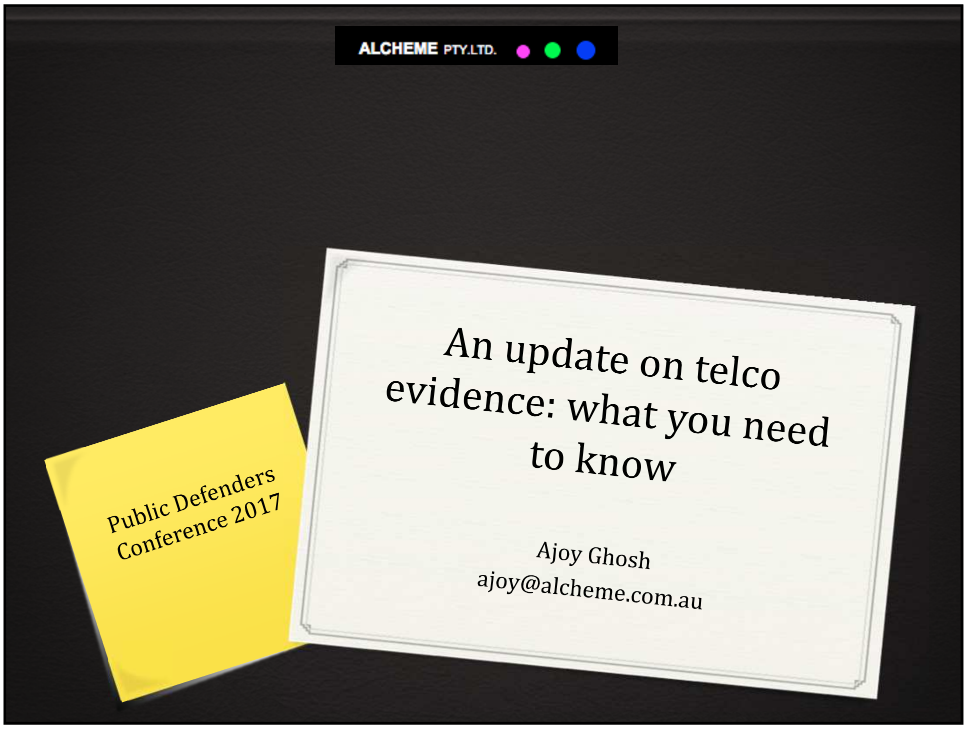


ALCHEME PTY.LTD.

Public Defenders Conference 2017

An update on telco evidence: what you need to know

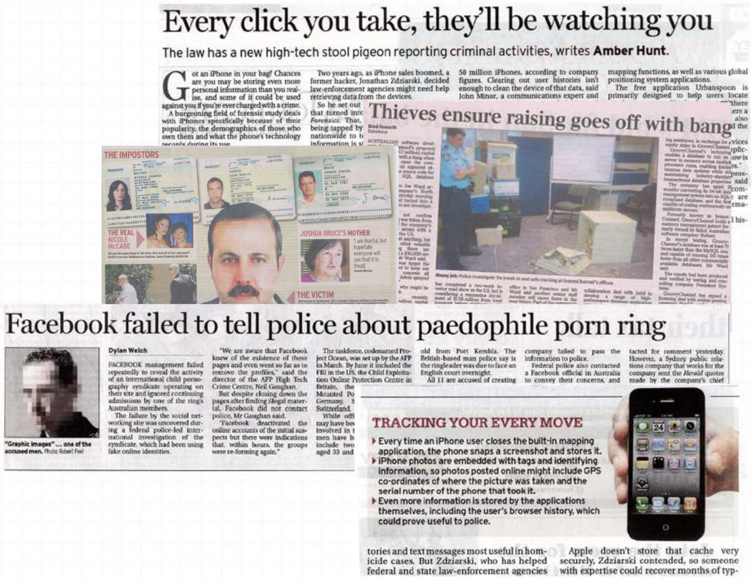
Ajoy Ghosh
ajoy@alcheme.com.au

Why I've been asked to present

- Lecture in cyberlaw, electronic evidence and computer forensics at Australian and international law schools
- Australian and international standards:
  - Author of Australian handbook on Management of IT Evidence
  - Co-author of Australian standard on Information Security Risk Management (now ISO 27005)
  - Contributor to Australian standard on Corporate Governance of IT (now ISO 38500)
  - ISO Blockchain committee meeting in April 2017
- Expert witness:
  - Complex technical crimes: hacking, cyber stalking, cyber bullying, child pornography, fraud and forgery, circumvention, organised crimes, terrorism
  - Politically sensitive and high profile e.g. Sef Gonzales, James Hardie, Sydney terrorism trials, Simon Gittany
- Advisor to Government and industry:
  - IRAP Assessor with Australian government clearance NV2
  - Protect significant critical infrastructure and safety-critical systems

HB171: Guidelines for the Management of IT Evidence (above)
HB231: Guidelines for Information Security Risk Management (below)

ALCHEME PTY.LTD.



Every click you take, they'll be watching you

The law has a new high-tech stool pigeon reporting criminal activities, writes **Amber Hunt**.

Got an iPhone in your bag? Chances are you may be storing even more personal information than you realise, and some of it could be used against you if you're ever charged with a crime.

A burgeoning field of forensic study deals with iPhones specifically because of their popularity, the demographics of those who own them and what the phone's technology records during its use.

Two years ago, as iPhone sales boomed, a former hacker, Jonathan Zdziarski decided law-enforcement agencies might need help retrieving data from the devices.

So he set out … that turned into … *Forensics*. That, … being tapped by … nationwide to … information is st…

50 million iPhones, according to company figures. Clearing out user histories isn't enough to clean the device of that data, said John Minor, a communications expert and

mapping functions, as well as various global positioning system applications.

The free application Urbanspoon is primarily designed to help users locate

Thieves ensure raising goes off with bang

THE IMPOSTORS

THE REAL NICOLE McCABE

JOSHUA BRUCE'S MOTHER

'I am fearful, but hopefully everyone will see that it is fraud.'

Sarah Bruce

THE VICTIM

Facebook failed to tell police about paedophile porn ring

"Graphic images" … one of the accused men. Photo: Robert Peel

Dylan Welch

FACEBOOK management failed repeatedly to reveal the activity of an international child pornography syndicate operating on their site and ignored continuing admissions by one of the ring's Australian members.

The failure by the social networking site was uncovered during a federal police-led international investigation of the syndicate, which had been using fake online identities.

