

# Look Who's Talking

## 2



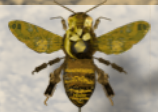
# whoami;

“I don’t know who you are. I don’t know what you want. If you’re looking for ransom, I can tell you I don’t have money; but what I do have are a very particular set of skills; skills I have acquired over a very long career; skills that make me a nightmare for people like you”

- Bryan Mills



So how did we get here?



# What about the Metadata?

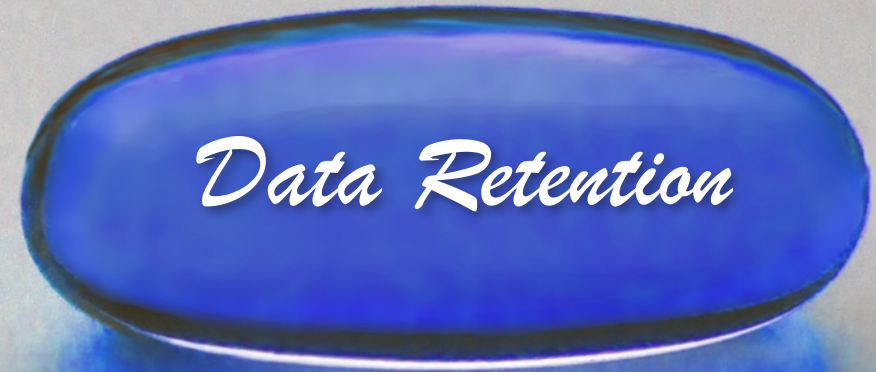


- Suggested by the AFP/AG in 2012
- Came in to being in 2015
- CSP's could defer until 4/17
- \$128m / 180 CSP's (~300) Using this methodology



You take the **blue pill**, the story ends. You wake up in your bed and believe whatever you want to believe. You take the **red pill**, you stay in Wonderland, and I show you how deep the **rabbit hole** goes

-Morpheus



**WHAT IS  
METADATA**

**ART**

**LOVE**

**BIG DATA**

**THREAT INTEL**

**CLOUD**

"When *I* use a word," Humpty Dumpty said, in rather a scornful tone,  
"it means just what I choose it to mean - neither more nor less."

-Lewis Carrol

**RISK**

**Artificial  
Intelligence**

**MEDICINE**

**ARCHITECTURE**

**GOVERNANCE**

**CYBER**



# Is it a Honey-pot for Hackers?



**alastair macgibbon** ✓

@macgibbon

Following



I agree PII is valuable. Telcos have always collected PII: they need it 2 bill u. I just don't agree data retention makes them bigger target

**eyeT Systems** @eyeTSystems

Replying to @macgibbon @zzap @SandraRagg

People rob banks, because of the high value. Less likely to rob Trash & Treasure because low value. PII is valuable, ergo will be targeted.



# What Metadata is Metadata



## Subscriber Information

- Name
- Address
- Billing and contact information



## Source & Destination

- Identifiers, including forwarding, routing, xfer
- FNN
  - IP
  - IMEI
  - IMSI
  - Username



## Time Date Duration

- Start
- End
- Time zone



## Service Type

- Internet
- Wi-Fi
- Voice
- SMS
- (The amount of data uploaded and downloaded by the subscriber)



## Location (at start and end of communication)

- Cell towers
- Wi-Fi hotspot





# What Metadata is NOT Metadata



## Web Browsing History

- URL's
- IP's
- Cookies



Passwords, PINs, secret questions or token codes, which are used for authentication purposes.



