PRIVACY TRAINING

Susan Bennett
Sibenco Legal & Advisory
e: susan.bennett@sibenco.com
p: +61 409 480 840
@sibenco
Privacy

A strong privacy culture is critical for ensuring personal information security.

Privacy champions essential for strong privacy culture.
Personal Information
Personal Information
Global Digital Economy – data flows
Insights from Data Analytics & Data Sharing
Information

Freedom of Information
FOI Act 1982

Privacy
Privacy Act 1988
Privacy now in focus
Cambridge Analytica & Facebook

Cambridge Analytica scandal: the biggest revelations so far

Since Christopher Wylie blew the whistle in the Observer, developments have been rapid. Here’s what we know about the analytics firm, Facebook and Trump’s election team.

Cambridge Analytica and Facebook: The Scandal and the Fallout So Far

Revelations that digital consultants for the Trump campaign trained for and obtained millions of Facebook users’ profiles have shock the world.

Cambridge Analytica’s Facebook data was accessed from Russia, MP says

The new, infamous Facebook data scandal involving millions of Americans gathered by a Cambridge University scientist for a firm that ran training for Donald Trump’s 2016 campaign was accessed from Russia, a British member of parliament tells CNN.

The Cambridge Analytica Files

A year-long investigation by the Observer reveals the secrets behind the Cambridge Analytica scandal.

How to check if your Facebook information was shared with Cambridge Analytica by the RNC

Uncover the “grossly unethical experiment” and how your data may have been compromised.

Facebook Cambridge Analytica Scandal: 10 Questions Answered

Deep dive into the scandal with answers to the most important questions about how and why.

©2020 Sibenco Pty Ltd
Cambridge Analytica & Facebook

How Cambridge Analytica Exploited the Facebook Data of Millions

New York Times
PageUp – June 2018

Bank details, TFNs, personal details of job applicants potentially compromised in major PageUp data breach

The personal details of thousands of Australians have potentially been compromised, with HR company PageUp, which counts Telstra, NAB, Coles, Australia Post, Aldi and Medibank as clients, revealing a massive data breach.

PageUp data breach forces Coles, Aus Post and more to close careers websites

PageUp data breach: ABC, Asahi, Myer, Macquarie pull jobs pages

PageUp faces customer losses, lawsuits after data breach
Universities impacted

Universities victims of data breach at PageUp incl: Melbourne, RMIT, UNSW, Macquarie, ANU, Tasmania.

Reported that ‘malicious code executed inside PageUp’s systems’.

Major universities hit by data breach affecting thousands of job applicants at top firms

Leading universities including Melbourne and Macquarie have become the latest victims of a major data breach at human resources firm PageUp, forcing them to suspend their job boards and urge applicants to check their affairs for unusual activity.

PageUp People, which manages recruitment for ASX200 firms including AMP, Telstra and Coles, revealed it had detected ‘unusual activity’ on its IT infrastructure last month and received ‘some indicators that client data may have been compromised’.

The breach is under investigation by the government-run Cyber Security Centre. PageUp advised there was “no evidence that there is still an active threat, and the jobs website can continue to be used” – though many of its clients were being more cautious.
ANU says 'sophisticated operator' stole data in new cyber breach

By Max Koslovski and David Wroe
Updated June 4, 2019 – 4:49pm, first published at 11:33am

Up to 200,000 students and staff of the Australian National University have had personal data stolen in a “sophisticated” cyber attack that echoes a similar breach last year attributed to the Chinese government.

The university has admitted the hackers stole data stretching back 19 years that included bank details, passport information and academic records of current and former students and staff.

ANU data breach stretching back 19 years detected

Updated 4 Jun 2019, 5:02pm

The Australian National University has been hit by a massive data hack, with unauthorised access to significant amounts of personal details dating back 19 years.

A sophisticated operator accessed the ANU’s systems illegally in late 2018 but the breach was only detected two weeks ago, the university said in a statement.

Based on student numbers over that time, as well as staff turnover, the university has estimated approximately 200,000 people were affected by the breach.

“We believe there was unauthorised access to significant amounts of personal staff, student and visitor data extending back 19 years,” ANU vice-chancellor Brian Schmidt said.

