

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 realize, and some of it could be used against you if you're ever charged with a crime.

A burgeoning field of forensic study looks at iPhones specifically because of their popularity, the demographics of those who own them and what the phone's technology reveals about its user.

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

So he set out that forward law enforcement. They being tapped by national law enforcement agencies.

50 million iPhones, according to company figures. Clearing out user histories isn't enough to clean the device of that data, said John Mauer, a communications expert and mapping function, as well as national global positioning system applications.

The fine application UltraSnoop is primarily designed to help users locate their own data. But it also can be used to find data on other devices.

There are a number of other applications that can be used to find data on other devices.

Thieves ensure raising goes off with bang

Their methods in finding out what you've done on your phone is not just a matter of time, but of space. It's a matter of where you are when you're using your phone.

When you're using your phone, you're also using a location-based service. And that's where the trouble starts.

When you're using your phone, you're also using a location-based service. And that's where the trouble starts.

Facebook failed to tell police about paedophile porn ring

Dylan Welch

Facebook management failed to tell police about a paedophile porn ring, according to a report by the Australian media.

The failure by the social networking site was discovered during a federal police-led international investigation of the ring, 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 Coughlan.

But despite drawing down the pages after they had been removed, Facebook did not contact police, Mr Coughlan said.

Facebook's disclosure of online accounts of the initial reports for these were indications that, within hours, the groups were re-forming again.

The incident, codenamed Project Orion, was set up by the AFP in March, by June it included the FBI in the US, the Child Exploitation and Online Protection Centre in Britain, the Met and the German Federal Police.

Subsequent police raids on servers involved in the case have included two aged 13 and old from Port Kembla. The company failed to pass the information to police.

The ring leader was identified as a British man who had been in contact with a British public relations company that works for the company and the third person made by the company's chief.

All 11 are accused of creating a network for comment yesterday.

Facebook's failure to disclose information to police was a key factor in the company's decision to sue the company that works for the company and the third person made by the company's chief.

TRACKING YOUR EVERY MOVE

- Every time an iPhone user closes the built-in mapping application, the phone takes a screenshot and stores it.
- iPhone photos are embedded with tags and identifying information, so photos posted online might include GPS coordinates 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.

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

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

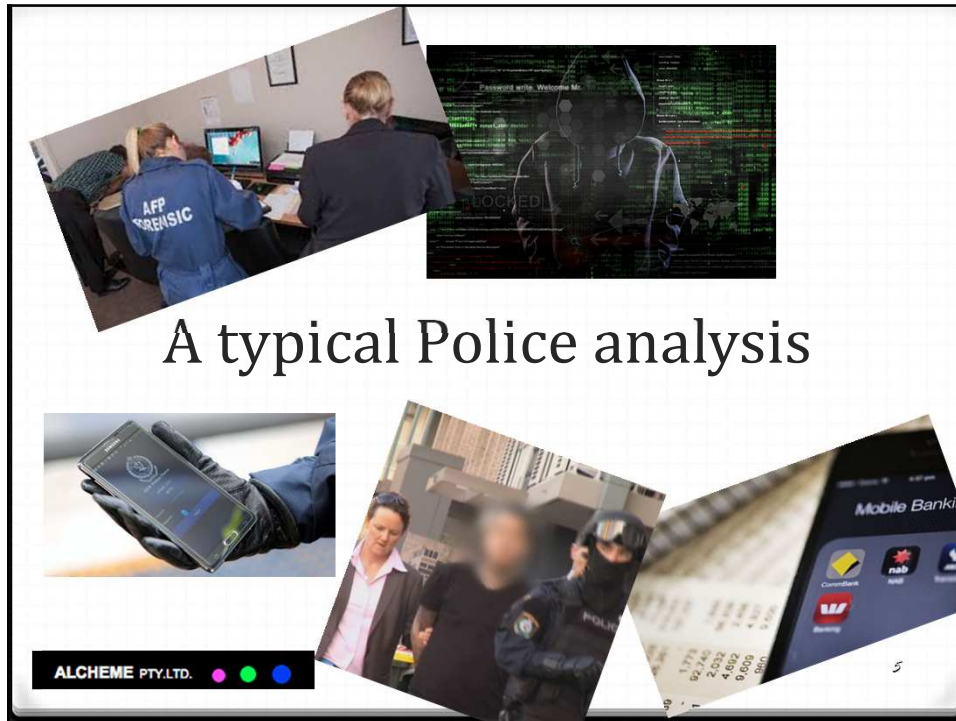
ALCHEME PTY.LTD.