## Billing Information for Free Services

- Start
- End
- Time zone



## Content of Communication

- Internet
- Wi-Fi
- Voice
- SMS

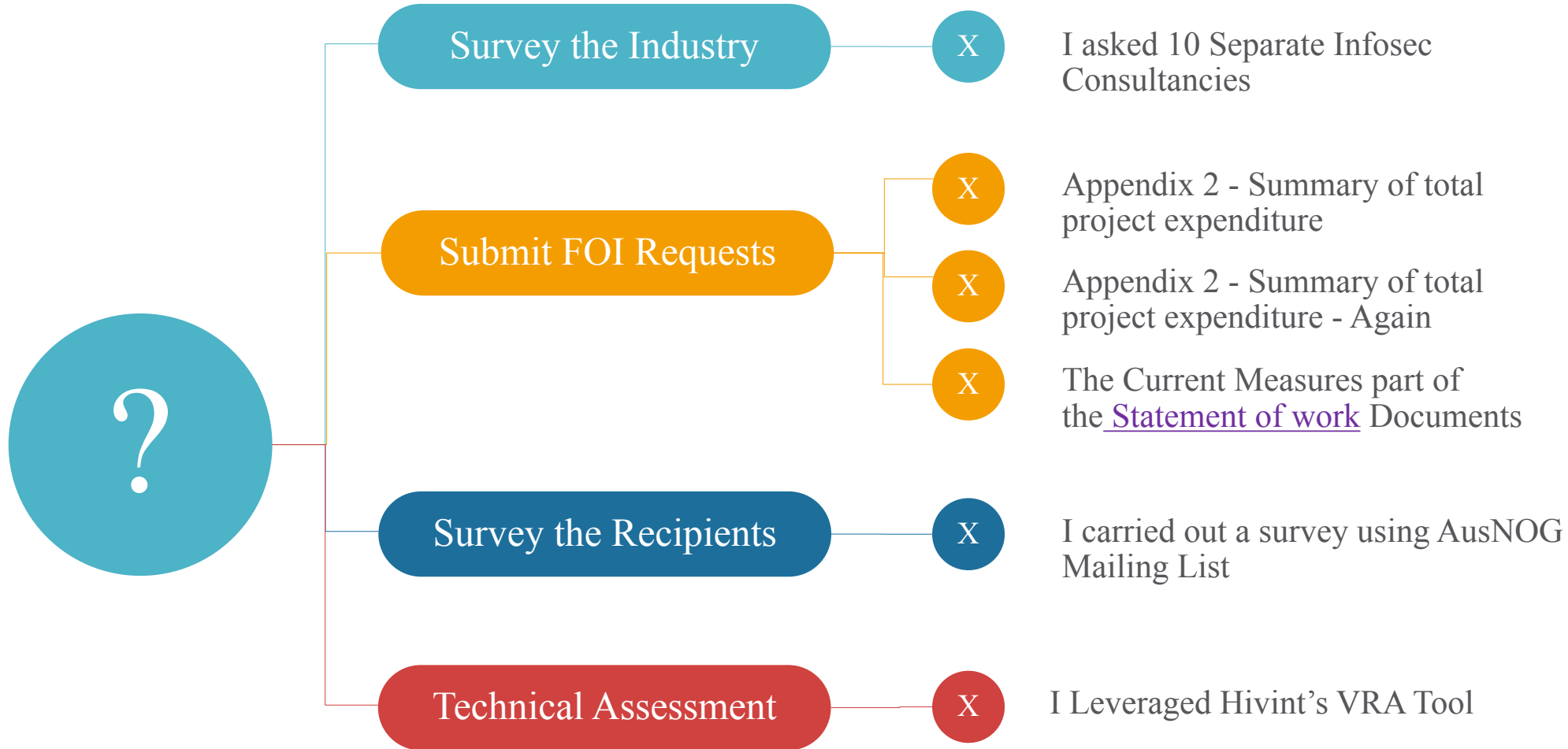


## Ongoing Location

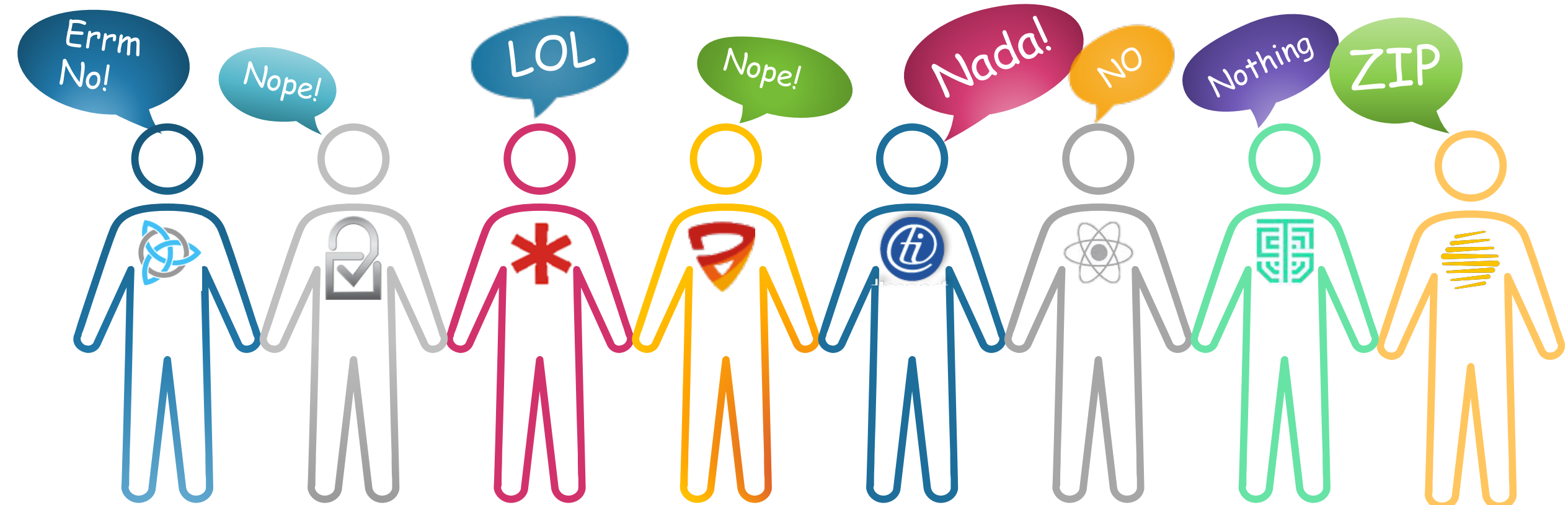
- Cell towers
- Wi-Fi hotspot



# So I was interested to know how secure these ‘hacker honeypot’s’ are:



# Phone a Friend



# FOI Requests

FOI > INFO



# FOI Requests

## Current measures

Describe how you currently secure retained data for this service in line with your obligations. Detail what measures you have in place to protect the information from unauthorised interference or access.

Do not include encryption keys, username, passwords or other similar information.

Data is stored on a SAN running a Linux (s 33) encrypted with (s ) file system. The SAN is on a private network firewalled from the internet, only the required servers plus 2 staff members have access to this SAN. This SAN is physically housed at a Secure Data Centre in (s 22) with the following security features:

- Physical – (s 33)
- Human – (s 33)
- Electronic – (s 33)

(s 22)

S33. National Security  
“Disclosure of this material could reasonably be expected to cause damage to the security of the commonwealth”

S22. Irrelevant Materiel



The metadata is stored in (s 22), (s databases in encrypted volumes in Linux virtual servers that have been built specifically for the purpose of secure storage of the metadata. The volumes were encrypted with the following options:

(s 22), (s 33)

(s 33)

(s 33), (s 47G)

(s 33)

(s 33), the records in the database will also be encrypted.