"We are aware that Facebook knew of the existence of these pages and even went so far as to remove the profiles," said the director of the AFP High Tech Crime Centre, Neil Gaughan.

But despite closing down the pages after finding illegal material, Facebook did not contact police, Mr Gaughan said.

"Facebook deactivated the online accounts of the initial suspects but there were indications that, within hours, the groups were re-forming again."

The taskforce, codenamed Project Ocean, was set up by the AFP in March. By June it included the FBI in the US, the Child Exploitation Online Protection Centre in Britain, the … Mounted Po… Germany, S… Switzerland.

While offi… may have bee… involved in t… men have b… include two … aged 33 and

old from Port Kembla. The British-based man police say is the ringleader was due to face an English court overnight.

All 11 are accused of creating

company failed to pass the information to police.

Federal police also contacted a Facebook official in Australia to convey their concerns, and

tacted for comment yesterday. However, a Sydney public relations company that works for the company sent the *Herald* quotes made by the company's chief

TRACKING YOUR EVERY MOVE

- Every time an iPhone user closes the built-in mapping application, the phone snaps a screenshot and stores it.
- iPhone photos are embedded with tags and identifying information, so photos posted online might include GPS co-ordinates of where the picture was taken and the serial number of the phone that took it.
- Even more information is stored by the applications themselves, including the user's browser history, which could prove useful to police.

tories and text messages most useful in homicide cases. But Zdziarski, who has helped federal and state law-enforcement agencies

Apple doesn't store that cache very securely, Zdziarski contended, so someone with expertise could recover months of typ-

Agenda

1. A typical Police analysis
2. Accessing the device and other investigative issues relating to encryption
3. Installation of surveillance software
4. ~~Exculpatory evidence not typically looked for~~
5. The emerging issue of mandatory data retention and finding data from the teclo instead of the device(s)

A typical Police analysis

ALCHEME PTY.LTD.

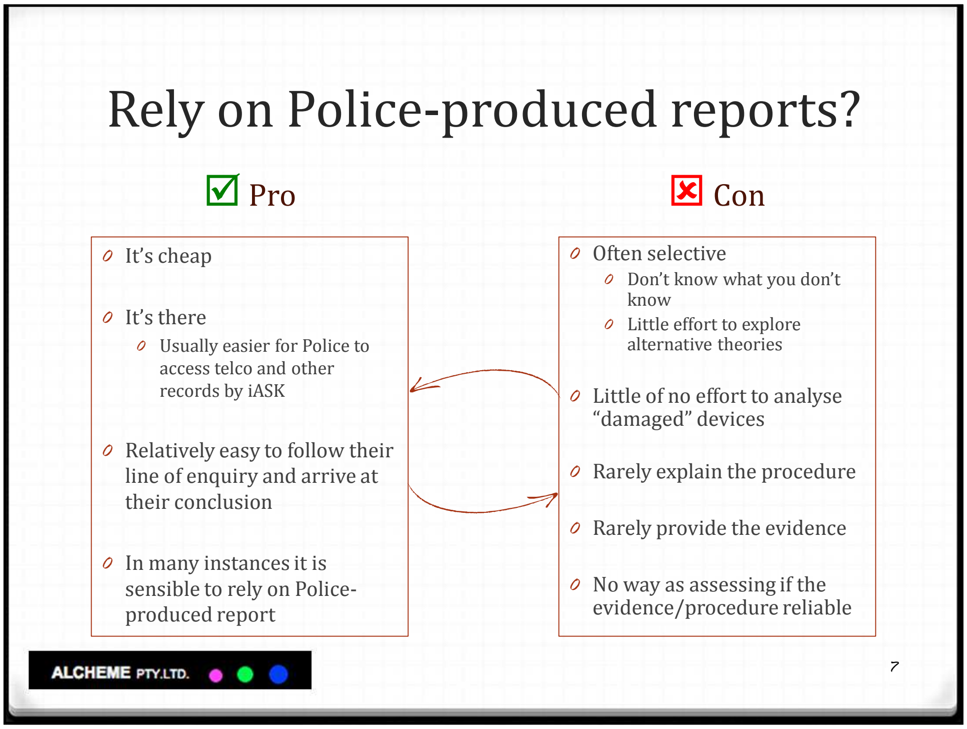
5

Defendant might get

- Report or materials from the OIC, investigator, analyst
- Report from a Police expert, typically from SEEB
- May get CD/DVD/USB with spreadsheets and “extracts”
- For CP and other “sensitive” or “restricted” evidence
  - NSW Police: require examination to be conducted in SEEB office or at Police Station
  - ASIO/AFP: will readily provide material on hard disk

ALCHEME PTY.LTD.

6



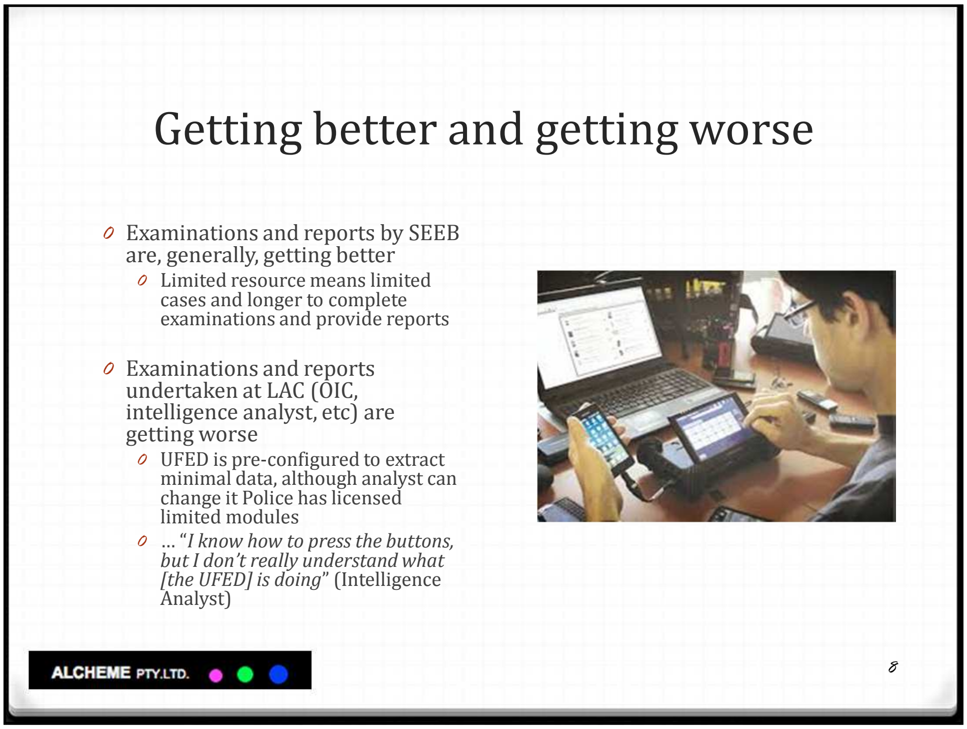
Rely on Police-produced reports?

