. However, some practitioners felt that broader consideration should be given to this issue within either the courts or government. The data breach, in drawing attention to the risks facing protection visa applicants, should be seen as an appropriate trigger for that broader consideration to occur.

- The notification letter the Court sent to affected individuals and legal representatives drew attention to the facility in s 48B of the Migration Act to request the Minister for Home Affairs to 'lift the bar' and allow a fresh protection visa application to be made. The Court has provided the names of the 1,037 affected individuals to the Department of Home Affairs.

  Based on their experience with applications under s 48B, practitioners observed that it can take a couple of years to receive a response. They urged that s 48B requests that are prompted by this data breach should be given priority treatment by the Department. To the extent that it can properly do so, the Court was urged to lend its support to this priority treatment. The practitioners also commented that it should be taken into account when a s 48B request is being considered that the applicant may be hampered by the fact that the Court did not record the IP addresses from which information in the electronic court files was accessed.

- There was mention of the inconvenience created by the restrictions that have been placed on online access through Federal Law Search to migration and appeal matters. In particular, a practitioner or support service that is not a party to a proceeding is unable to access relevant documents through Federal Law Search and provide advice to a person, even though the practitioner may be a registered user in relation to other Court proceedings.

  The Court is aware of these difficulties and is considering options for restoring online access to migration and appeal matters. The practitioner concern about the inconvenience they face underscores the importance of **Recommendation 2**, that the Court continue to be as transparent as possible in considering the options for restoring public access to migration and appeal matters through Federal Law Search.

- A related matter, as noted in an internal Court options paper, is that providing online access to non-party users to files in which a pseudonym has been assigned is likely to be complex, costly and time-consuming. The potential cost and complexity was also raised by other persons and organisations who were consulted for this Review. They wished to emphasise the importance of maintaining online public access to information about Court proceedings and urged that Government consider favourably the possible need to supplement the Court's budget funding.

APPENDIX A

Terms of Reference for this Review

INDEPENDENT REVIEW OF ACTION TAKEN BY THE FEDERAL COURT FOLLOWING A DATA BREACH CONTRARY TO SECTION 91X OF THE *MIGRATION ACT 1958*

Background to the Review

This review has been commissioned by the Federal Court of Australia after becoming aware that information was accessible from a Federal Court website that may have led to the publication of the names of litigants contrary to section 91X of the *Migration Act 1958* (Cth).

The Federal Court, through senior officers of the Court, became aware in late March 2020 that the names of some litigants who had commenced protection visa proceedings in the Federal Court and the Federal Circuit Court could be accessed on the Commonwealth Courts Portal through Federal Law Search. Those web-based services are managed under the *Federal Court of Australia Act 1976*.

The access that could be obtained to the names of some litigants was or could be, if obtained, publication contrary to the Migration Act s 91X. That provision provides that a federal court must not publish (in electronic form or otherwise) the name of a person in a proceeding relating either to their application for a protection visa or related bridging visa, or to the cancellation of such a visa. This state of affairs is referred to in these terms of reference as a 'data breach' or 'the data breach'.

Steps were taken by the Court on the day it was notified of the data breach to disable online access to information about individual court proceedings, while the cause and scope of the issue was examined. Limited and modified online access and search functions have since been restored. Some of the former online search functions remain disabled.

Steps have been taken by the Court to identify specific migration protection visa application proceedings that may be affected by the data breach, and to ensure compliance with s 91X.

The data breach was brought to the attention of the Chief Justices, Judges and Chief Executive Officers of both courts, the Attorney-General, the Attorney-General's Department, the Audit Committee of the Federal Court, the Law Council, the Presidents of the Bar Associations and Law Societies, and was discussed with the Office of the Australian Information Commissioner.

The Court also responded to enquiries that it received about the data breach from a media organisation and from legal representatives and advocacy groups. A notice about the data breach was published on the Court's website.

The Federal Court decided in April 2020 to commission an independent review of the circumstances relating to the data breach and the Court's response.

Scope of the Review

The Review is to consider:

1. the nature, extent and cause of the data breach
2. whether the Federal Court responded in a timely and appropriate way upon becoming aware of the data breach, and in particular whether the Court has taken or is taking adequate steps:
    a) to identify the cause of the data breach

b) to identify individual proceedings or parties that may be affected by the data breach
c) to ensure that the circumstances giving rise to the data breach have been rectified and that proscribed data exposure will not occur
d) to notify and consult the Attorney-General, Attorney-General's Department and other relevant Australian Government agencies about the data breach
e) to respond to persons (or their legal representatives) who were concerned about whether they may have been adversely affected by the data breach
f) to consider the application of the *Privacy Act 1988* (Cth) to the data breach and to the Court's response
g) to implement suitable risk control and oversight mechanisms to prevent proscribed data exposure, and to ensure timely identification and response to any data breach that contravenes s 91X
h) to ensure that staff and officers of the Federal Court and Federal Circuit Court are properly aware of the *Migration Act 1958* (Cth) s 91X, and of necessary measures to ensure compliance with that section.

The Review may consider any other matter that it considers relevant to the purpose or subject matter of the Review, even if it does not fall strictly within the terms of the scope of the review as set out above.

The Review may make recommendations as to any action that the Federal Court may take in response to the findings of the Review.

The Review may take notice of any deliberation occurring within the Federal Court or the Federal Circuit Court as to the effect (if any) that the data breach may have on individual proceedings before either court. However, the Review is not to make findings or express an opinion on any such issue, recognising that the conduct of proceedings falls within the judicial function of the courts.

Conduct of the Review

The Review is expected to commence in April 2020. The Reviewer shall provide a report to the Court within six weeks of commencing the Review.

The Review may consult:

- staff and officers of the Federal Court and the Federal Circuit Court
- members of the Audit Committee of the Federal Court
- the Attorney-General's Department, the Office of the Australian Information Commissioner and any other Australian Government agency with a relevant interest in the matters being examined by the Review
- legal professional associations and other non-government associations with a relevant interest in the matters under review
- the legal representatives of parties who may have been adversely affected by the data breach and who contacted the Court about the matter
- any other person or body with a relevant interest in the Review
- and after consultation with the Chief Justices or Chief Judge, judges of their respective Courts.

The Review is not to contact any person or body external to the Court for the purposes of the Review without first advising the Court of its intention to do so. The Review will take account of any view expressed by the Court as to the suitability of a particular person or body being consulted, and as to how any such consultation should be arranged or may be undertaken