The metadata is replicated between a primary virtual server in the (s 22) Datacentre and a secondary virtual server in the (s 22) Disaster Recovery site.

The virtual server disks are provisioned in dedicated LUNs on SAN storage.

(s 33) Hard Drive encryption on folders. Encryption key not stored electronically.

All metadata is stored on a secure server deployed only for the purposes of metadata collection within the same data centre as the (s 22) service, only key staff within our organisation have access to this server. The metadata collection server is then backed up daily to a second site using encryption with a 730 day (2 Year) retention period. The backups are stored on a Network storage device purchased for this purpose. Backups of the metadata cannot be interfered with without breaking the backup storage "chain". This ensures that no tampering is possible with the long term and anti-tamper requirements in the Data Retention legislation. Additionally no logs are purged from the Metadata collection server ensuring that there are two copies of the data available, one being live and the other an encrypted backup.

(s 22) stores primary meta data retention in an ISO 27001 secure datacentre with 24 hour onsite security, finger print and swipe card access to the building and additional swipe card access to a locked rack containing our the physical infrastructure.

(s 22) has deployed security best practice with remote access to the primary meta data storage via jump host remote access only with two factor security to core network infrastructure for select senior personnel.

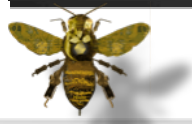
(s 22) has additional secondary storage of meta data which is (s 33) encrypted at rest and additionally sent to our secondary storage via (s 33). Decryption keys are secured out of band of (s 22) network.

Data that is retained as required by the Act is encrypted prior to storage using the (s 33). The encryption keys are stored in two disparate geographical locations in storage that has an Australian Standards 3809:1998 resistance grade of no less than X grade. Access to the retained data can only be made by a Director of the Applicant (as defined by the Corporations Act 2001).

Encrypted database



## Lack of Security Controls (%)



- My Dashboard
- Resource Library
- Breach Intelligence
- Ask Hivint
- Incident Response
- Hivint Research
- Vendor Risk **NEW**
- Private Forums
- Breach Monitor

## Vendor Risk Assessment

Web domain: gmail.com Email domain: gmail.com

Last scan: 2017-08-26

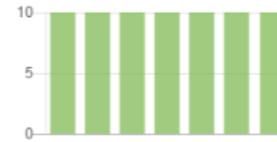
Overall Risk Score



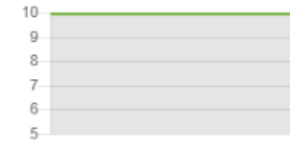
Grade



Last Week



Trend from 2017-02-26



Warning! Your account seems to be registered with a webmail domain. To get most value of this service, please create an account with your corporate email account.

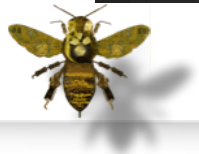
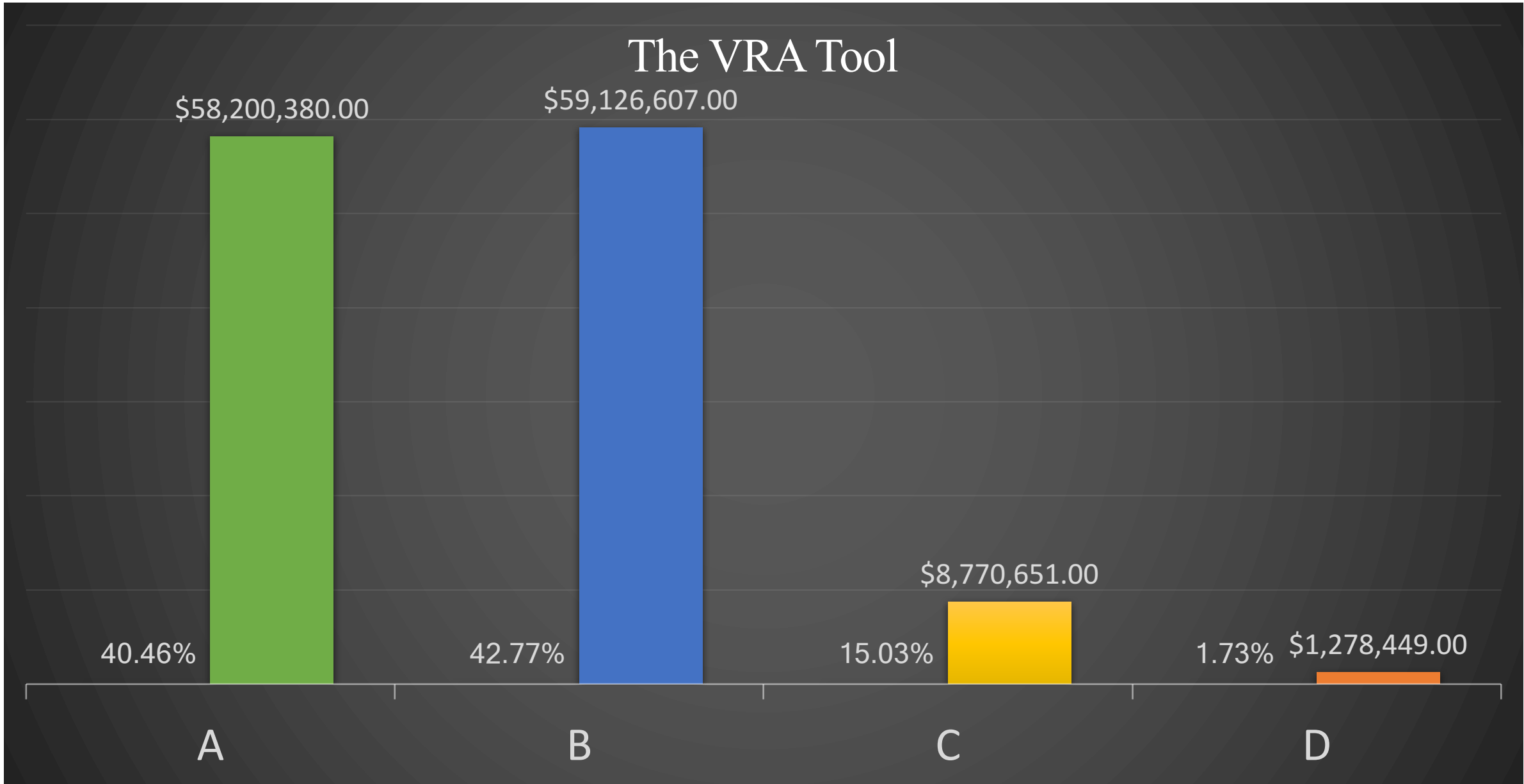
### Result Details