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)

ALCHEME PTY.LTD.

4



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

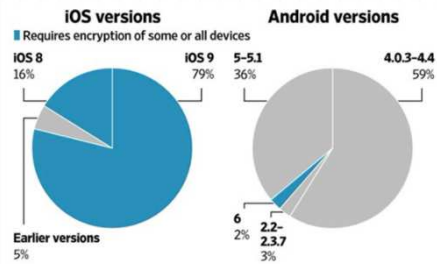


ALCHEME PTY.LTD.



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 BreakingView

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.

the guardian

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

BBC NEWS

Phone-cracking firm Cellebrite hacked

By Chris Barakuk
Technology reporter

13 January 2017 Technology

DISCOVER A LAND ALIVE WITH OPPORTUNITY >

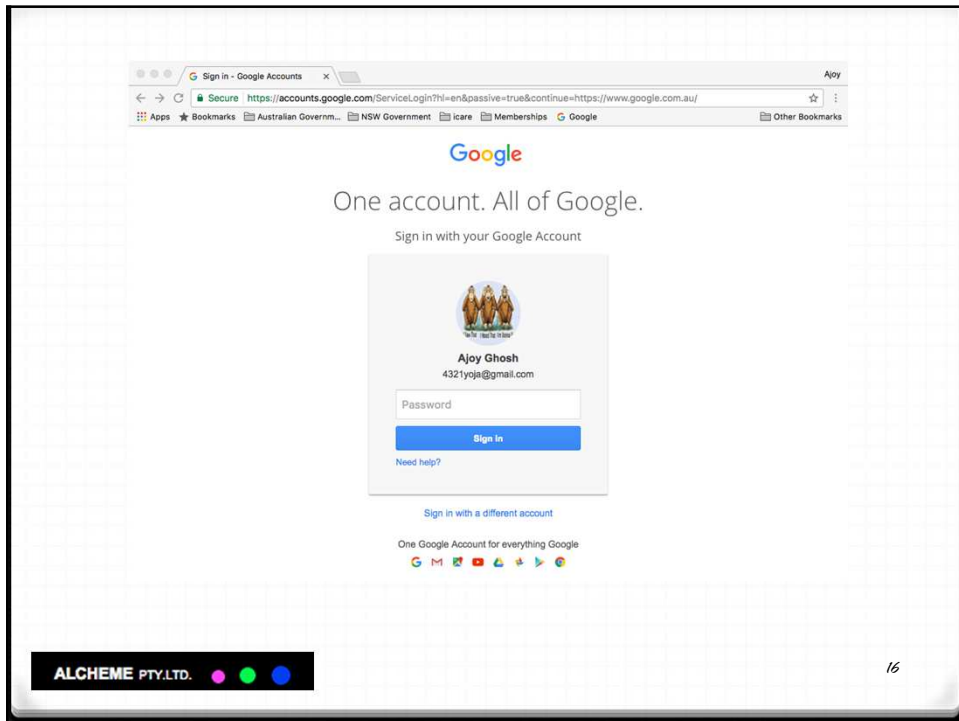
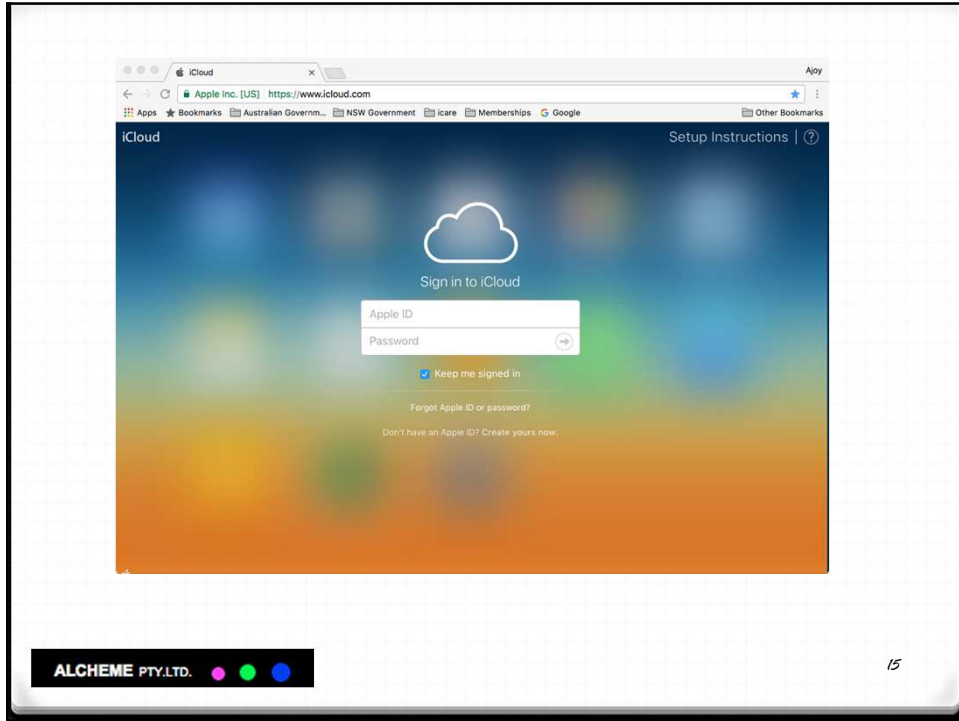
F5 F5