☑ Pro

- It's cheap
- It's there
  - Usually easier for Police to access telco and other records by iASK
- Relatively easy to follow their line of enquiry and arrive at their conclusion
- In many instances it is sensible to rely on Police-produced report

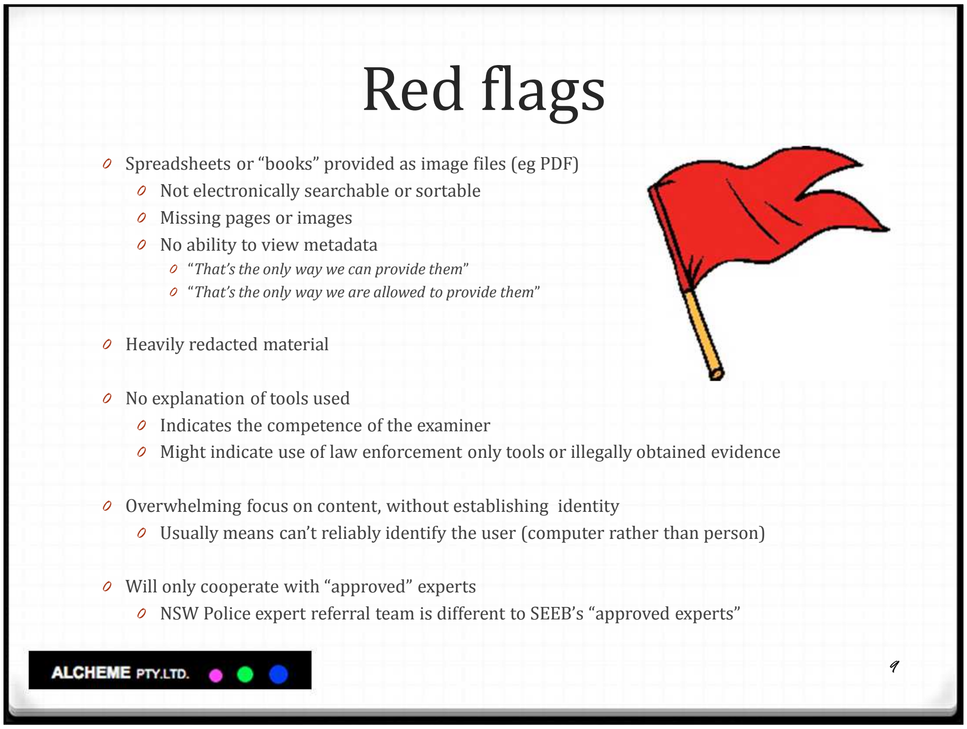
☒ Con

- Often selective
  - Don't know what you don't know
  - Little effort to explore alternative theories
- Little of no effort to analyse "damaged" devices
- Rarely explain the procedure
- Rarely provide the evidence
- No way as assessing if the evidence/procedure reliable



Getting better and getting worse

- Examinations and reports by SEEB are, generally, getting better
  - Limited resource means limited cases and longer to complete examinations and provide reports
- Examinations and reports undertaken at LAC (OIC, intelligence analyst, etc) are getting worse
  - UFED is pre-configured to extract minimal data, although analyst can change it Police has licensed limited modules
  - ... *"I know how to press the buttons, but I don't really understand what [the UFED] is doing"* (Intelligence Analyst)



Red flags

- Spreadsheets or "books" provided as image files (eg PDF)
  - Not electronically searchable or sortable
  - Missing pages or images
  - No ability to view metadata
    - *"That's the only way we can provide them"*
    - *"That's the only way we are allowed to provide them"*
- Heavily redacted material
- No explanation of tools used
  - Indicates the competence of the examiner
  - Might indicate use of law enforcement only tools or illegally obtained evidence
- Overwhelming focus on content, without establishing identity
  - Usually means can't reliably identify the user (computer rather than person)
- Will only cooperate with "approved" experts
  - NSW Police expert referral team is different to SEEB's "approved experts"

ALCHEME PTY.LTD.

9

Enter Passcode
USA TODAY Tech
Is there a way to keep your information safe...
Share
I DO NOT CONSENT TO THE SEARCH OF THIS DEVICE.

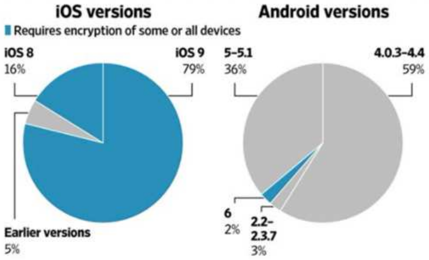
Accessing the device

and other investigative issues relating to encryption

ALCHEME PTY.LTD.

10

Operating System Version



http://bgr.com/2016/03/15/iphone-vs-android-phone-encryption/

- iOS 10.3.x ☑
- Android
  - Lollipop 5.x
  - Marshmallow 6.x ☑
  - Nougat 7.x ☑
- Windows 10 mobile ☑
- Blackberry 10.3.x ☑
- In 2016, Alcheme didn't examine a single device which wasn't protected by at least a PIN

