Privacy & Pwnage

Privacy Law, Data Breaches and Lessons for Security Pros

Nicholas Van Exan

A Few Disclaimers

- I’m a lawyer.
- I’m not your lawyer.
- This is not legal advice.
- If you have legal questions specific to your business, get in touch with your legal counsel.

Sources of Privacy Law re Data Breaches

- Statutory Law
  - Federally: PIPEDA
  - Provincially: PIPA (AB, BC), etc.
  - Internationally: GDPR
- Common Law
  - Tort (Negligence, Breach of Confidence, Intrusion Upon Seclusion, Public Disclosure of Private Facts, etc.)
  - Contract (e.g. privacy policies, controller / processor agreements)
  - Waiver of Tort

PIPEDA

Application

- Application (s. 4)
  - Applies to every organization in respect of personal information that the organization collects, uses or discloses in the course of commercial activities

- But see s. 26(2): substantially similar legislation

Personal Information

- Personal Information => information about an identifiable individual
- Information is about an identifiable individual where there is a "serious possibility" that an individual could be identified through the use of that information, alone or in combination with other available information.
- PI can range from more to less sensitive

Principles

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting use, disclosure, retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

Safeguards

- 4.7 - Principle 7 (Safeguards)
  - Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
  - The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.
  - The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.

Breach Defined

- Breach of security safeguards =>
  - the loss of, unauthorized access to or unauthorized disclosure of personal information that either results from a breach of an organization's administrative, technical or physical security safeguards or from a failure to establish those safeguards.

The Ashley Madison Hack

ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

See Your Matches »

Over 37,565,000 anonymous members!

00%
-minded
eople

As seen on: Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today

Ashley Madison is the world's leading married dating service for ***discreet*** encounters

Trusted Security Award

100% DISCREET SERVICE

SSL Secure Site

Timeline

- July 15, 2015: notified by “The Impact Team” it had been hacked - threat to expose PI if AM not shut down

- July 20, 2015: *after* media reports, ALM reported breach to OPC

- August 18-20, 2015: Impact Team publishes PI for 36 million accounts

Attack Strategy

- The attackers' initial path of intrusion involved the compromise and use of an employee's valid account credentials
- The attacker then used those credentials to access ALM's corporate network and compromise additional user accounts and systems

Attack Strategy

- The attacker took a number of steps to avoid detection and to obscure its tracks. For example…
  - accessed the VPN network via a proxy service that allowed it to ‘spoof’ a Toronto IP address
  - accessed the ALM corporate network over a long period of time in a manner that minimized unusual activity or patterns in the ALM VPN logs that could be easily identified
  - once the attacker gained administrative access, it deleted logs to further cover its tracks
- ALM was unable to fully determine the path the attacker took but believes that **the attacker had some level of access to ALM’s network for at least** several months before its presence was discovered in July 2015

Several. Months.

Several.


YOU JUST GOT
PWNED!

Safeguards

- Nature of information: account information, profile information, billing information
- OPC: assessment of level of security safeguards required should not focus solely on financial risk
- OPC: must also consider physical and social well-being at stake, including potential impacts on relationships and reputational risks, embarrassment or humiliation.

“Harm to reputation is a potentially high-impact risk as it can affect an individual’s long term ability to access and maintain employment, critical relationships, safety, and other necessities depending on the nature of the information held… even information that in isolation might be regarded as innocuous in a different context (such as names or email addresses) can take on a more sensitive nature when connected with the Ashley Madison website.”

Key Facts / Findings

- ALM could have reasonably foreseen that the disclosure of the information held by it to an unauthorized person, or to the world at large, could have significant adverse consequences for the many people who could be identified

- Discretion and security were marketed and highlighted to its users as a central part of the service it offered and undertook to provide, in particular on the Ashley Madison website

- At the time of the data breach, the front page of the Ashley Madison website included a series of trust-marks which suggested a high level of security and discretion


Trusted
Security
Award
100%
DISCREET
SERVICE
SSL
Secure
Site

100%!

