KPMG

cutting through complexity

Management initiated review

Privacy breach – Data management

Abridged report

Department of Immigration and Border Protection

20 May 2014

Contents

KPMG
cutting through complexity

1. Disclaimers

This report has been prepared at the request of the Department of Immigration and Border Protection (the DIBP) for the purpose of providing the DIBP with an abridged factual report which may be appropriate for public release, on the events leading up to the disclosure of personal information of detainees, in connection with a document uploaded to its website on 10 February 2014.

In providing this report ("the abridged report"), we have had regard to the DIBP's responsibility to manage the risk of potential further privacy breaches in relation to this incident, by not disclosing information which may alert potential recipients of their possession of, or ability to access, the personal information, or identifying how access to personal information was gained by unauthorized person/s. Further, we understand that the DIBP wishes to manage the risk of future data compromises by not disclosing the detailed workings of the DIBP and any potential system weaknesses, which could be exploited, whilst they are being rectified. A separate report including the aforementioned sensitive material was issued to the DIBP on 5 April 2014.

We have prepared this report pursuant to the terms of reference set out in our Management Initiated Review, dated 24 February 2014, and the terms and conditions of the Deed of Standing Offer (DOSO) with KPMG, under which the DIBP has engaged KPMG to provide Forensic services, and they are not to be used for any other purpose without our prior written consent. Other than our responsibility to the DIBP, neither KPMG nor any member or employee of KPMG, undertakes responsibility arising in any way from reliance placed by a third party on this report. KPMG does not consent to any reliance by any third party on this report. Any such reliance placed is that party's sole responsibility and KPMG excludes any liability to that party.

The services provided in connection with this engagement comprise an advisory engagement, which is not subject to assurance or other standards issued by the Australian Auditing and Assurance Standards Board and, consequently no opinions or conclusions intended to convey assurance have been expressed.

We have considered and relied upon information, which we believe to be reliable, complete and not misleading. Nothing in these documents should be taken to imply that we have verified any information supplied to us, or have in any way carried out an audit of any information supplied to us other than as expressly stated in this report. The statements and observations included in these documents are given in good faith, and in the belief that such statements and findings are not false or misleading.

These observations are based solely on the information provided to us during the course of our fieldwork up to 13 March 2014. We reserve the right to amend any findings, if necessary, should any further information become available.

2. Executive summary

Background

The 'Immigration Detention and Community Statistics Summary' (the **Document**), a Microsoft Word document dated 31 January 2014, which was published on the DIBP's website, allowed access to source data containing personal information of approximately 10,000 detainees. KPMG was appointed to undertake a Management Initiated Review (**MIR**) into the matter.

The review has been undertaken through two work streams. One focussed on establishing the chronology of events leading to the disclosure and the second a technical examination of the data associated with the disclosure and the potential extent of access to that data. Our report on the review was issued to the DIBP on 5 April 2014, following which the DIBP requested a report which may be appropriate for public release.

In providing this report ("the abridged report"), as requested by the DIBP, we have had regard to the DIBP's responsibility to manage the risk of potential further privacy breaches in relation to this incident, by not disclosing information which may alert potential recipients of their possession of, or ability to access, the personal information, or identifying how access to personal information was gained by unauthorized person/s. We understand the DIBP also wishes to manage the risk of future data compromises by not disclosing the detailed workings of the DIBP and any potential system weaknesses, which could be exploited, whilst they are being rectified.

Observations

How did the data become embedded in the 'Immigration Detention and Community Statistics Summary' dated 31 January 2014?

- The data extract obtained to produce the analysis for the Document contained the personal information of the detainees. Personal information was not removed prior to the analysis being performed.
- The process adopted in producing and publishing the Document appears to have not conformed with the roles and responsibilities set out in either the web publishing and governance intranet guidance or the online style guide. Although potentially ambiguous in some relevant areas, the online style guide sets out specific requirements for the publication of documents, which appear not to have been followed. Factors potentially contributing to the incident having occurred may include time pressures, unfamiliarity with certain functionality of Microsoft Word, lack of awareness of roles and responsibilities and limited awareness of IT security risks associated with online publishing.

Is there any indication that the privacy breach may have been malicious or intentional?

- We have not identified any indications that the disclosure of the underlying data was intentional or malicious.

Do earlier versions of the same report contain the same exposure to the underlying data?