<b>Malware Source</b> Domain not found on Malware Domain List	<b>PASS</b>	<b>Sensitive Ports</b> Subdomains are not found	<b>N/A</b>
<b>Badware Source</b> Domain not found on Desenmascarama Blacklist	<b>PASS</b>	<b>Breached Emails</b> Emails associated with this domain are not found	<b>N/A</b>
<b>Spyware Source</b> Domain not found on the SAGADC Blacklist	<b>PASS</b>	<b>SPF Record Check</b> SPF record was found for the domain	<b>PASS</b>
<b>Risky or Malicious Site</b> Domain not identified by Google as a harmful application source	<b>PASS</b>	<b>DMARC Check</b> DMARC record found for the domain	<b>PASS</b>
<b>Malware Threat</b> Domain not identified by Google as a malware threat	<b>PASS</b>	<b>Domain Expiry</b> The domain is current	<b>PASS</b>





# The VRA Tool



SHALL WE PLAY A GAME?

#TinDerpDerp

# You Totally Need a VPN



Australian Data Retention laws make it completely unsafe for Australians to surf the internet privately; Worry not, hide.me's Australian VPN IPs help you stay anonymous.



Metadata is described as data about data. It shows when a communication took place, the sender and recipient, the devices used, their location, and much more. Although it excludes the communication content, having access to thousands upon thousands pieces of data allows drawing many correct conclusions about your life: from your home and work addresses to which health clinics you visit.



ExpressVPN



Hotspot Shield

Hotspot Shield VPN accused of spying on its web traffic users



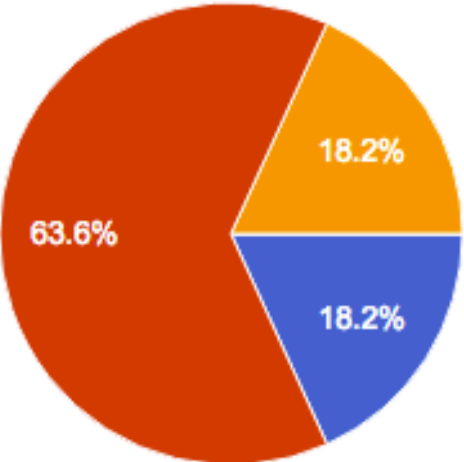
Avira



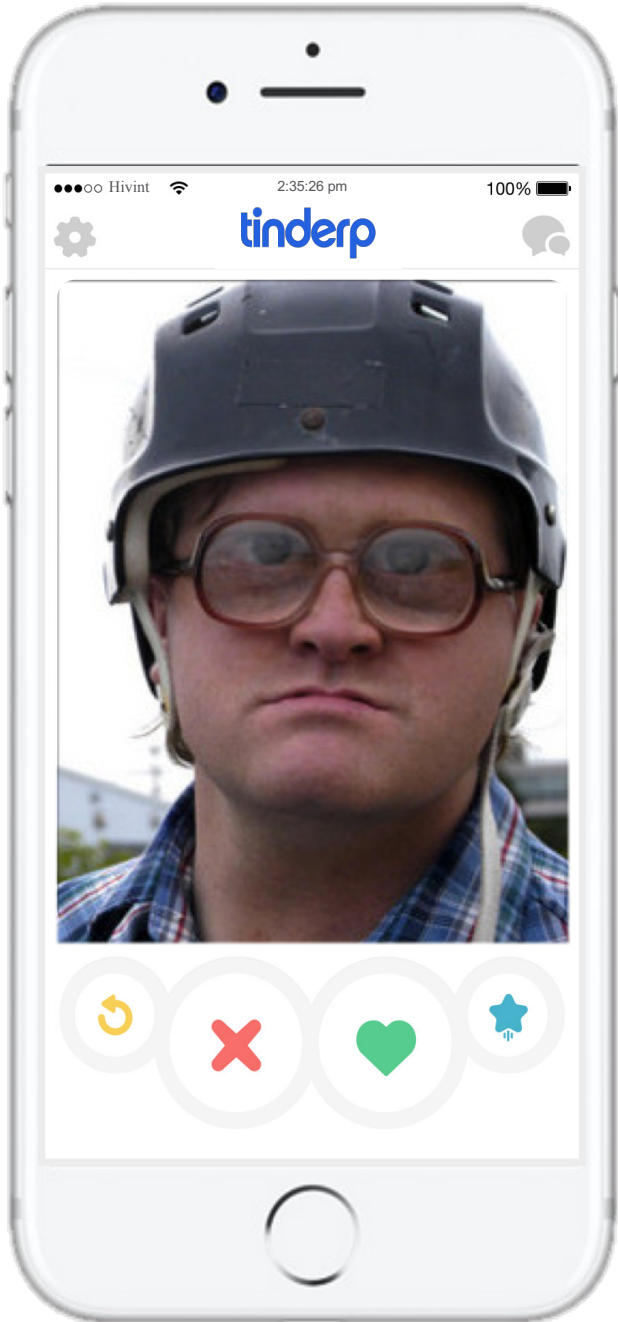
# Telco's were already collecting this info