When was the last time you had a 100% guarantee of anything, let alone information security?

FYRE

APRIL 28-30 | MAY 5-7

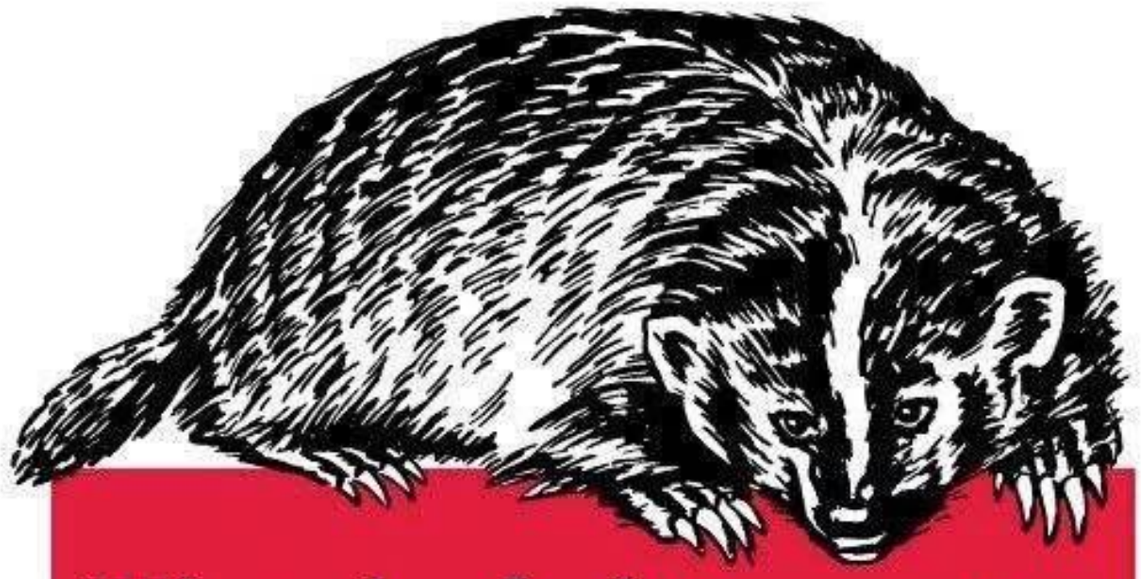
2017

EXUMAS

Key Facts / Findings

- At the time of the incident, ALM did not have documented information security policies or practices for managing network permissions
- ALM did undertake patch management and quarterly vulnerability assessments as required for an organization to accept payment card information (to be PCI-DSS compliant). However, it could not provide evidence that it had undertaken any structured assessment of the overall threats facing it, or that it had assessed its information security framework through standard exercises such as internal or external audits or evaluations.

The definitive guide for all project managers



What the fuck is security

How to ignore it and deliver your project

O'RLY

Awn Thyme

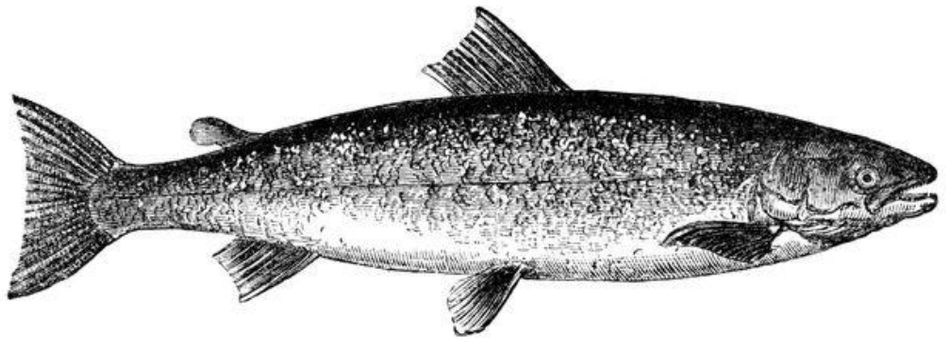
:P orly.coloncapitalp.com

Key Facts / Findings

- ALM noted that prior to the breach, it had, at one point, considered retaining external cybersecurity expertise to assist in security matters, but ultimately elected not to do so

- ALM did not implement multi-factor authentication => "Given the risks to individuals' privacy faced by ALM, **ALM's decision not to implement multi**-factor authentication for administrative remote access in these circumstances is a significant concern."

