

A typical Police analysis

Defendant might get

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

Rely on Police-produced reports?

✓ Pro

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

✗ Con

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

ALCHEME PTY.LTD.



7

Getting better and getting worse

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



ALCHEME PTY.LTD.



8

Red flags

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



ALCHEME PTY.LTD.



9



Accessing the device

and other investigative issues relating to encryption

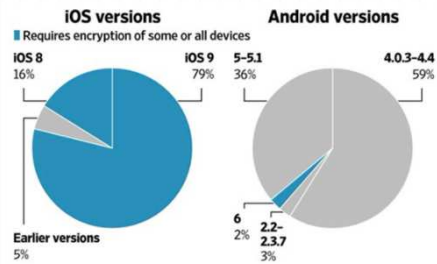


ALCHEME PTY.LTD.



10

Operating System Version



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

ALCHEME PTY.LTD.

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

= Encrypted by default or prompted at setup

//

The emerging problem

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

ALCHEME PTY.LTD.

//

REUTERS Business Markets World Politics Tech Commentary Breaking News

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/Hogart Cabrera

By Julia Edwards | WASHINGTON

Federal Bureau of Investigation Director James Comey paid more to get into the iPhone of one of the suspects in the remaining seven years and four months.

According to figures from the FBI and the U.S. Justice Department, Comey's annual salary as of January 2015 was \$1.34 million over the remainder of his term.

That suggests the FBI paid the largest ever payment to a private company.

ALCHEME PTY.LTD.

BBC NEWS Home Video World Asia UK Business Tech Science Magazine Entertainment

DISCOVER A LAND ALIVE WITH OPPORTUNITY >

Technology

Phone-cracking firm Cellebrite hacked

By Chris Barakuk
Technology reporter

13 January 2017 Technology [Share](#)

Customers of Cellebrite, an Israeli firm that markets its tools that enable clients - such as law enforcement agencies - to access data on stolen smartphones in a cyber-attack.