- The DIBP provided, for our review, versions of this publication released by the DIBP in prior months. We did not identify the same issue during our review, so it appears isolated to the version dated 31 January 2014.

What was the extent of potential access to the 'Immigration Detention and Community Statistics Summary', dated 31 January 2014 and therefore, the underlying personal data?

- The potential data access and distribution is widespread, with 123 "hits" on the document from 104 unique IP addresses. Analysis of available data has provided the DIBP with some indication of the likelihood of each IP address having access to the personal information of detainees.

Recommendations

We proposed the following recommendations to prevent a similar incident occurring in the future:

- Develop and implement a procedure whereby any data to be extracted for the purpose of analysis is normalised and cleansed in a secure environment, to ensure that any personal or sensitive data is removed prior to any analysis being performed;
- Update online publishing quality assurance checklists to require approvers to confirm that the document has been reviewed in its native electronic form;
- Hold online publishing workshops involving Director level representation from Information Technology (IT) Security, Web Operations and Governance, User Centred Design Competency Section and all Branches involved in the creation of material that may be published online. The objectives being to identify risks associated with publishing content online, clarify roles and responsibilities with respect to online publishing, consider strategies for best managing associated IT security risks and what modifications to existing publication, prioritisation and clearance guidelines need to be made as a result of workshop outcomes;
- Develop an IT security training program, to be delivered to all personnel operating in an area of the DIBP responsible for handling private or sensitive data, and include specific day-to-day scenarios covering typical risks associated with handling such data;
- Incorporate lessons learned from this review into Privacy training to be delivered in connection with the operation of the Australian Privacy Principles; and
- Ensure that all policies, procedures and other guidance materials relating to roles and responsibilities of personnel involved in the creation, review and publishing of online content is updated on a timely basis and accessible to all areas of the DIBP.

3. Introduction

- Background
- Scope and objectives
- Limitations
- Approach

3.1. Background

The Department of Immigration and Border Protection (DIBP) has inadvertently allowed access through its website to the personal information (including names, dates of birth, nationality) of a large number of detainees. The access was gained by a person/s unknown and passed to journalist/s at The Guardian.

The DIBP loaded a Microsoft Word document titled 'Immigration Detention and Community Statistics Summary' (the Document), dated 31 January 2014, onto its website, which inadvertently allowed access to data that contained personal information as outlined above. The DIBP removed the document from its website immediately after the matter came to its attention.

The *Privacy Act 1988* required the DIBP to adhere to a number of Information Privacy Principles (IPPs) (now replaced by the Australian Privacy Principles) governing the collection, use and disclosure of personal information. "Personal information" is relevantly defined to mean information about an individual whose identity is apparent, or can reasonably be ascertained, from the information.

KPMG Forensic was engaged by the DIBP to conduct a management initiated review of the matters set out in above background information, provided by the Department.

3.2. Scope and objectives

The objectives of this Management Initiated Review (MIR) were to identify how access to personal information was allowed by unauthorised person/s and any recommendations to prevent this occurring again.

This MIR included the following scope of work:

1) Explaining the chronology of how access to personal information was gained.
2) Determining who accessed the information and who may retain access to the personal information?
3) Reporting on remaining departmental vulnerabilities that may allow access to sensitive or personal information.
4) Reviewing policy and management practices that contributed to this significant breach of privacy.
5) Proposing Options to prevent a recurrence of this incident.

Limitations

Our scope of work was subject to several limitations, which we informed the DIBP of, and certain aspects of our work were, necessarily, undertaken within tight timeframes.

3.3. Approach

In completing the above scope or work, we adopted the following approach:

- Reviewed policies and procedures relevant to understanding the DIBP's management of personal information and protocols applied when loading material on the internet;
- Met with appropriately informed persons to collect information about policy, protocols and practices within the scope of this investigation;
- Analysed the final version of earlier editions of the Document published online in the twelve months prior to 31 January 2014, to determine whether any other versions exhibit vulnerabilities that may allow access to sensitive or personal information;
- Analysed Internet Protocol (IP) addresses, external to the DIBP, identified as attempting to access the file;
- Provided regular briefings to the relevant Deputy Secretary, or his representative; and

- Prepared reports[1] addressing the scope of work set out above. In providing this abridged report, requested by the DIBP, we have had regard to the DIBP's responsibility to manage the risk of potential further privacy breaches in relation to this incident, by not disclosing information which may alert potential recipients of their possession of, or ability to access, the personal information, or identifying how access to personal information was gained by unauthorized person/s. We understand the DIBP wishes to manage the risk of future data compromises by not disclosing the detailed workings of the DIBP and any potential system weaknesses, which could be exploited, whilst they are being rectified.