Did you collect and store any of the information required under this legislation prior to this legislation?

(22 responses)



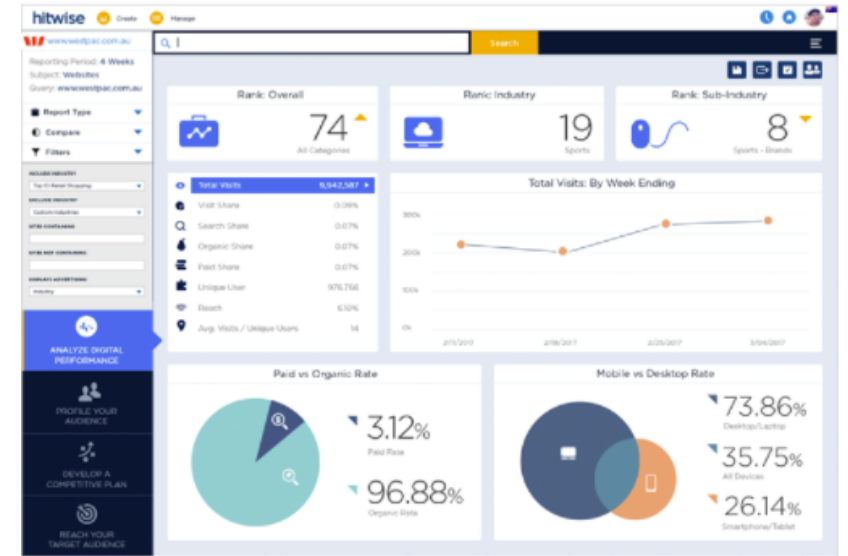
- None of the Info
- Some of the info
- Most of the Info
- All of the Info



# My Data is Private



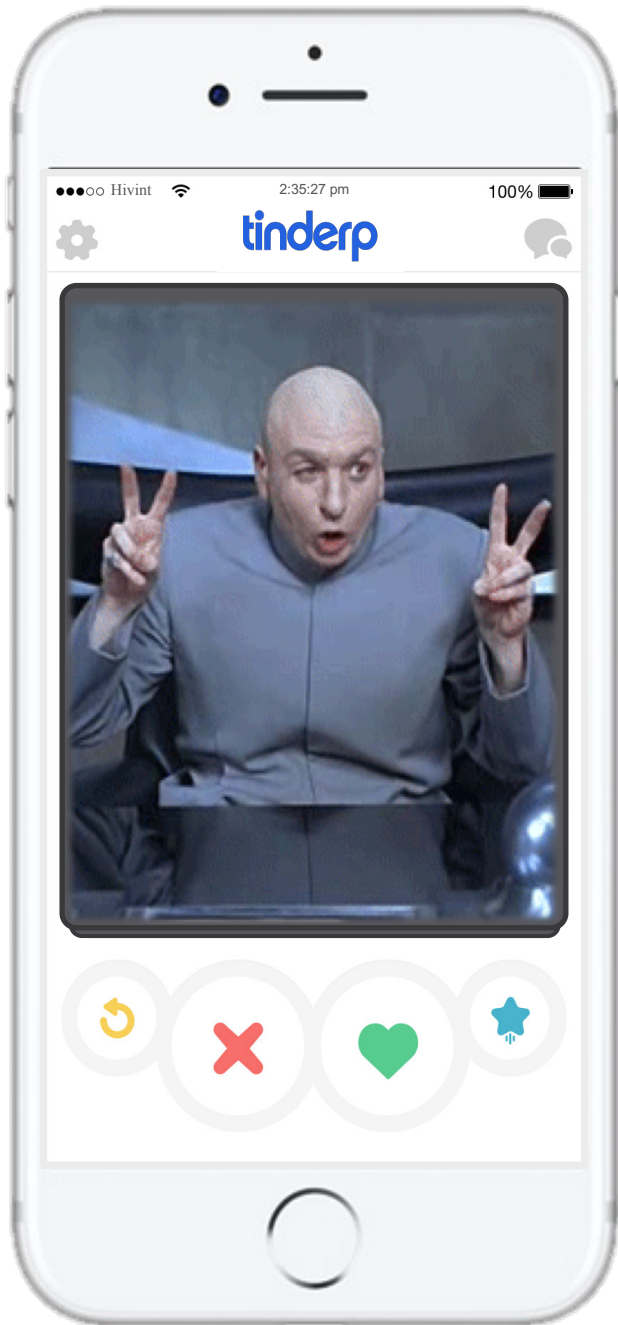
Our intuitive segment builder enables you to pick the exact attributes you need to define any target audience. Build an audience based on consumer characteristics, website visits, search terms and more. There are unlimited combinations.