Security by optimism and prayer



Expert

Hoping Nobody Hacks You

O RLY?

@ThePracticalDev

Conclusions / Key Takeaways

- ALM did not have appropriate safeguards in place considering the sensitivity of the personal information under PIPEDA
- Security framework was lacking the following key elements:
  - documented information security policies or practices, as a cornerstone of fostering a privacy and security aware culture including appropriate training, resourcing and management focus;
  - an explicit risk management process — including *periodic and pro-active assessments of privacy threats*, and evaluations of security practices to ensure ALM's security arrangements were, and remained, fit for purpose; and
  - adequate training to ensure all staff (including senior management) were aware of, and properly carried out, their privacy and security obligations appropriate to their role and the nature of ALM's business.

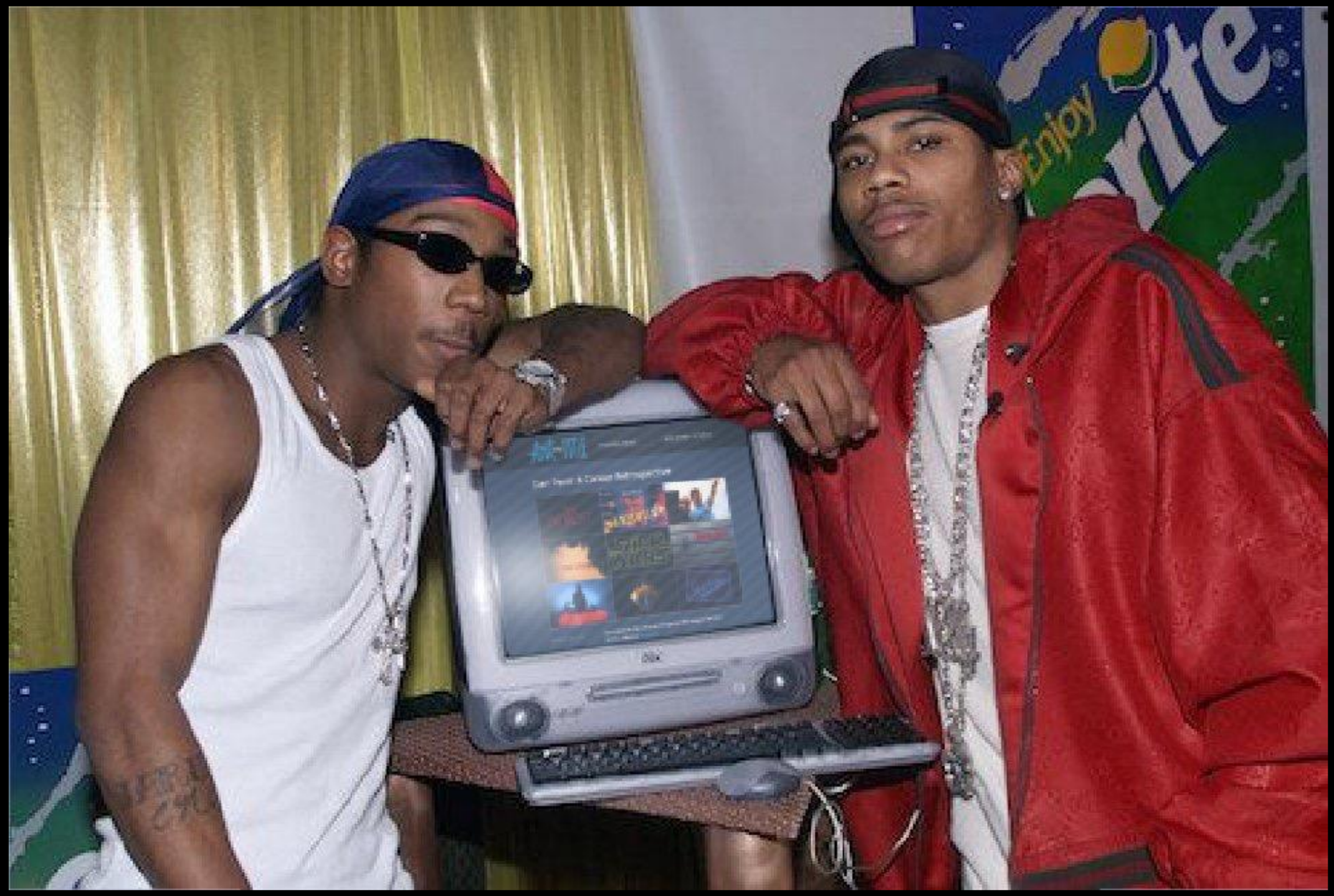
Aftermath

- ALM suffered very public investigation by OPC and is now subject to compliance obligations / undertakings
- ALM is also now subject of $750,000,000 class action in Canada


OOOOHHH!
SOMEONE GOT BURNED...
memecrunch.com

But that was then and this is now.

And things are about to get a lot more real (legislatively speaking)



Hold on to your Sprite website…

Coming Soon to PIPEDA:
Data Breach Notification Requirements

- Amendments to PIPEDA via *Digital Privacy Act* will create new mandatory breach notification requirements:
  - organizations must keep records of any breach of security safeguards - must be produced to OPC if requested
  - if reasonable to believe breach creates a real risk of significant harm to individual, organization must report breach to the OPC as soon as 'feasible' after the org determines a breach has occurred
  - the organization must also notify the individual if it is reasonable to believe that the breach creates a real risk of significant harm to the individual - must also be made as soon as feasible

The General Data Protection Regulation (GDPR)

GDPR

- The EU's new omnibus data protection law
- Set to replace the existing 20-year-old Data Protection Directive 95/46/ec on May 25, 2018