[1] Our report on the review was issued to the DIBP on 5 April 2014, following which the DIBP requested a report appropriate for public release.

4. Observations

- Timeline of events
- Procedural guidance
- Forensic examination of the data disclosure
- Policies and management practices that contributed to the data disclosure

4.1. Chronology of the creation, review and publishing of the Document

A chronological summary of events that transpired, in connection with the publication of the Document, is set out below.

- A data set, including personal details of detainees was extracted from a data warehouse by a member of the responsible reporting team, for the purpose of preparing the Monthly Detention and Community Statistics Summary (the Document), to be published on the DIBP's website. In this instance, the data set was extracted manually using data analytics queries over the weekend of 1 / 2 February 2014. Ordinarily this process would be automated, however, it was manually expedited to assist in meeting the target publication date of 10 February 2014.
- The data set was imported into a Microsoft Excel template used to perform statistical analysis. A quality assurance review of formulae contained in the template was completed.
- Additional quality assurance procedures were performed on the data set contained in the Microsoft Excel template, for the purpose of rectifying data integrity issues. This involved, for example, clarification of such things as blank fields and age/classification discrepancies.
- Charts and tables from the Microsoft Excel template were copied into the Microsoft Word version of the Document. The member of the responsible reporting team who undertook this task had not previously prepared the Document. The responsible reporting team provided direct support by way of a supervisor and step by step instructions for the completion of the task.
- Clearance for the content of the Document was escalated, for review and approval, in accordance with the responsible reporting team's content clearance matrix.
- Throughout the content clearance process, various aspects of the Document were amended, based on reviewer comments. In some instances, this involved alterations to the underlying Microsoft Excel template and copying of data to the Microsoft Word Document.
- The responsible reporting team sent the Document to the responsible web management team for publishing to the internet. The Document was escalated through the responsible web management team's clearance process, which involved review and approval up to Assistant Secretary level. The reviews resulted in various amendments to the Document, with the incident occurring at some point in the process of making those amendments.
- A communication, noting Director level approval from the responsible web management team, was submitted to the Web operations, Publishing and Governance group mail box, where it entered a queuing system to be actioned.
- The Document was randomly allocated to a Web publisher, in accordance with standard procedures. The Web publisher renamed, optimised and checked the properties of the MS Word and pdf versions of the Document in accordance with accessibility requirements of the Web Content Accessibility Guidelines 2.0 (WCAG 2.0).
- The Document was uploaded to a test environment by the Web Publisher and screenshot and document links emailed to the responsible web management team for review and approval.
- Approval was provided and the Document was migrated to the live environment and uploaded to the internet. We understand that when the initial version of the Document was uploaded, a member of the responsible reporting team encountered difficulties with accessing hyperlinks, which were rectified before the Document was accessible online.

We note the following with respect to the quality assurance reviews performed:

- Reviews were performed predominantly on a hardcopy of the Document and focused on ensuring the writing style, grammar and spelling were consistent with Departmental guidelines and that calculations were arithmetically correct;
- When an electronic version was reviewed, quality assurance checks focused on ensuring compliance with accessibility guidelines; and
- Authors and approvers were generally unaware that the IT security risk which led to this incident, could occur and were therefore not mindful of checking for indicators of this risk.

4.2. Departmental policies and guidance regarding online publishing

Online style guide and web governance intranet guidance

An overview of roles and responsibilities with respect to web publishing and governance and compliance with Privacy legislation, as set out in the DIBP's Online Content Governance procedures, is summarised below.

Role	Online style guide compliance
Division Head	Expected to....monitor quality, relevancy, accuracy and legality of web content under their responsibility
Branch Head	Will....guarantee their web content meets the governance requirements set out in this document
Director *(responsible for viewing information prepared by authors)*	Ensure new web content and major changes...are usability and accessibility tested to meet online publishing guidelines
Area web coordinator	Ensure content for their division meets the department's publishing standards
Author *(responsible for preparing information for websites)*	Ensure that information submitted for approval: • ....follows the departmental style guide • meets Australian Government Online and Departmental online publishing requirements and standards; and • does not infringe copyright and privacy legislation.