## Privacy Compliant

Data is sourced from providers who obtain opt-in consumer consent

# It's all about National Security



Crime	# Requests 15/16
1 Illicit Drugs	57,166.00
2 Homicide	25,245.00
3 Miscallanious	12,716.00
4 Robbery	11,795.00
5 Fraud	11,282.00
6 Theft	10,347.00
7 Abduction	10,047.00
8 Unlawful Entry	9,521.00
9 Acts Injury	9,480.00
10 Sexual Assault	9,397.00
11 Weapons	6,864.00
12 Loss of Life	6,237.00
13 Bribery or Corruption	6,146.00
14 ACC Investigation	5,973.00
15 Property Damage	4,956.00
16 Cybercrime	4,482.00
<b>17 Terrorism</b>	<b>4,454.00</b>
18 Dangerous Acts	4,359.00
19 Organised Offences	4,048.00
20 Serious Damage	2,288.00
21 Justice Proceedings	1,328.00
22 Traffic	763.00
23 Pecunary Penalty	407.00
24 Conspire	398.00
25 Public Order Offences	181.00
26 People Smuggling	153.00
27 Public Revenue	85.00
28 Cartel Offences	57.00
<b>Total</b>	<b>427164</b>

# There are safeguards in place



**WA policeman charged over disclosing Ben Cousins secrets to journalist girlfriend**

 Nicole Cox  

**Customs may have misused telecommunications access powers**

**AFP officer accessed journalist's call records in metadata breach**

By [Luke Royes](#)  
Updated 29 Apr 2017, 1:42am

**Police Officers Misuse Private Information for Personal Gain**


By [Ugur Nedim](#) | 20/05/2016 | No Comments

PRINT

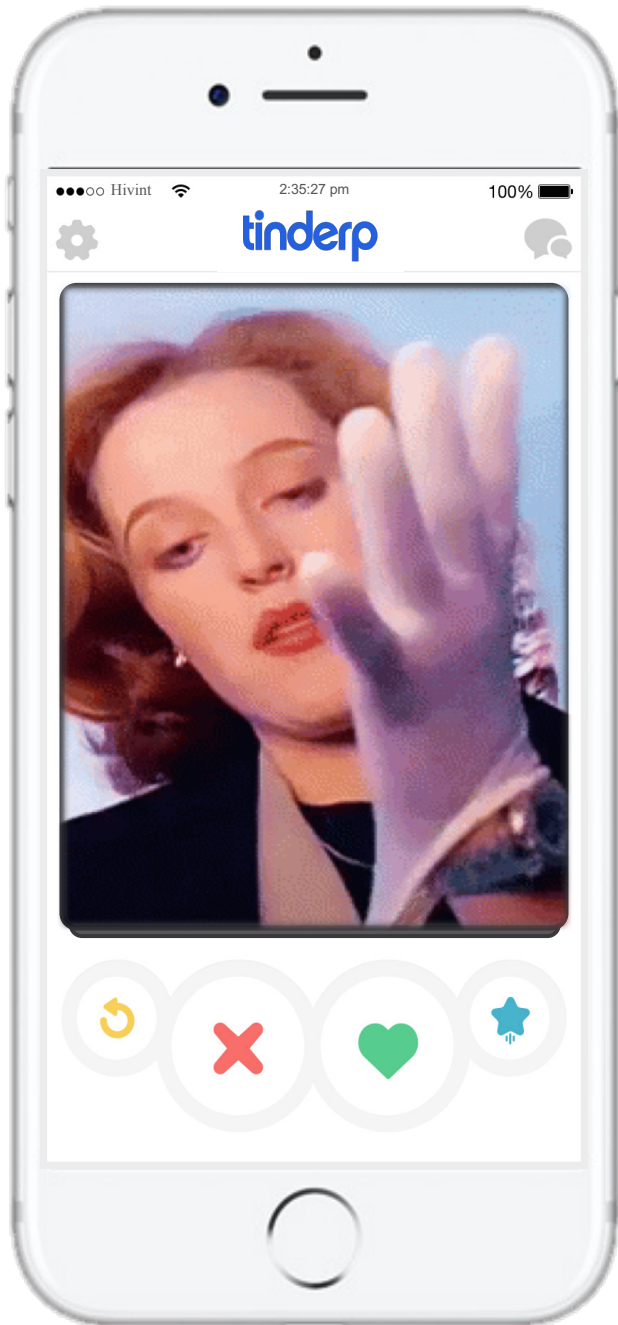
**Police under fire for probing phone records of their own in 'disturbing' breach of officers' privacy**