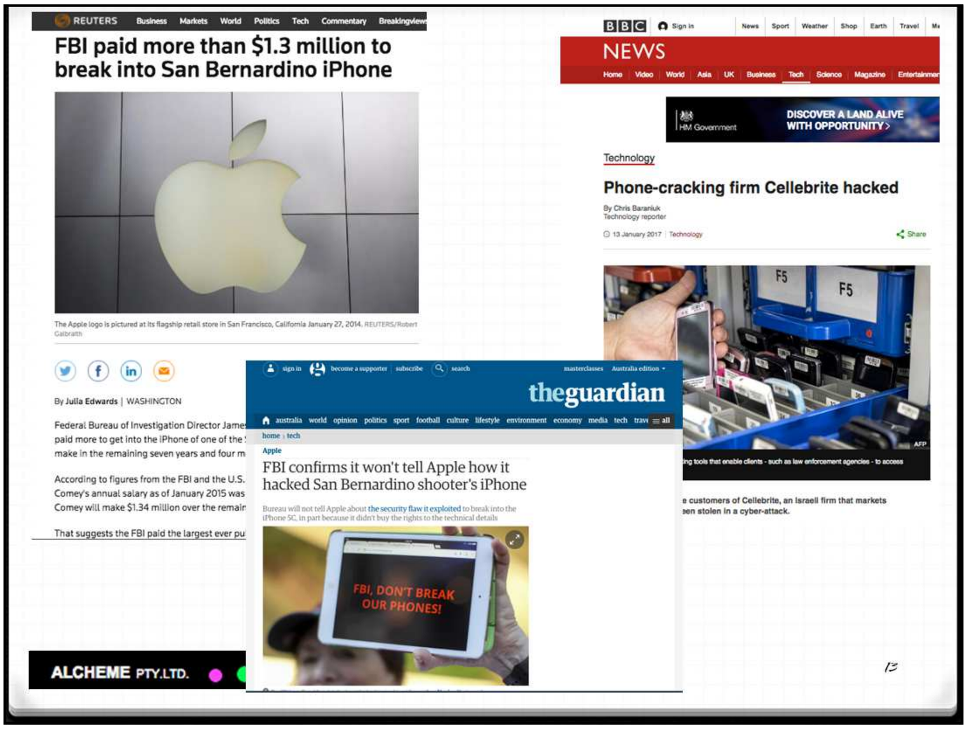
☑ = Encrypted by default or prompted at setup

ALCHEME PTY.LTD.

The emerging problem

- Technology giants such as Apple, Google and Microsoft see protecting their customer's data as a way to differentiate themselves
- Encryption is now almost always set by default (for newer devices)
  - Device is likely to be protected by a PIN/password
- The encryption used on devices has become more reliable than ever before
  - The tool that worked last month doesn't work this month
  - Its more and more unlikely there is a "*crack*"
- Manufacturers are restricting the software that can be installed
  - Now difficult to "*jailbreak*" or "*root*" devices (without the PIN/password)
- Increasingly rely on knowing, finding or guessing the password
  - Need a copy of the device (or at least a backup)
  - The computer(s) used to access the "cloud" version is really useful
  - Might use software from a "*hacker*" or "*cracker*" - difficult to demonstrate procedure is reliable

ALCHEME PTY.LTD.


REUTERS
Business Markets World Politics Tech Commentary Breakingviews
BBC Sign in News Sport Weather Shop Earth Travel
NEWS
Home Video World Asia UK Business Tech Science Magazine Entertainmen
HM Government DISCOVER A LAND ALIVE WITH OPPORTUNITY >
sign in become a supporter subscribe search masterclasses Australia edition
theguardian
australia world opinion politics sport football culture lifestyle environment economy media tech trav all
FBI, DON'T BREAK OUR PHONES!
F5
AFP
Share
ALCHEME PTY.LTD.

FBI paid more than $1.3 million to break into San Bernardino iPhone

The Apple logo is pictured at its flagship retail store in San Francisco, California January 27, 2014. REUTERS/Robert Galbraith

By Julia Edwards | WASHINGTON

Federal Bureau of Investigation Director James
paid more to get into the iPhone of one of the
make in the remaining seven years and four m

According to figures from the FBI and the U.S.
Comey's annual salary as of January 2015 was
Comey will make $1.34 million over the remain

That suggests the FBI paid the largest ever pu

Technology

Phone-cracking firm Cellebrite hacked

By Chris Baraniuk
Technology reporter

13 January 2017 | Technology

ing tools that enable clients - such as law enforcement agencies - to access

e customers of Cellebrite, an Israeli firm that markets
een stolen in a cyber-attack.

home › tech

Apple

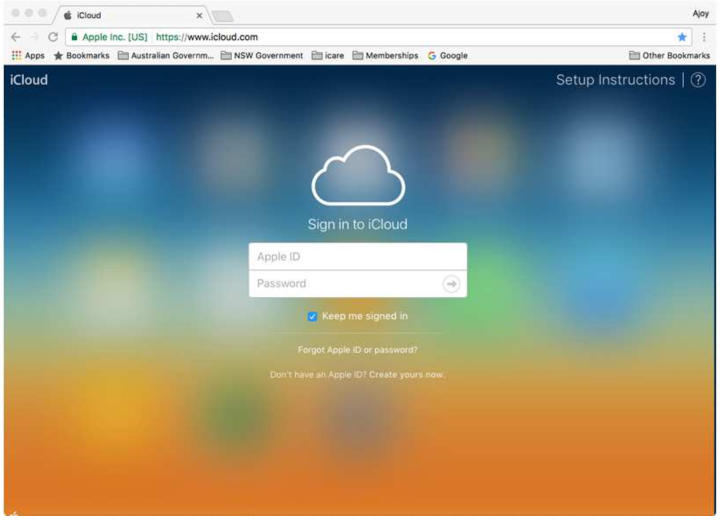
FBI confirms it won't tell Apple how it hacked San Bernardino shooter's iPhone

Bureau will not tell Apple about the security flaw it exploited to break into the iPhone 5C, in part because it didn't buy the rights to the technical details

There are some ways (today)

- The phone or the backup
  - Guess the password
  - Brute-force
    - 48 mins for 4 digit PIN (doesn't include time for set up)
    - 5-7 days for 6 character password
    - 38 years for 8 character password with complexity
- A computer used to access email, etc
  - Extract the token
  - Access the online version (need owner's permission)
  - Most people use the same PIN/password over and over
- "Advanced" security, such as fingerprint and facial recognition is easily tricked (for today's devices)
- Other
  - CCTV or intercept
  - Wear and tear on the screen

ALCHEME PTY.LTD.



iCloud

Setup Instructions | ?