- Huge fines and penalties - up to $20 million or 4% of company revenue, whichever is higher!

GDPR

- Also has data breach notification requirements:
  - Article 33 requires controllers to notify the appropriate supervisory authority of the personal data breach "without undue delay" and in any event within 72 hours of learning about a breach
  - Article 34 requires controllers to notify data subjects of breaches "[w]hen the personal data breach is likely to result in a high risk [to] the rights and freedoms of individuals". Data subjects must also be notified of the breach "without undue delay."

GDPR

- A data controller does not have to provide notice to data subjects, however, if:
  - the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
  - has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or
  - it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

The GDPR has extra-territorial application and Canadian businesses can be subject to it.

Common Law

Trends & Recent Developments

- Historically at common law there was no specific cause of action for invasion of privacy
- Basic principle of civil liability that one must prove actual harm, compensable in damages, before requiring someone else to pay for a commitment of a wrong

- This all changed in 2012 with ONCA's landmark ruling in *Jones v. Tsige*

Intrusion Upon Seclusion

- To succeed in a claim for intrusion upon seclusion, one must demonstrate:
  - an intentional act (which includes recklessness);
  - an invasion, without lawful justification, of the plaintiff's private affairs or concerns; and
  - a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.
- Personal and sensitive nature of the information and lawful justification are key issues

Intrusion Upon Seclusion

- Proof of harm to a recognized economic interest is not an element of the cause of action

- Given the intangible nature of the interest protected, damages for intrusion upon seclusion will ordinarily be measured by a modest conventional sum

- But… damages should be sufficient to "mark the wrong that has been done"

Trends

- Huge increase in privacy class actions since 2013
- Being fuelled by novel claims of intrusion upon seclusion and waiver of tort
- Potentially large awards
- Less barriers to certification