Renee Viellaris Legal Affairs, CourierMail  
August 30, 2013 12:00am

**A Queensland cop hacked into government databases 50 times to spy on potential dates**

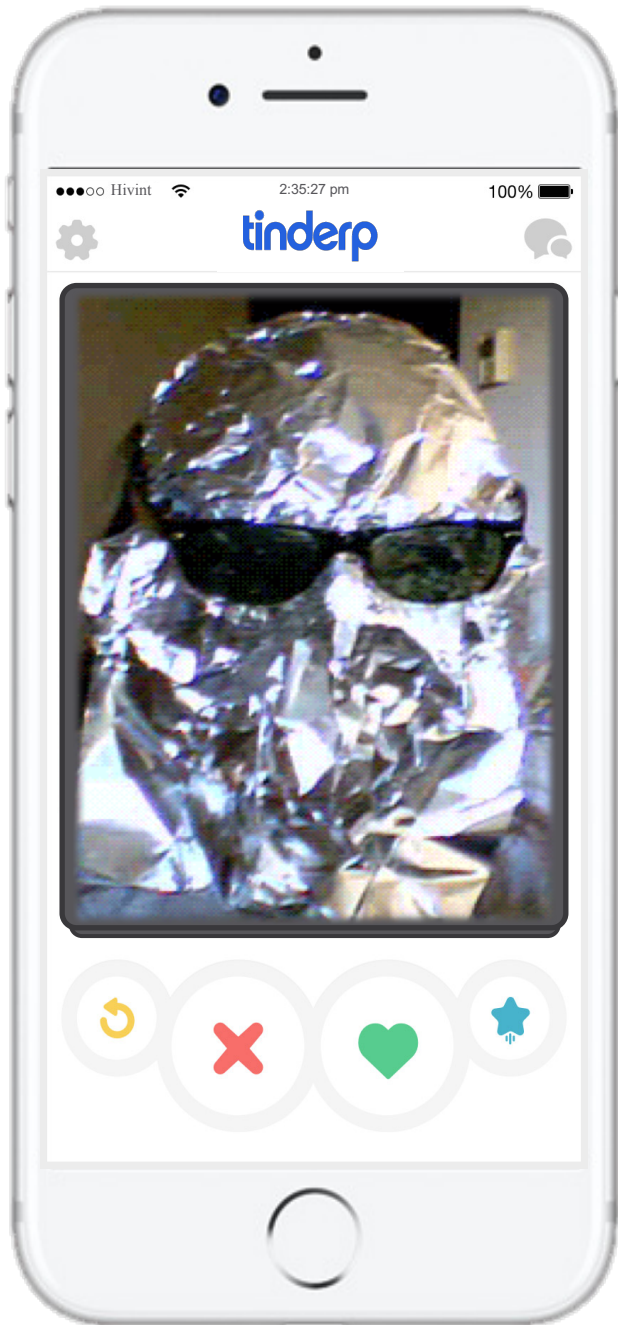
 HARRY TUCKER   
MAY 13, 2016, 11:27 AM 

# It's pointless because <Technology>

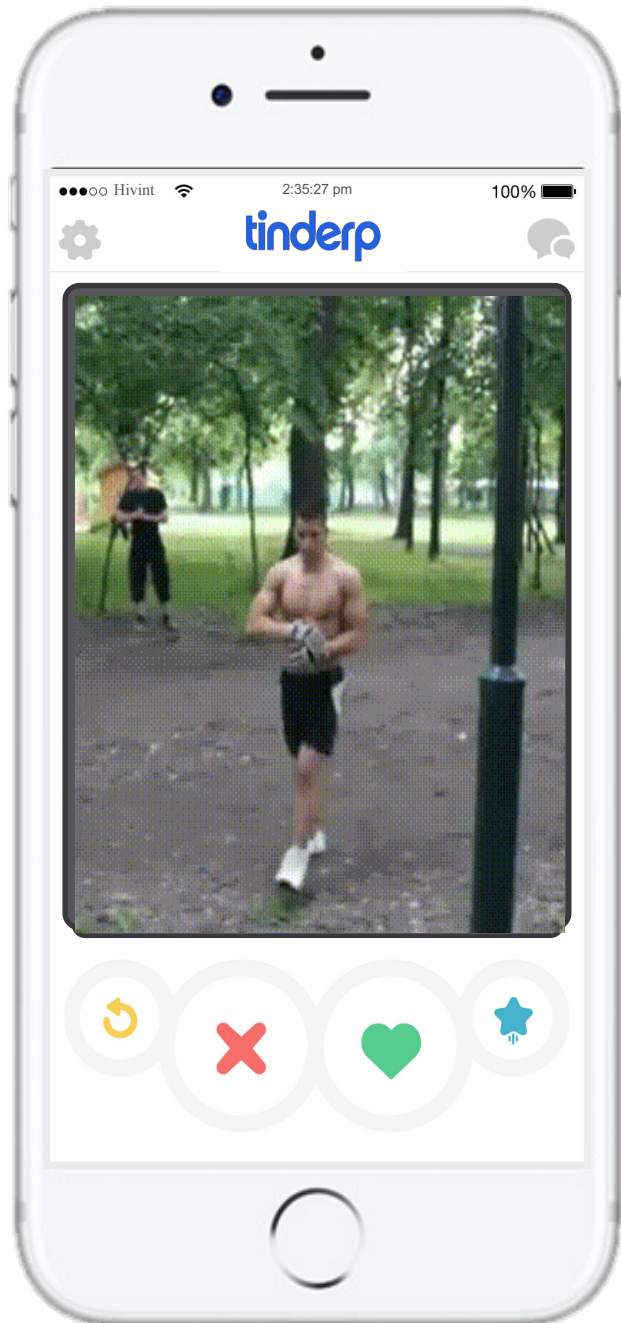




# Metadata is more useful than content



# It's not Personal Identifiable Information



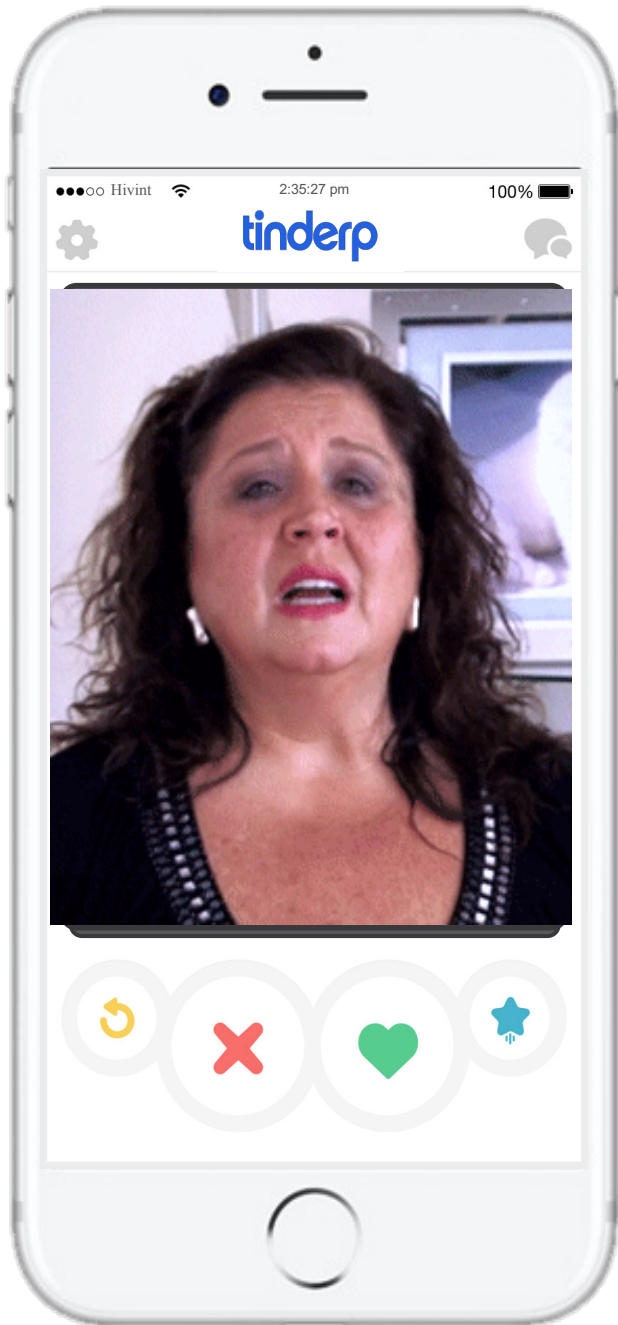
"*personal information* " means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- (a) whether the information or opinion is true or not; and
- (b) whether the information or opinion is recorded in a material form or not.

In 2013 such a breach notification scheme was recommended by the Parliamentary Joint Committee on Intelligence and Security, and then again was recommended in February 2015 by the committee in response to the inquiry into the data retention bill.

The telecom data retention laws were passed with a provision making it very clear that data that is required to be kept under the new data retention provisions is to be considered 'personal information' under the Privacy Act

# It will bankrupt the ISP's



- PWC priced this at between \$118 and \$130 per record
- The communications Alliance came out with a report that said that iiNet said it would add AU\$130 to every bill every year.
- Brandis said between \$1.83 and \$6.11 per record (breakdown)
- The Govt supplied 128m (But didn't release it until Sept 2016)
- The Australian National Audit Office conducted an audit of the government's Data Retention Program.
- Nobody has mentioned the fact that the agencies for satisfying these requests are offering it to Individuals starting at \$100 per record
- The TIA Report put the industry's cap on this at \$200 million

Information request	Cost (per service)