Sign in to iCloud

Apple ID

Password

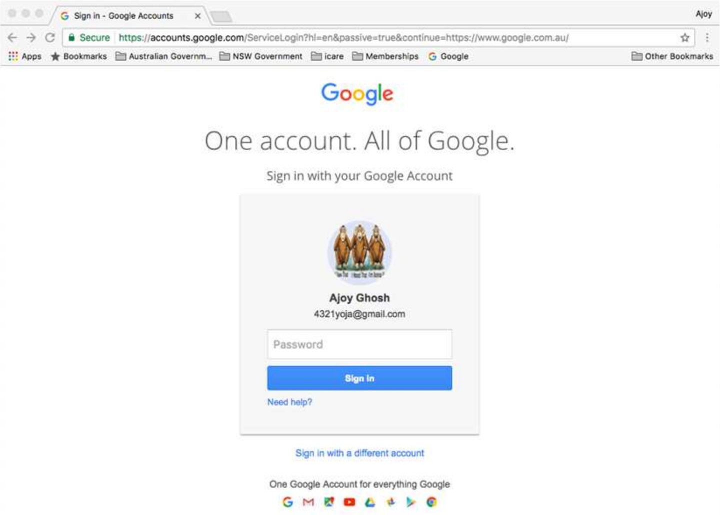
☑ Keep me signed in

Forgot Apple ID or password?

Don't have an Apple ID? Create yours now.

ALCHEME PTY.LTD. ● ● ●

15


Sign in - Google Accounts
Ajoy
Secure https://accounts.google.com/ServiceLogin?hl=en&passive=true&continue=https://www.google.com.au/
Apps
Bookmarks
Australian Governm...
NSW Government
icare
Memberships
Google
Other Bookmarks

Google

One account. All of Google.

Sign in with your Google Account

Ajoy Ghosh

4321yoja@gmail.com

Password

Sign in

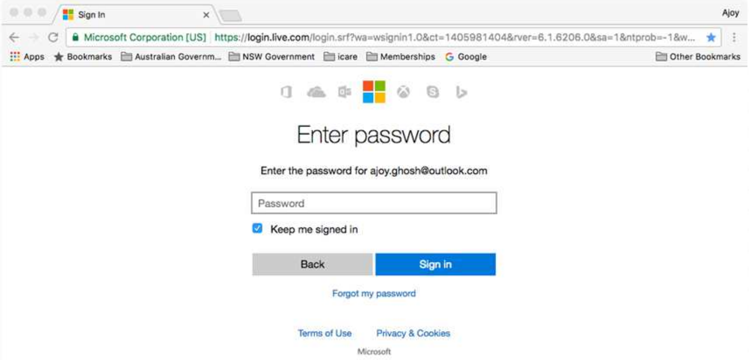
Need help?

Sign in with a different account

One Google Account for everything Google

ALCHEME PTY.LTD. ● ● ●

16



Enter password

Enter the password for ajoy.ghosh@outlook.com

Password

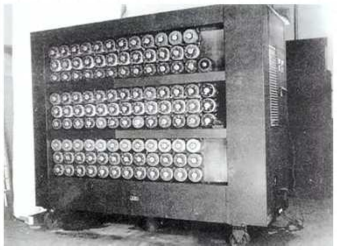
☑ Keep me signed in

ALCHEME PTY.LTD.

17

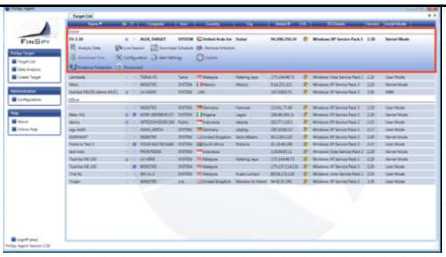
Other challenges

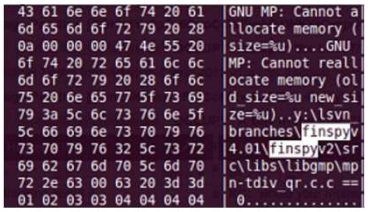
- Language
  - Methods rely on statistical analysis, so need to be familiar with the language
  - Double-byte languages (eg arabic, chinese) are four times the work effort
  - Right-to-left or vertical languages are twice the work effort
- 3rd party and cloud applications
  - Data is not in the “usual” place
  - Data is not on the device
- Subpoena to Apple, Google, Microsoft or Amazon is beyond most defendants
  - Also beyond law enforcement (mostly)
- Manufacturers
  - Once they know its breakable, they fix it
  - Methods are closely guarded and avoid scrutiny of an expert’s report



ALCHEME PTY.LTD.

18





```
43 61 6e 6e 6f 74 20 61  |GNU MP: Cannot a|
6d 65 6d 6f 72 79 20 28  |llocate memory (|
0a 00 00 00 47 4e 55 20  |size=%u)....GNU |
6f 74 20 72 65 61 6c 6c  |MP: Cannot reall|
6d 6f 72 79 20 28 6f 6c  |ocate memory (ol|
75 20 6e 65 77 5f 73 69  |d_size=%u new_si|
79 3a 5c 6c 73 76 6e 5f  |ze=%u)..y:\lsvn_|
5c 66 69 6e 73 70 79 76  |branches\finspyv|
73 70 79 76 32 5c 73 72  |4.01\finspyv2\sr|
69 62 67 6d 70 5c 6d 70  |c\libs\libgmp\mp|
72 2e 63 00 63 20 3d 3d  |n-tdiv_qr.c.c ==|
01 02 03 03 04 04 04 04  | 0..............|
```

Installation of surveillance software

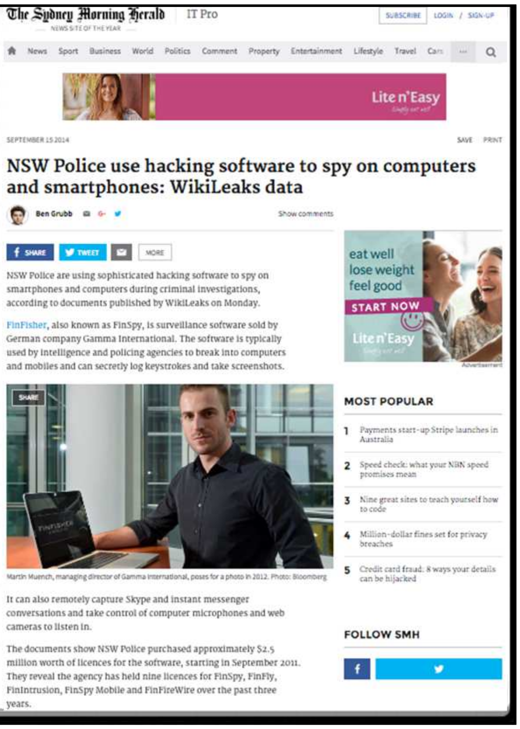
ALCHEME PTY.LTD.