“Depending on the information you have provided to the university, this may include names, addresses, dates of birth, phone numbers, personal email addresses and emergency contact details, tax file numbers, payroll information, bank account details, and passport details. Student academic records were also accessed.”

However, Professor Schmidt said the hack had not accessed credit card details, travel information, medical records, police checks, workers’ compensation information, vehicle registration numbers, and some performance records.

Key points:
• ANU vice-chancellor Brian Schmidt said the university had been made aware of the breach two weeks ago
• Professor Schmidt said there had been unauthorised access to “significant amounts” personal data
• IT upgrades put in place after a different breach last year helped detect the incident
The Australian Catholic University has been hit by a data breach, with the attacker(s) using a phishing email to trick users into revealing their credentials on a fake ACU login page. The ACU has three public websites, with the main one running on Linux, while two others, which allow staff to log in, run on Windows Server 2008.
The laptops – which were taken in a break-in at a UWA administration building – contain the Tax File Numbers and student identification numbers of people who applied to study at the university between 1988 and January 2018.

“Separately, and in varying degrees of completeness, there are also details across the laptops from applicants who may have provided the University with information such as names, dates of birth and passport numbers to obtain a confirmation of enrolment,” Vice-Chancellor Professor Dawn Freshwater”
'Alarming' Data Breach Exposes 50,000 Students In Ticketing Website Bungle

Get, an online service used by a numerous clubs, societies, and student organisations around Australia, has suffered a major data breach, potentially
Student claims 'insane' amount of information available
Claims about the system vulnerability emerged over the weekend, after a University of Canberra software engineering student posted on social media.

The student, who asked to remain anonymous, told the ABC he found the data when applying for a club membership. "[The website] showed a list of all the people that were part of that society, which seemed a bit strange to me," the student said. He said a quick online search found the personal data of about 200,000 users dating back more than a year. "I looked at the information that was being sent from Get to my computer ... it's things like name, phone number, date of birth, addresses, student number."
March 2020

Australia data breach: 90,000 staff, students, suppliers impacted at Melbourne Polytechnic

Personal data, including e-mail addresses, passwords, driver’s license, passport details, and financial and health information of 90,000 staff, students and suppliers

Victoria Police notified Melb Polytechnic that an individual who attended the campus in **late 2018** had ‘obtained unauthorised access to Melbourne Polytechnic’s computer systems by hard logging onto the network; overcoming security measures.’
Data Breach Causes – OAIC, 28 Feb 2020

- Human error: 32%
- Malicious or criminal attack: 64%
- System faults: 4%
Malicious or criminal attacks

- Theft of paperwork or data storage device: 12%
- Social engineering/impersonation: 9%
- Rogue employee/insider threat: 12%
- Cyber incident: 67%
Cyber incident

- Phishing (compromised credentials): 36%
- Compromised or stolen credentials (method unknown): 32%
- Malware: 10%
- Ransomware: 6%
- Brute force attack (compromised credentials): 6%
- Hacking: 6%
- Other: 4%
Human Error Causes – OAIC, 28 Feb 2020
Data Breach

A data breach happens when personal information is accessed or disclosed without authorisation or is lost.
Top 5 Sectors – July to Dec 2019

- Health service providers: 22%
- Finance: 14%
- Education: 9%
- Legal, accounting & management services: 7%
- Recruitment & training agencies, childcare, vets & community services: 4%
OAIC report – 1st 12 months of NBD Scheme

964 data breach notifications
- From 1 April 2018 to 31 March 2019

114 data breach notifications
- for financial year 2016/2017
OAIC report – 19% increase in 2019

- 537 data breach notifications
  - From 1 July 2019 to 31 December 2019

- 460 data breach notifications
  - From 1 January 2019 to 30 June 2019
What do you do if you identify a data breach of personal information?
Notify the ANU Privacy Officer
Data breach notification

You must notify affected individuals and OAIC when a data breach involving personal information is likely to result in serious harm.