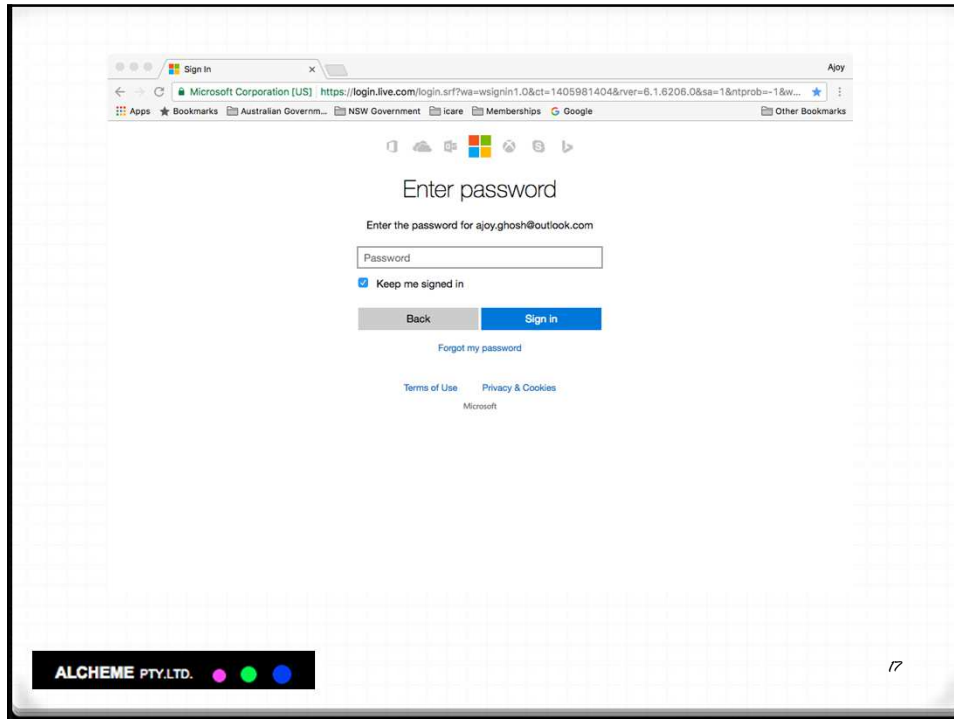
FBI, DON'T BREAK OUR PHONES!