19

A number of cases where Police have withdrawn computer evidence

Increasingly being used by Police, but also:

- Private investigator
- Spouse/partners/family
- Employer/co-workers
- “hackers”



The Sydney Morning Herald IT Pro
NEWS SITE OF THE YEAR

SUBSCRIBE
LOGIN / SIGN-UP
News Sport Business World Politics Comment Property Entertainment Lifestyle Travel Cars

SEPTEMBER 15 2014

NSW Police use hacking software to spy on computers and smartphones: WikiLeaks data

Ben Grubb

Show comments
SHARE
TWEET
MORE

NSW Police are using sophisticated hacking software to spy on smartphones and computers during criminal investigations, according to documents published by WikiLeaks on Monday.

FinFisher, also known as FinSpy, is surveillance software sold by German company Gamma International. The software is typically used by intelligence and policing agencies to break into computers and mobiles and can secretly log keystrokes and take screenshots.

Martin Muench, managing director of Gamma International, poses for a photo in 2012. Photo: Bloomberg

It can also remotely capture Skype and instant messenger conversations and take control of computer microphones and web cameras to listen in.

The documents show NSW Police purchased approximately $2.5 million worth of licences for the software, starting in September 2011. They reveal the agency has held nine licences for FinSpy, FinFly, FinIntrusion, FinSpy Mobile and FinFireWire over the past three years.

MOST POPULAR

1 Payments start-up Stripe launches in Australia

2 Speed check: what your NBN speed promises mean

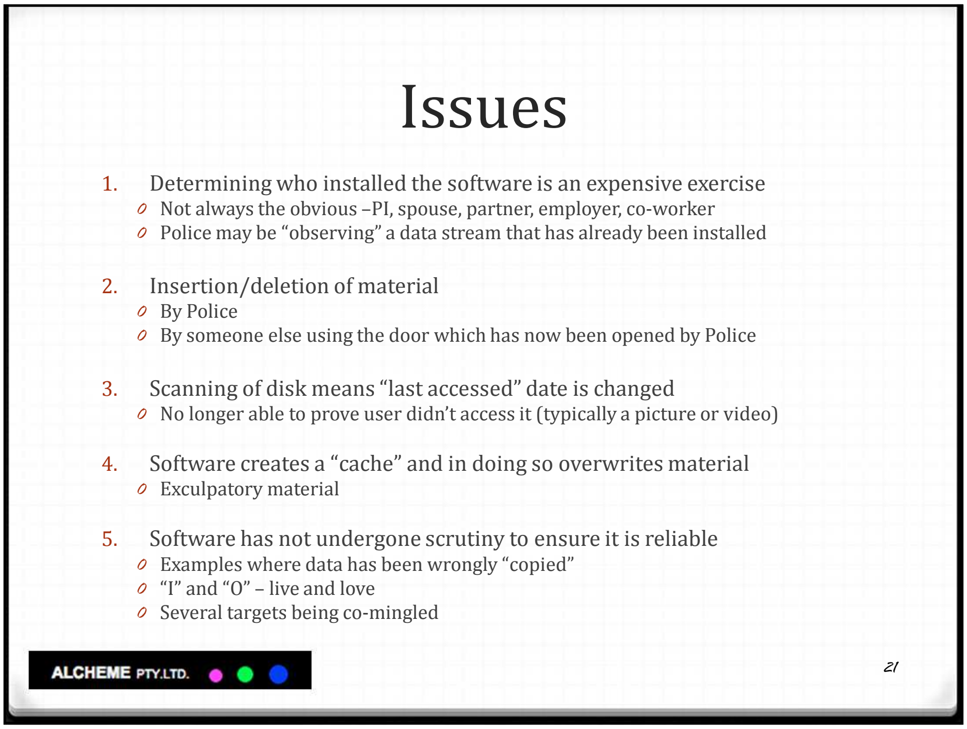
3 Nine great sites to teach yourself how to code

4 Million-dollar fines set for privacy breaches

5 Credit card fraud: 8 ways your details can be hijacked

FOLLOW SMH

ALCHEME PTY.LTD.

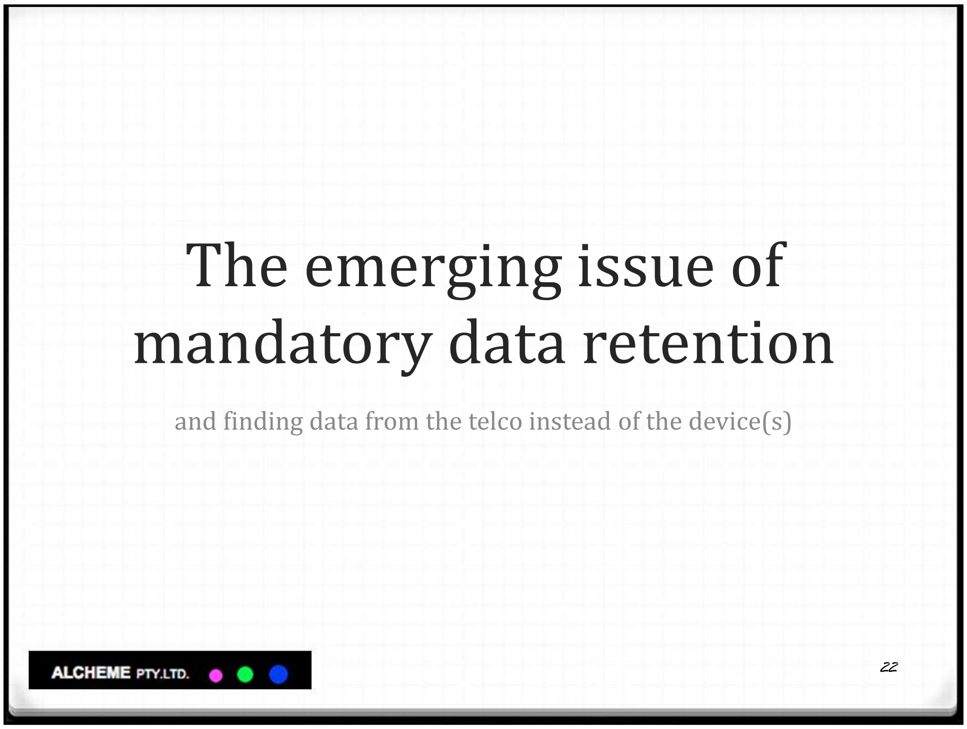


Issues

1. Determining who installed the software is an expensive exercise
   - Not always the obvious –PI, spouse, partner, employer, co-worker
   - Police may be "observing" a data stream that has already been installed
2. Insertion/deletion of material
   - By Police
   - By someone else using the door which has now been opened by Police
3. Scanning of disk means "last accessed" date is changed
   - No longer able to prove user didn't access it (typically a picture or video)
4. Software creates a "cache" and in doing so overwrites material
   - Exculpatory material
5. Software has not undergone scrutiny to ensure it is reliable
   - Examples where data has been wrongly "copied"
   - "I" and "O" – live and love
   - Several targets being co-mingled

ALCHEME PTY.LTD.