Click on the "View sample data" button to confirm that you are ordering the correct information.	
Basic Customer Information	No cost
Outgoing call and SMS details for mobile phones / fixed phone services:	\$25 (GST incl.) <sup>2</sup> for records equal or less than 1 year old  \$40 per hour (GST incl.) for records older than 1 year
Data sessions for mobile phones / mobile devices: only available for 6 months	\$25 (GST incl.) <sup>2</sup>
BigPond broadband service information (Information more than 2 years old may not be available)	\$40 per hour (GST incl.) <sup>3</sup>
Detailed cell tower location for mobile phones / mobile devices (only available from November 2013)	\$40 per hour (GST incl.) <sup>3</sup>

# Conclusions

- Talks like this are best delivered after a really big night out
- New laws do not give the police any more powers
- Don't buy in to the Hype, It doesn't include your browsing data, geolocation data, but
- I believe carriers may have been collecting and selling that to some extent for years.. and
- Some of the 300 odd CSP's will get compromised...
- Customers will find out about breaches (Due to Breach Notification laws) and many smaller ISP'S will end up being acquired by larger ISP's as a result.
- As for the use of Metadata, It's being misused, it's always been misused and it will continue be misused, but the scale of misuse is probably insufficient to abandon the entire concept. More work needs to be done here (The Commonwealth Ombudsman report is a good step).
- A final point about the context of this information....



# How much do 'they' know about you?

And this is what worries you ? ->

- Aus Government
- Your ISP
- Mass Transit Cards
- Your Partner
- Your Parents
- Fitness Trackers
- Store Loyalty



# Thankyou

@ericpink  
[eric@hivint.com](mailto:eric@hivint.com)  
[misterpink@gmail.com](mailto:misterpink@gmail.com)