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

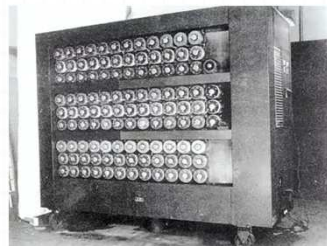




17

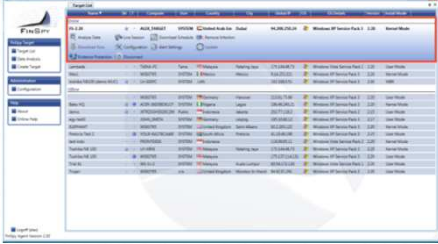
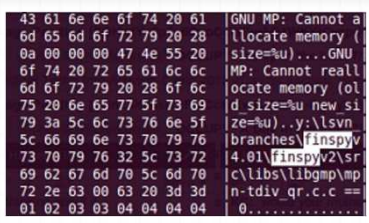
Other challenges

- 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"



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

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

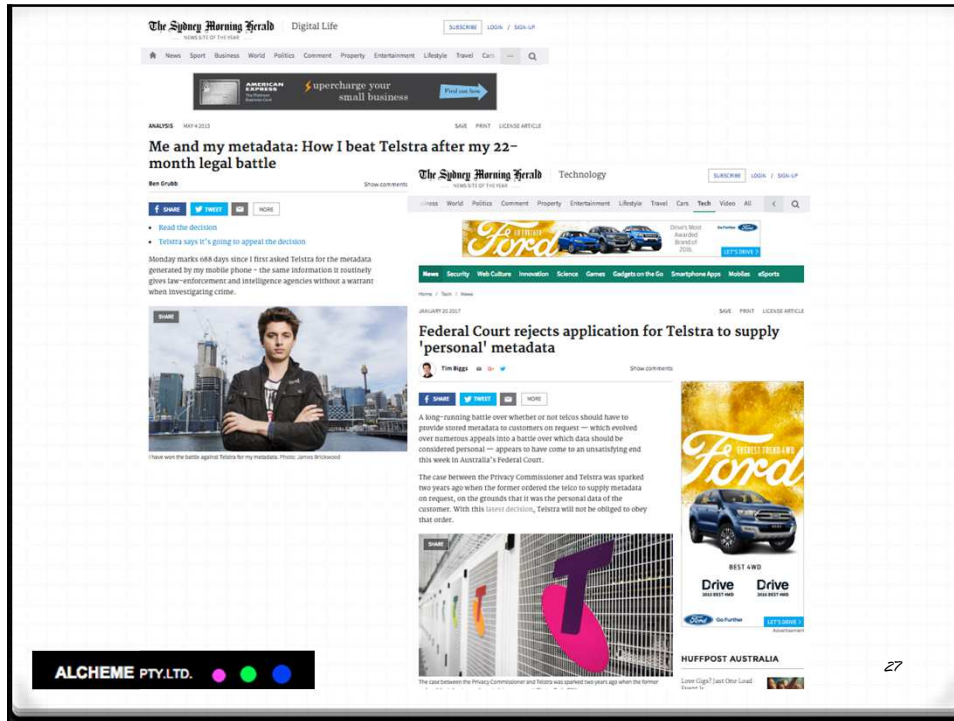
- o Retain specific telecommunications data (the data set) for two years. Data about a communication rather than the content or substance of a communication
 - o Phone calls: the phone numbers of the people talking to each other and how long they talked for—not what they said;
 - o Emails: information 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





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