21

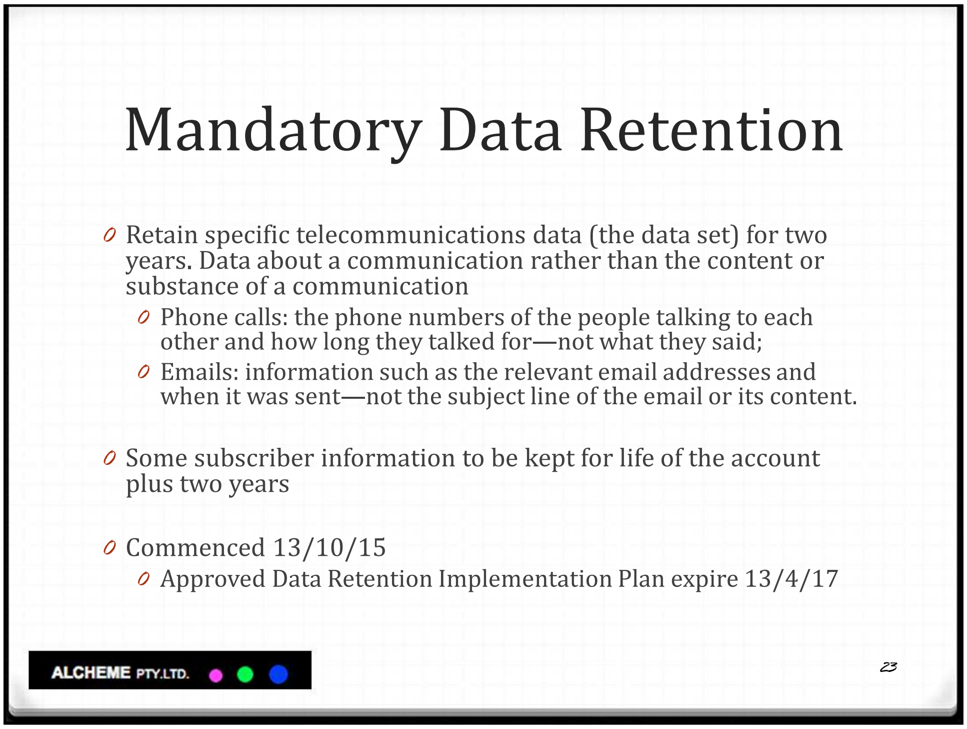


The emerging issue of mandatory data retention

and finding data from the telco instead of the device(s)

ALCHEME PTY.LTD.

22

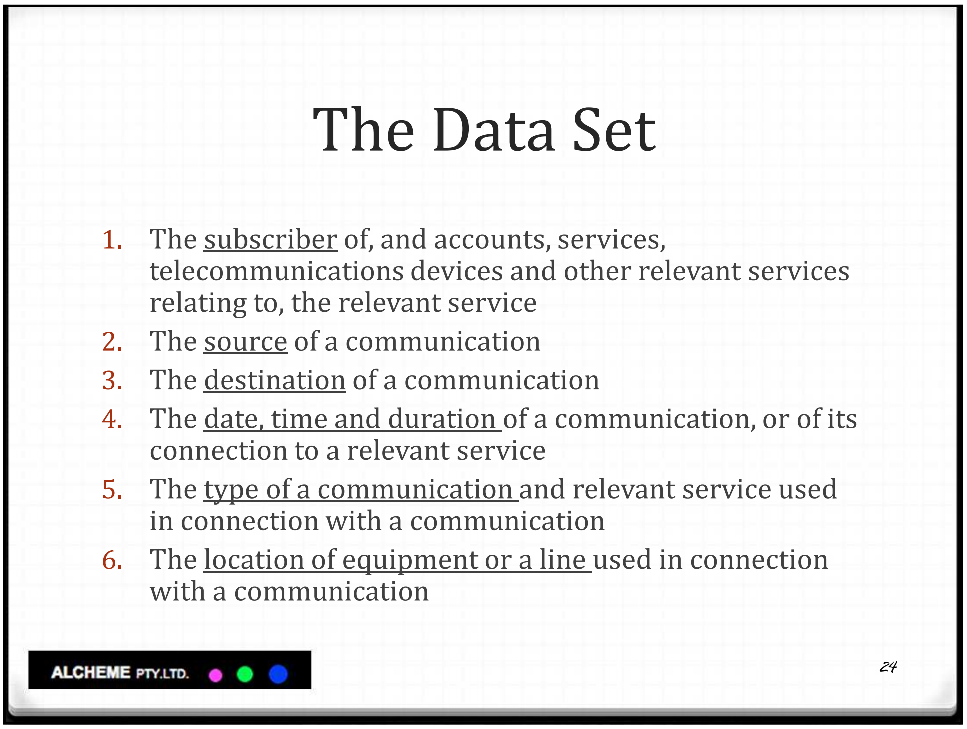


Mandatory Data Retention

- Retain specific telecommunications data (the data set) for two years. Data about a communication rather than the content or substance of a communication
  - Phone calls: the phone numbers of the people talking to each other and how long they talked for—not what they said;
  - Emails: information such as the relevant email addresses and when it was sent—not the subject line of the email or its content.
- Some subscriber information to be kept for life of the account plus two years
- Commenced 13/10/15
  - Approved Data Retention Implementation Plan expire 13/4/17

ALCHEME PTY.LTD.

23



The Data Set

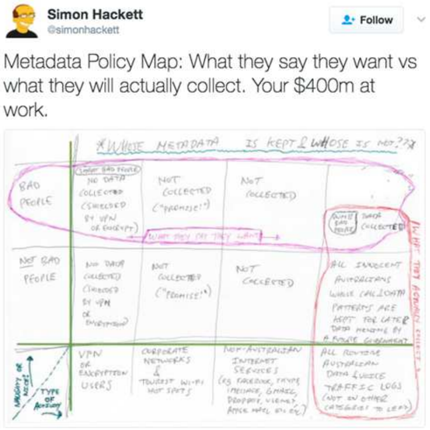
1. The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service
2. The source of a communication
3. The destination of a communication
4. The date, time and duration of a communication, or of its connection to a relevant service
5. The type of a communication and relevant service used in connection with a communication
6. The location of equipment or a line used in connection with a communication

ALCHEME PTY.LTD.