the guardian Home Tech

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

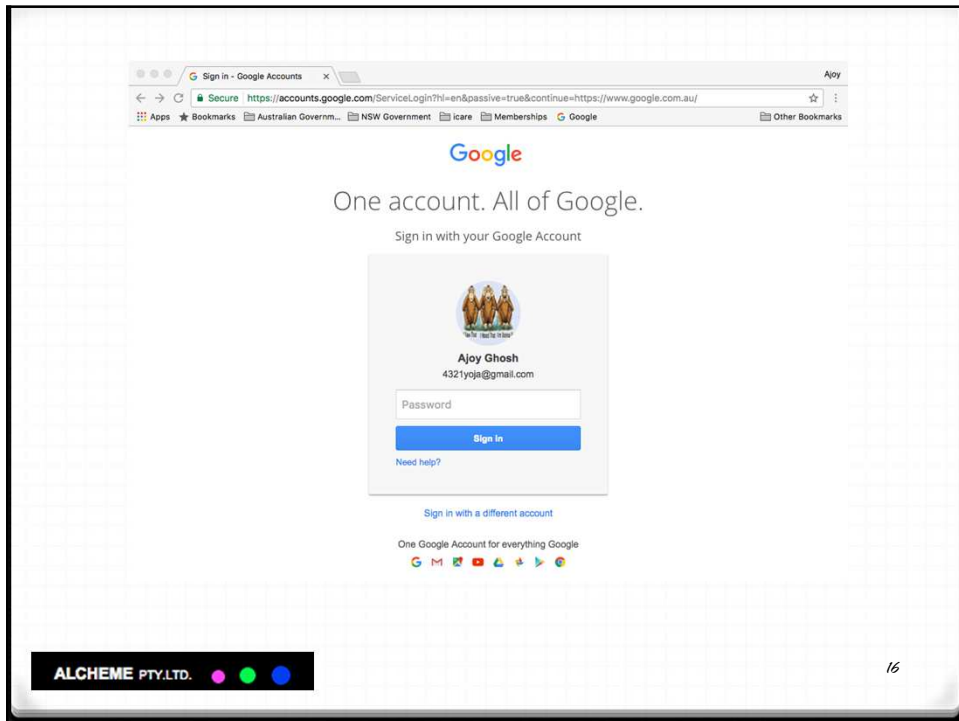
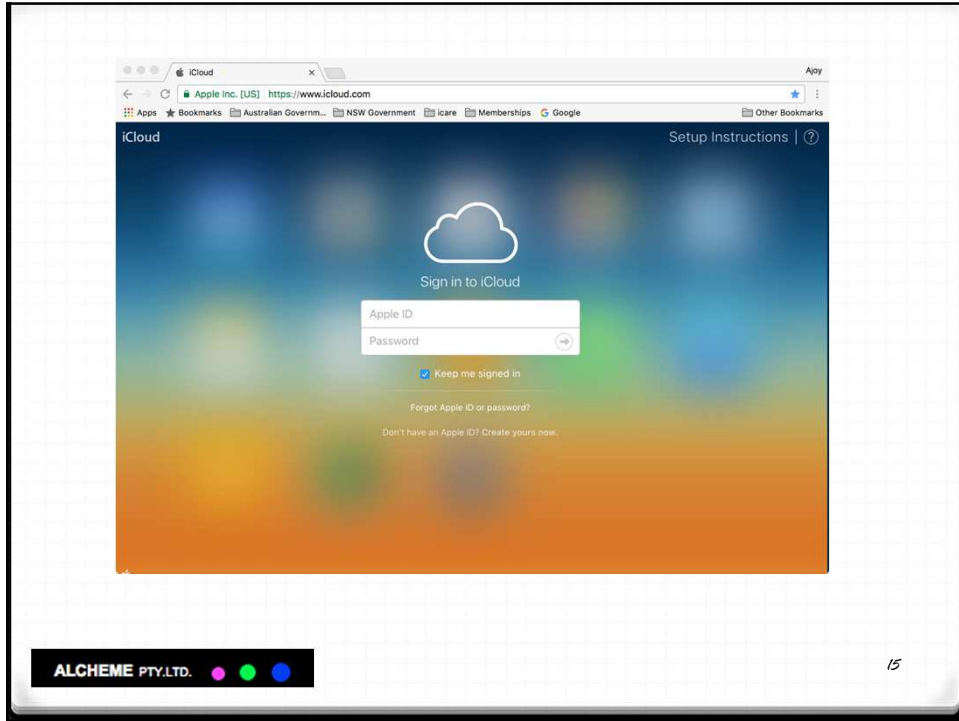
Bureau will not tell Apple about the security flaw it exploited to break into the iPhone 5C, in part because it didn't buy the rights to the technical details

FBI, DON'T BREAK OUR PHONES!

ALCHEME PTY.LTD.

There are some ways (today)

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

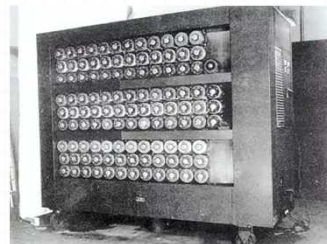


ALCHEME PTY.LTD. ● ● ●

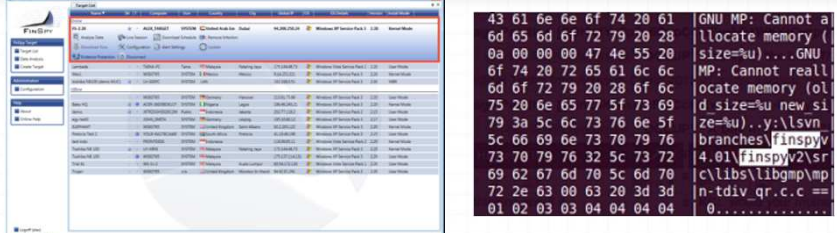
17

Other challenges


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

ALCHEME PTY.LTD. ● ● ●

18




Installation of surveillance software



ALCHEME PTY.LTD.

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"



ALCHEME PTY.LTD.