- Enables students, staff and affected individuals to take any steps required to protect themselves from risk that may occur as a result of the data breach.
- Assist to mitigate any damage and reflect positively on the University’s reputation.
Serious Harm

The types of PI involved more likely to cause serious harm include:

- sensitive information – e.g. health
- documents commonly used for ID fraud e.g. Medicare number, student number, driver license, passport details
- financial information
- a combination of types of PI that allows more to be known about the individuals
Nature of Harm

Examples likely to result in serious harm include:

- identity theft
- significant financial loss
- threats to an individual’s physical safety
- loss of business or employment opportunities
- humiliation, damage to reputation or relationships
- workplace or social bullying or marginalisation
Notify the ANU Privacy Officer
Process for managing a data breach

- Contain & Notify PO
- Evaluate
- Notify - affected persons - OAIC & other agencies
- Act
- Prevent
When are affected individuals and OAIC notified of data breach?
Assessment - As Short a Time as Possible

Section 26WH(2): An organisation must take all reasonable steps to complete the assessment within 30 calendar days after the day it became aware of the grounds that caused it to suspect an eligible data breach.

But....

wherever possible entities to treat 30 days as a maximum time limit ..., and endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time.
Assessing a Suspected Data Breach

The assessment:

- Must be reasonable and expeditious
- Entities may develop their own procedures for assessing a suspected data breach
General Data Protection Regulation (GDPR)
EU- GDPR

The biggest change to Europe’s privacy laws in 20 years

Enforced from 25 May 2018

Penalties of up to 4% of global turnover or €20 million, whichever is higher
Notification of Data Breach under GDPR

Under the GDPR, notification must be made where a data breach is likely to ‘result in a risk for the rights and freedoms of individuals’.

Notification must be made within 72 hours of first having become aware of the breach.

Data processors are required to notify their customers and the controllers ‘without undue delay’ after first becoming aware of a data breach.
GDPR applies to Australian orgs that -

- are data processors or controllers with an establishment in the EEA
- offer goods or services to individuals in the EEA
- monitoring the behavior of individuals in the EEA, where that behavior takes place in the EEA
Personal Information
Mandatory Data Breach Reporting

Australia’s notifiable data breach (NDB) scheme - 23 February 2018
APP entities – incls orgs with $3m turnover, health care providers, ANU, private tertiary education providers, & breaches of TFNs

EU - General Data Protection Regulation (GDPR) - 25 May 2018
Australian orgs incl education providers, tertiary institutes if they are operating in the EU or offering goods & services to EU residents – i.e. prospective or current students or alumni residing in EU
Notification of Data Breach under GDPR

Under the GDPR, notification must be made where a data breach is likely to ‘result in a risk for the rights and freedoms of individuals’.

Notification must be made within 72 hours of first having become aware of the breach.

Data processors are required to notify their customers and the controllers ‘without undue delay’ after first becoming aware of a data breach.
Rights of Individuals Under the GDPR

- Right of access
- Right to be informed
- Right to object
- Right to withdraw consent
- Right to restrict processing (in certain circumstances)
- Right to object to automated decision making (in certain circumstances)
- Right to erasure / be forgotten
- Right to data portability
- Right to rectification
Global Digital Economy – data flows
Changes to Privacy Act ahead

Federal Government announcement in March 2019 that:

• OAIC will be provided with an additional $25 million over three years to give it the resources it needs to investigate and respond to breaches of individuals’ privacy

• Amendments to Privacy Act will be drafted for consultation.
Privacy Check List

- Check - are you collecting PI?
- Check/think - do you need the PI, or all of the PI?
- Check before using and/or disclosing PI - i.e. is the use or disclosure permitted?
- Think before you send - avoid email address errors and/or wrong recipients
- Secure your computer and other devices; keep passwords safe
- Don’t fall for phishing or other scams
- Be vigilant about information security
The challenge of Shadow IT
Comply with ANU Policies

- Acceptable Use of IT Policy
- Code of Conduct
- Records & Archive Management Policy
What is Personal Information?

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable.

What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.
Personal Information at the University

- Student/staff - name, address, ID number
- Family details, bank account details
- Medical Info incl medicare number
- Counselling notes
- Photographs, recorded images
What are the risks?