24

Exclusions

1. Does not apply to web browsing histories or the contents of communications
2. Does not apply to a person's "immediate circle"
   - Networks not available to public e.g. workplace management and employees
3. Does not apply to "same area" services
   - Same property or building
4. Does not apply to broadcasting



Simon Hackett
@simonhackett

Follow

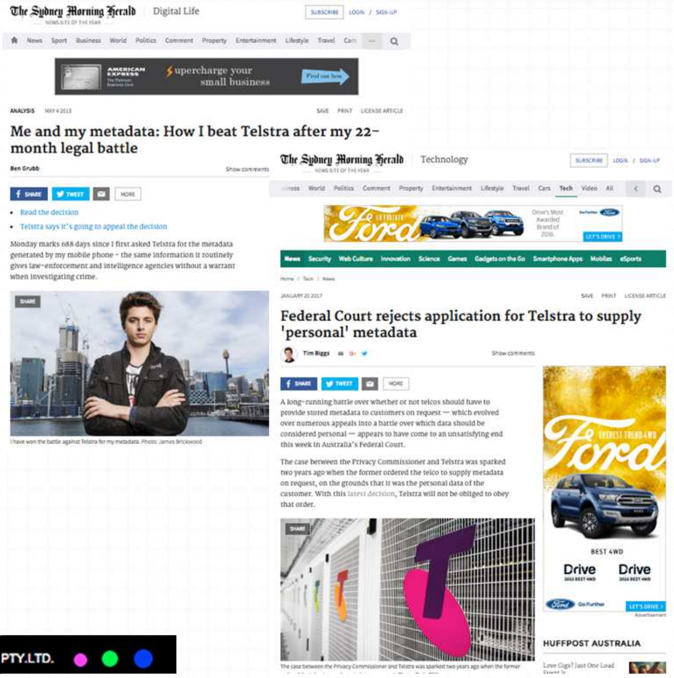
Metadata Policy Map: What they say they want vs what they will actually collect. Your $400m at work.

WHOSE METADATA IS KEPT & WHOSE IS NOT??
BAD PEOPLE
SMART BAD PEOPLE
NO DATA COLLECTED (SHIELDED BY VPN OR ENCRYPT)
NOT COLLECTED ("PROMISE!")
NOT COLLECTED
DUMB BAD PEOPLE
DATA COLLECTED
WHAT THEY SAY THEY WANT
NOT BAD PEOPLE
NO DATA COLLECTED (SHIELDED BY VPN OR ENCRYPTION)
NOT COLLECTED ("PROMISE!")
NOT COLLECTED
ALL INNOCENT AUSTRALIANS WHOSE CALL DATA PATTERNS ARE KEPT FOR LATER DATA MINING BY A FUTURE GOVERNMENT
WHAT THEY ACTUALLY COLLECT
NAUGHTY OR NICE?
TYPE OF ACCESS
VPN OR ENCRYPTION USERS
CORPORATE NETWORKS & TOURIST WI-FI HOT SPOTS
NON-AUSTRALIAN INTERNET SERVICES (EG FACEBOOK, SKYPE, IMESSAGE, GMAIL, DROPBOX, VIBER, APPLE MAIL ETC ETC)
ALL ROUTINE AUSTRALIAN DATA & VOICE TRAFFIC LOGS (NOT IN OTHER CATEGORIES TO LEFT)

https://twitter.com/simonhackett/status/568966153076240385

Safeguards

- Access is limited to a defined list of law enforcement and national security agencies
- Agencies are subject to independent oversight by the Commonwealth Ombudsman, or by the Inspector-General of Intelligence and Security
- Attorney-General reports to Parliament on the operation of the data retention scheme each year
- Where ASIO or enforcement agencies require access to a journalist's data for the purpose of identifying a source, those agencies are required to obtain a warrant, and report all such requests to their independent respective oversight body
- Data retained is personal information for the purposes of the Privacy Act 1988
- Privacy Commissioner assesses telecommunications companies' compliance and monitors industry's non-disclosure obligations



The Sydney Morning Herald | Digital Life

ANALYSIS MAY 4 2015

Me and my metadata: How I beat Telstra after my 22-month legal battle

Ben Grubb

- Read the decision
- Telstra says it's going to appeal the decision

Monday marks 688 days since I first asked Telstra for the metadata generated by my mobile phone - the same information it routinely gives law-enforcement and intelligence agencies without a warrant when investigating crime.

I have won the battle against Telstra for my metadata. Photo: James Brickwood

The Sydney Morning Herald | Technology

JANUARY 20 2017

Federal Court rejects application for Telstra to supply 'personal' metadata

Tim Biggs

A long-running battle over whether or not telcos should have to provide stored metadata to customers on request — which evolved over numerous appeals into a battle over which data should be considered personal — appears to have come to an unsatisfying end this week in Australia's Federal Court.

The case between the Privacy Commissioner and Telstra was sparked two years ago when the former ordered the telco to supply metadata on request, on the grounds that it was the personal data of the customer. With this latest decision, Telstra will not be obliged to obey that order.

The case between the Privacy Commissioner and Telstra was sparked two years ago when the former

News Sport Business World Politics Comment Property Entertainment Lifestyle Travel Cars
SUBSCRIBE LOGIN / SIGN-UP
SAVE PRINT LICENSE ARTICLE
SHARE TWEET MORE
Show comments
News Security Web Culture Innovation Science Games Gadgets on the Go Smartphone Apps Mobiles eSports
HUFFPOST AUSTRALIA

ALCHEME PTY.LTD.

27

Ben Grubb and Telstra

- On 1 May 2015 the Privacy Commissioner determined that Telstra had breached National Privacy Principle 6.1[1]
- Telstra appealed to the Australian Administrative Appeals Tribunal
- On 18 Dec 2015 the Tribunal set aside the Commissioner's determination
  - not "about an individual", rather about operation of Telstra's mobile service
- Privacy Commissioner appealed to the Federal Court of Australia which on 19 Jan 2017 dismissed the appeal[2]

ALCHEME PTY.LTD.

1. Ben Grubb v Telstra Corporation Limited [2015] AICmr 35
2. Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4

28

ACS CERTIFIED PROFESSIONAL
CP
irap
CISA
CISSP

Thank You and Questions

Ajoy Ghosh
ajoy@alcheme.com.au