We note the following with respect to the above guidance material:

- Neither the content authors, nor the Director of the responsible reporting team, were aware of these responsibilities, nor had they received any training in their application;
- Though available on the intranet, it was not readily accessible by users; and
- The DIBP's Online Style Guide, discussed below, is not something that either the content authors, or the Director of the responsible reporting team, were aware of.

We have noted that the DIBP's Online Style Guide provides relevant guidance, which may have assisted those responsible for the creation, approval and publishing of the Document, to detect the potential disclosure of personal information not meant for disclosure. However, in the absence of accompanying training, demonstrating the range of ways in which the risks set out in these guidelines could occur, it is unlikely that less technically proficient readers would understand the risks or how to protect against the risks occurring.

Procedures relating specifically to the creation, review and publishing of online content

Each team involved in the creation, review and publishing of the Document, has procedural guidance available to team members. We set out below our observations with respect to each team's respective guidance:

Responsible reporting team guide to preparing the Monthly Detention and Community Statistics Summary

- This guide includes an explicit instruction regarding the preparation of the Monthly Detention and Community Statistics Summary which, if followed, could have prevented the incident from occurring;
- Despite being aware of this explicit instruction, no members of the responsible reporting team involved in creating or reviewing the document understood the IT security context or the risks associated with failing to adhere to the instruction;
- Without proper training, the instruction in itself is insufficient in its application; and
- Whilst the document sets out the clearance process escalation chain, it does not provide any guidance in respect of specific quality assurance checks to be performed at each level.

Responsible web management team procedural guidance

- Procedural guidance regarding quality assurance checks to be undertaken by the responsible web management team did not provide sufficient detail regarding the risk of an incident such as this occurring.

Web operations and governance procedural guidance

- The Web operations, publishing and governance section maintains procedural documentation relating to internal processes around online publishing. This includes, inter alia, RACI matrices, process flows and both pre-publishing and quality assurance checklists.

  It is possible that adherence to certain checks set out in these documents could have detected the issue and prevented the incident occurring. However, it is unclear whether this procedural guidance or its associated learnings have been made available to other relevant personnel, such as content authors.

  Further, quality assurance checklists included focus more on compliance with writing style and accessibility guidelines with no explicit reference to consideration of IT security risks that may be associated with the publishing of content online.

4.3. Forensic examination of the data disclosure

Our observations with respect to the forensic examination of the data disclosure are summarised as follows:

- 123 accesses via 104 unique internet protocol (IP) addresses attempted to retrieve the file at least once. Analysis of available data has provided the DIBP with some indication of the likelihood of each IP address having access to the personal information of detainees;
- It is not in the interests of detainees affected by this incident to disclose further information in respect of entities to have accessed the Document, other than to acknowledge that access originated from a range of sources, including media organisations, various Australian Government agencies, internet proxies, TOR network and web crawlers;
- Attempts were made by KPMG Forensic, as instructed by the DIBP, to reduce the risk of republication of material contained in the Document where a high likelihood of this occurring was identified. Any such efforts were considered in the context of the DIBP wanting to avoid disclosing any information which may alert potential recipients of their possession of, or ability to access, the personal information;
- We have not identified any indications that the disclosure of the underlying data was intentional or malicious; and
- The DIBP provided us with earlier versions of the publication, which it had released in prior months. Our review did not identify the same issue, so it appears isolated to the version dated 31 January 2014.

4.4. Policies and management practices that contributed to the data disclosure

Based on observations from our work completed to date, we note the following policies and management practices that contributed to the disclosure of the personal data:

- Previously, the DIBP published monthly online editions of the Document in PDF form only. A desire to achieve compliance with legislative requirements on Government, to publish information in accessible form for the visually impaired, led to a decision to publish the Document in Microsoft Word form also. Different document formats pose particular security risks, and in this instance staff involved in preparing, reviewing and publishing the Document were unfamiliar with the risks, and potential control measures, associated with publishing material online.
- Staff involved in the preparation, review and publishing of the Document were unaware of the particular IT security risk that led to this incident occurring. This was exacerbated by the fact that when the incident occurred, the personal information was not immediately visible to a reviewer. None of the personnel who reviewed an electronic version of the document undertook any steps to check for any potential indicators of the personal information being disclosed.
- In the majority of instances, a hardcopy version of the Document was reviewed. This was unlikely to result in the personal information being detected.
- Although the DIBP's online style guide provides some guidance addressing certain IT security risks associated with online publishing , no procedural guidance adequately explains the privacy / security risks associated with the specific actions that led to the incident occurring.
- Procedural guidance for creating the publication provided an explicit instruction which, if followed, could have prevented the incident occurring. However, staff involved in this process had no understanding of the context for why this instruction needed to be followed. The instruction was, in itself, insufficient in its application as the outcome would visually appear to be the same, even if the user chose one of several different courses of action in deviating from the explicit instruction.
- There was a general lack of understanding, amongst the various teams involved in online publishing, as to the clearance checks undertaken by each group and / or reviewer. In several instances, it was assumed that prior reviewers had undertaken more extensive checks than had actually occurred.
- There was a view expressed that the Document was handled by too many reviewers and that each additional layer of the quality assurance review process did not always add value.
- The responsible reporting, web management and web operations, publishing and governance teams face significant time pressure in publishing the Document. In respect of this publication, there are several contributing factors, including:
  - Whether the publication's assigned priority status as urgent, based on an impact and urgency assessment against specified criteria, is reasonable in the context of the DIBP's prioritisation matrix for online publishing, and whether the matrix or communication protocols could be updated to better reflect the business context;
  - The amount of data cleansing and normalisation required to get the data set in the appropriate form to complete the analysis for the publication; and
  - The number of reviews required as part of the clearance process and the time required coordinating this.
- The primary author of this edition of the publication had not prepared the document previously. Although this delegated responsibility was planned and supported by supervision, training, and step by step instructions, the process was more susceptible to human error on this occasion.

5. Recommendations

- Handling of sensitive data
- QA processes
- Consultation with IT security
- Training
- Australian Privacy Principles
- Policies and procedures

Based on observations from our work completed to date, as well as consideration of suggestions from personnel consulted as part of the review, we recommend consideration of the following measures designed to prevent recurrence of this specific incident, or an incident of a similar nature, that may occur as a result of the vulnerabilities identified through this review:

- Consider the development and implementation of a procedure whereby any personal data extracted for the purpose of analysis is normalised and cleansed in a secure environment, to ensure that any private or sensitive data, not necessary for the analysis, is removed prior to any analysis being performed;
- Update online publishing quality assurance checklists to require approvers to confirm that the document has been reviewed in its native electronic form, and include an end-to-end checklist with clearly defined responsibilities. Reviewers may, at their discretion also choose to review a copy of the publication in hardcopy, however, the electronic review should constitute the base line check;
- Hold online publishing workshops involving Director level representation from Information Technology (IT) Security, Web Operations and Governance, User Centred Design Competency Section and all Branches involved in the creation of material that may be published online. The objectives being to identify risks associated with publishing content online, clarify roles and responsibilities with respect to online publishing, consider strategies for best managing associated IT security risks and what modifications to existing publication, prioritisation and clearance guidelines need to be made as a result of workshop outcomes;
- Develop an IT security training program, to be delivered to all personnel operating in an area of the DIBP responsible for handling private or sensitive data, and include specific day-to-day scenarios covering typical risks associated with handling such data;
- Consider liaising with appropriate Commonwealth bodies regarding organisational readiness with respect to accessibility guidelines. In particular, confirming the current status regarding acceptable publication formats and whether any recent technological advances in that regard alter the DIBP's current position with respect to online publishing preferences[2];
- Incorporate lessons learned from this review into Privacy training to be delivered in connection with the Australian Privacy Principles; and
- Ensure that all policies, procedures and other guidance materials relating to roles and responsibilities of personnel involved in the creation, review and publishing of online content is updated on a timely basis and accessible to all areas of the DIBP.

In addition to the specific measures set out above, we recommend that the DIBP, in responding to this incident, also take the opportunity to consider its current practices and procedures with respect to handling of sensitive data and, in particular, the level of consultation with the DIBP's IT security team in managing this risk.

[2] It is important to emphasise that modifications to the online publishing process do not become the sole focus of remedial efforts going forward and that the handling and transmission of sensitive data more broadly is also considered.