- Risk to student and/or staff safety
- Financial loss to the student/family, and/or staff and/or University
- Reputational damage
- Loss of trust in University
- Regulatory investigation, litigation
Personal information about an individual which is apparent or can reasonably be ascertained

**Redaction of name**

*AIN v Medical Council of New South Wales* [2016] NSWCATAD 5

‘While the Applicant’s personal information was masked from the human eye, her personal information was able to be ‘read’ by the Google search engine. This resulted in a search for ‘Dr [AIN]’ (or similar) leading to a link to a copy of the (human eye redacted) Medical Tribunal’s decision. The Respondent accepted, properly in my view, that a Google search for ‘Dr [AIN]’ would link the Medical Tribunal’s decision to her’
De-identification of Personal Information

De-identified information is information from which identifiers have been permanently removed, or where identifiers have never been included. De-identified information cannot be re-identified.
Personal information from linking with other information

‘We have concluded that, depending on the circumstances, sources of information other than the information or opinion which contains the personal information, may be consulted to ascertain the person's identity.’

*APV and APW and Department of Finance and Services [2014] NSWCATAD 10 at [54]*
Australia – Re-identification of dataset

THE SIMPLE PROCESS OF RE-IDENTIFYING PATIENTS IN PUBLIC HEALTH RECORDS

In late 2016, doctors’ identities were decrypted in an open dataset of Australian medical billing records. Now patients’ records have also been re-identified - and we should be talking about it.

By Dr Vanessa Teague, Dr Chris Culnane and Dr Ben Bahamonde, University of Melbourne

In August 2016, Australia’s Federal Department of Health published medical billing records of about 3.9 million Australians online. These records came from the Medicare Benefits Scheme (MBS) and the Pharmaceutical Benefits Scheme (PBS) containing 1 billion lines of historical health data from the records of around 30 per cent of the population.

These longitudinal records were of person’s identity being used to fund the government’s open data website.

Health pulls Medicare dataset after breach of doctor details

[Updated] Researchers say govt encryption was poor.

The Department of Health has removed a research dataset based on Medicare and PBS claims from its open data portal after 3 years of Melbourne researchers pounced out that patient data could be decrypted.

The government today advised that the data was withdrawn yesterday following “an alert raised to the public of the public interest” by researchers Dr Vanessa Teague from Melbourne University on September 22.

Teague said the department that she and her colleagues had analysed 10 percent of the linked dataset and found it was possible to decrypt some of the sensitive personal ID numbers associated to doctors.

“As a result of the potential to exploit some doctors and other service providers’ ID numbers, the Department of Health immediately removed the dataset from the website to ensure the security and integrity of the data is maintained”, the researchers in a statement.

©2020 Sibenco Pty Ltd
Australian Privacy Principles (APPs)
13 Australian Privacy Principles

There are 13 APPs and they govern standards, rights and obligations around:

- the collection, use and disclosure of PI
- ANU’s governance and accountability
- integrity and correction of PI
- the rights of individuals to access PI
The Privacy Principles (APPs)

1. Open and transparent management of PI - incl. having a clearly expressed and up to date privacy policy

2. Anonymity and pseudonymity

3. Collection of PI - outlines when you can collect PI

4. Dealing with unsolicited PI - outlines steps to be taken where unsolicited PI is received
The Privacy Principles (APPs)

- **Notification** – outlines what an individual must be informed
- **Use or Disclosure** – outlines the circumstances in which PI may be used or disclosed
- **Direct marketing** - may only use or disclose PI for direct marketing purposes if certain conditions are met
- **Cross-border disclosure of PI** - outlines steps that must take to protect PI before it is disclosed overseas
<table>
<thead>
<tr>
<th>9</th>
<th>Gov’t related identifier – outlines limited circumstances when a gov’t identified may be adopted</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Accuracy – reasonable steps must be taken to ensure PI is accurate, up to date and complete</td>
</tr>
<tr>
<td>11</td>
<td>Security - reasonable steps must be taken to protect PI from misuse, interference and loss, and from unauthorised access</td>
</tr>
<tr>
<td>12</td>
<td>Access – incls a requirement to provide access unless a specific exception applies</td>
</tr>
<tr>
<td>13</td>
<td>Correction – outlines the obligation to correct PI held about individuals</td>
</tr>
</tbody>
</table>
Privacy Check List

- Check - are you collecting PI?
- Check/think - do you need the PI, or all of the PI?
- Check before using and/or disclosing PI - i.e. is the use or disclosure permitted?
- Think before you send - avoid email address errors and/or wrong recipients
- Secure your computer and other devices; keep passwords safe
- Don’t fall for phishing or other scams
- Be vigilant about information security
Review and Discussion
Example