Issues

1. Determining who installed the software is an expensive exercise
 - o Not always the obvious -PI, spouse, partner, employer, co-worker
 - o Police may be "observing" a data stream that has already been installed
2. Insertion/deletion of material
 - o By Police
 - o By someone else using the door which has now been opened by Police
3. Scanning of disk means "last accessed" date is changed
 - o 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
 - o Exculpatory material
5. Software has not undergone scrutiny to ensure it is reliable
 - o Examples where data has been wrongly "copied"
 - o "I" and "O" - live and love
 - o Several targets being co-mingled

The emerging issue of mandatory data retention

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

Mandatory Data Retention

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



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

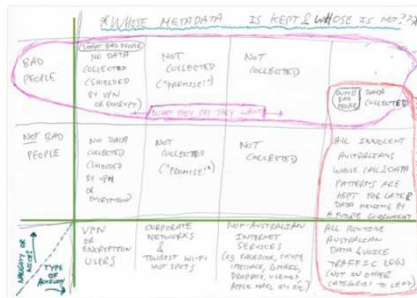


Exclusions

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



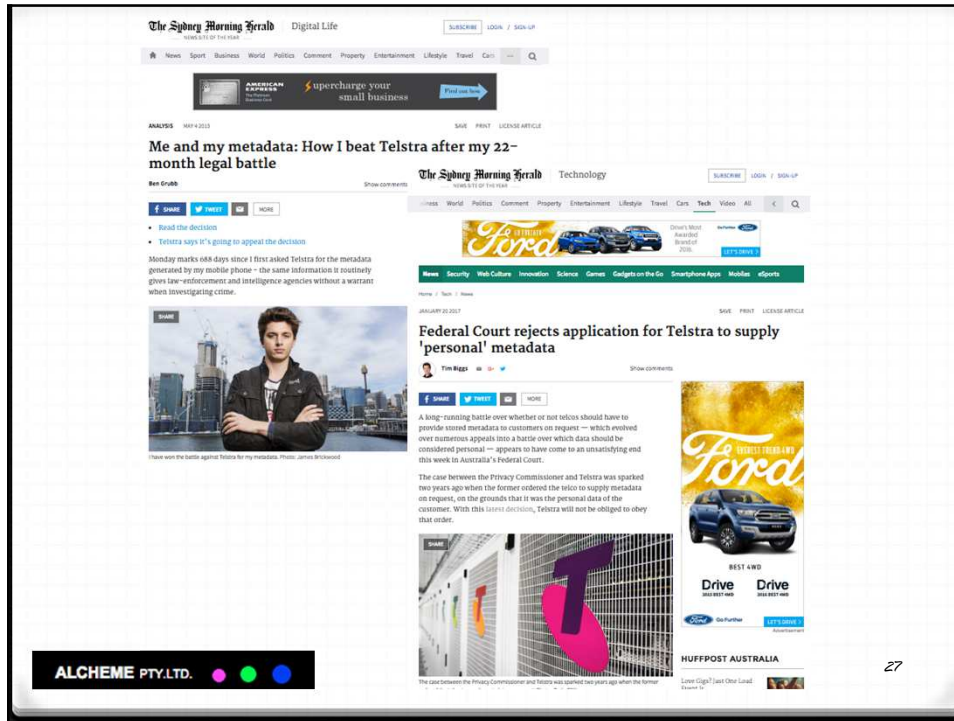
<https://twitter.com/simonhackett/status/568966153076240385>



Safeguards

- o Access is limited to a defined list of law enforcement and national security agencies
- o Agencies are subject to independent oversight by the Commonwealth Ombudsman, or by the Inspector-General of Intelligence and Security
- o Attorney-General reports to Parliament on the operation of the data retention scheme each year
- o 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
- o Data retained is personal information for the purposes of the Privacy Act 1988
- o Privacy Commissioner assesses telecommunications companies' compliance and monitors industry's non-disclosure obligations





Ben Grubb and Telstra

- o On 1 May 2015 the Privacy Commissioner determined that Telstra had breached National Privacy Principle 6.1¹
- o Telstra appealed to the Australian Administrative Appeals Tribunal
- o On 18 Dec 2015 the Tribunal set aside the Commissioner’s determination
 - o not “about an individual”, rather about operation of Telstra’s mobile service
- o Privacy Commissioner appealed to the Federal Court of Australia which on 19 Jan 2017 dismissed the appeal²

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