Recent Hacking Cases

- *Maksimovic v. Sony* - $1 billion claim
  - Settlement providing for various benefits, depending in part on an individual's account type, as well as ability to prove harm and obtain up to $2,500 out of pocket costs, and counsel fee $265,000.
- *Lozanski v. Home Depot* - $500 million claim
  - Court approved settlement, value of $400,000
- *Shore v. Avid Life* - $750 million claim
  - Pending
- *Zuckerman v. Target Corporation*
  - Class action was certified earlier this year

Home Depot

A Counterpoint to Ashley Madison

Home Depot

- April 11 - September 13, 2014: Home Depot's card payment system was hacked by criminals who used custom malware to access customer information at self-checkout terminals
- September 9, 2014: Home Depot notified OPC and Privacy Commissioners in Alberta, B.C. and Quebec
- Also issued press releases and directly notified 500,000 potentially affected customers

Home Depot

- Home Depot apologized for breach, confirmed removal of malware and assured customers they would not have to pay for fraudulent charges to their accounts
- Also offered free credit monitoring and identity theft insurance
- Class actions commenced in Ontario, Saskatchewan, B.C., Newfoundland and Quebec

Home Depot

- National Settlement reached April 25, 2016
- Terms of settlement:
  - Home Depot agreed to create $250,000 settlement fund to compensate any documented losses arising from breach, max of $5,000 per claimant
  - Also agreed to pay for credit monitoring up to a maximum of $250,000 and to cover costs of notifying class members and administering the fund

Home Depot

- Court approved the settlement and assessed maximum value of settlement at $400,000
- Noted that case was very weak:
  - breach was due to criminal hackers, not wrongdoing by Home Depot
  - Home Depot openly and promptly notified customers and sought to lessen potential harm arising from breach
  - Little documented losses

“Home Depot… responded in a responsible, prompt, generous, and exemplary fashion to the criminal acts perpetrated on it by the computer hackers”

Home Depot

- Home Depot was also subject to class action litigation by certain banks and other financial institutions

- March 8, 2017: settlement agreement was submitted for court approval

- Home Depot agreed to pay $25 million to a settlement fund

Home Depot

- Home Depot also agreed that for 2 years it would adopt and implement measures to reduce risks of future data breach:
  - safeguards to manage risks identified through data security risk assessments, tracked and managed using a risk exception process that involves Home Depot leadership and is reviewed on an annual basis;
  - annually assess, including with on-site visits, service providers and vendors with access to payment card information to validate compliance with security practices; and
  - design and implement an industry recognized security control framework

Takeaways

- Home Depot shows that it's helpful even in absence of data breach notification requirements to adopt proactive measures to notify and assist potentially affected individuals

- Timely notification can be helpful in mitigating liability - need to look at your security protocols to ensure you can react swiftly in event of breach

- Timely detection is also important to limit potential class size

Takeaways

- Super important to have a comprehensive data security incident response plan (“IRP”) and a trained incident response team
- IRPs = written plans designed to enable an organization to respond to various kinds of data security incidents in a way that minimizes harm, reduces recovery time and costs, and allows the organization to benefit from lessons learned

Takeaways

- IRP basic requirements:
  - identify the incident response team members (both internal personnel and external advisors and consultants) and their respective roles and responsibilities
  - set out the procedures they should follow to respond to and recover from a data security incident, to assess and mitigate the business and legal risks resulting from the incident and to take appropriate measures to prevent the same or a similar incident in the future
  - cover all phases of a data security incident response – discovery (initial assessment and team activation), containment, recovery, post-recovery investigation and post-incident review and report

Takeaways

- IRP best practices:
  - Keep it short, simple, actionable, practicable
  - Follow guidance from regulators in various jurisdictions you are subject to
  - Mandate involvement of legal counsel and plan for legal privilege protection
  - Include procedures for team communication, record keeping, evidence collection, notification and information sharing with the public

Takeaways

- Pay special attention to sensitive PI => ensure it is encrypted, anonymous or at least pseudonymous
- Conduct routine pen testing
- Advocate for active management of security findings to compliance
- Ensure data breaches are discovered as early as possible
- Ensure systems / procedures in place to report data breaches as soon as possible

Thanks!

- More questions / resources?
  - http://nicholasvanexan.com