Annabel’s father calls Linda, who is Annabel’s supervisor, and says he is concerned that he hasn’t heard from Annabel for 6 weeks as she usually speaks with him regularly. He is worried as she suffers from depression and would like Annabel’s contact details. Can you provide Annabel’s mobile number or email address to her father?
Example

ASIO contacts Anne who is a senior manager, asking for information about John who is a junior member of her team and says that he is suspected of being involved in a terror organisation. ASIO want access to John’s attendance records at events held over the last 4 months. Anne hands this information over to ASIO. Should Anne have done this?
Example

A detective contacts a University staff member and asks the staff member to provide contact details for one of the University employees within his area. They say that the disclosure is necessary for a fraud investigation and is required urgently, but is unwilling to provide further details in case it compromises the investigation.
A valued member of your team is seriously injured in a car accident and, due to their injuries, cannot give consent. Can the University disclose the individual’s health information to the treating health service where the University reasonably believes that disclosure of the information is necessary to lessen the serious threat to the individual’s life posed by those injuries?
Example

There is a new social plugin offering, which looks great, and can very simply be added by the database administrator in your area to the alumni database already being used by the University. Is this okay to be added as it would increase engagement with the alumni database.
The University receives a request for the names and email addresses of the last 5 years graduates to be surveyed on starting income. Can the list be provided?
Example

The University receives a request for the names and email addresses of last year’s graduates for one of its courses to be surveyed for a prestigious international ratings body. Can the list be provided?
Example

You have just received a letter that a software license, which is essential in your area is up for renewal. The annual license fee is $1,500. What is the process for review and approval?
Example

You have just received a letter that a software license, which is essential in your area is up for renewal. The annual license fee is $10,000. What is the process for review and approval?
You and another senior executive have dinner with Bill and Sally who are potential major donors to the University. They confide that unfortunately they won’t be in a position to make the foreshadowed major donation for another two years as the proposed sale of their business has just been delayed and they have just discovered their son has an ice addition. What is appropriate to record in internal communications reporting on the dinner and expected donation?
Example:
Anonymising qualitative data

This shows how a piece of qualitative personal data – in this case an interview with a student - can be converted into an anonymised form which still contains valuable information but does not identify the student.

Original text

Interview recorded: 3pm, 10 October 2011
Interviewee: Julius Smith
DoB: 9 September 2005
School: Green Hall School

I live on Clementine Lane so I walk to school every day. I live in a flat with my parents and my Uncle Jermaine. When I get home from school I watch TV. I don’t like reading but I like watching Harry Potter films. My favourite subject at school is art. My teacher is Mr Haines and he is very nice. I used to get bullied by Neil and Chris but I told Mr Haines and they stopped.

I play football for Junior Champs, and we are good. I play midfield.

Anonymised text

Interview recorded: October 2011
Interviewee ref: 2011/45
School year: Key Stage 1 School
Local authority area: City of Sydney Council

I live in [LM51 postcode] so I walk to school every day. I live with [family members]. When I get home from school I watch TV. I don’t like reading but I like watching Harry Potter films. My favorite subject at school is art. My teacher is Mr. [teacher’s name] and he is very nice. I used to get bullied by [other pupils] but I told [the teacher] and they stopped.

I play football for [a local team], and we are good. I play midfield.
Privacy Champions & Privacy Proactive

Be proactive, be prepared and able to quickly escalate and respond

- Be able to identify when there is a data breach
- Escalate and notify Privacy Office immediately
- Embed Privacy Culture – e.g. team meetings
- Staff training – identifying, escalating and knowing what to do in breach event
- Ensure suppliers comply with contractual requirements incl privacy regulations
Personal Information
## Privacy Check List

- **Check** - are you collecting PI?
- **Check/think** - do you need the PI, or all of the PI?
- **Check before using and/or disclosing PI** - i.e. is the use or disclosure permitted?
- **Think before you send** - avoid email address errors and/or wrong recipients
- **Secure your computer and other devices; keep passwords safe**
- **Don’t fall for phishing or other scams**
- **Be vigilant about information security**
Thank you

Susan Bennett
Sibenco Legal & Advisory
e: susan.bennett@sibenco.com
p: +61 409 480 840
www.sibenco.com
@sibenco