

Support those who support the greater good



The Little Bird

How anonymous are we?

Presenter: Rosie Williams | @info_aus | <https://whistleblower.network>

Images: pixabay.com.au

Icons flaticon.com



To do this lesson online aim a QR code scanner at the image or follow the link from
<https://whistleblower.network>

Additional resources

- Guided self help to secure your devices
<https://www.letsgetsafe.org/>
- Data Retention on YouTube https://www.youtube.com/results?search_query=data+retention+australia
- Links of interest
<https://whistleblower.network/2016/11/18/privacychat-faq>
- Events <https://www.meetup.com/CryptoAus-Sydney/>

Government

There are different levels of access government agencies can have of the information generated whenever we contact someone with an electronic device:

1. 'warrantless metadata'

So called 'metadata' that has been generated within the last two years is available to law enforcement agencies without a warrant.

2. data made available once a warrant is granted

All of the 'metadata' created and stored for the past two years on any device with Australian ISP, email or phone accounts as well as the 'content' & subject line of emails, voicemail and your web browsing history can be accessed by law enforcement agencies with a warrant.

It should be noted that the definition between the above categories is not set in stone. What is considered content today can be moved into the category for warrantless access as the definition of what is or is not metadata is not made clear in the legislation and can be changed without the need to change the underlying Act.

3. data collected & stored internationally

The Five Eyes intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States has great powers to access our data. According to Wikipedia:

"The Five Eyes has two types of information collection methods. The first is the PRISM program and the second is the Upstream system. The PRISM program gathers user information from technology firms such as Google, Apple and Microsoft, while the Upstream system gathers information directly from the communications of civilians via fiber cables and infrastructure as data flows past."

What Google Knows

Google compiles enough data to build comprehensive portfolios of most users—who they are, where they go and what they do—and the information is all available at google.com/dashboard. Here are just a few things WSJ reporter Tom Gara found out about himself.

GMAIL
134,966

All of Tom's emails since he first got a Gmail account in 2004. Google also stores his 6,147 chats.

CONTACTS
2,702

Google knows the people that Tom emails the most. At the top is a friend in Egypt.

GOOGLE SEARCH
64,019

Google thinks Tom performs most of his searches around 8 a.m. ET, but this is probably skewed by years spent outside the U.S.

YOUTUBE
9,220

Videos Tom has watched, listed in chronological order, including a series viewed in June about canoes.

ANDROID DEVICES
3

Google knows all of Tom's synched Android phones, including the old Nexus S phone that he gave to his mom.

GOOGLE PLAY
117

That's how many apps Tom has downloaded from Google's store.

WALLET
3

Credit cards (two expired) saved in Google Wallet, plus two shipping addresses and 13 itemized purchases since June 2009.

PASSWORDS
35

Number of website passwords saved in Google's Chrome browser.

DOCS
855

Documents Tom has created, plus the 115 he has opened that belong to other people.

LOCATION
Willunga, South Australia

Due to an unknown glitch, Google bases Tom's location from one of his old Android phones, which he gave to his mother in Australia.

Graphic by
Alberto Cervantes/
The Wall Street Journal

Corporations

Corporations also have access to a multitude of information which can be made available to government agencies under various conditions.

Metadata is generated whenever we take any action with our electronic devices. This data is stored by telcos as operational data and this data was always made available to government agencies without a warrant and also parties to civil disputes via subpoena (eg employers, private citizens in family law disputes, corporations in litigation).

When telcos began charging people in new and different ways, they didn't always keep the same data that law enforcement agencies wanted for their investigations



It was this desire for a standardised set of data for the benefit of law enforcement agencies that prompted the government to establish the Data Retention Scheme, which the government claimed was to be used only to combat the most serious types of crime: Terrorism, child exploitation and organised crime.

In the decades before we started carrying out most of our daily activities online, the collection and use of data was not such a pressing social and legal issue. Now that so much of our daily activities are captured, who has access to it and under what circumstances is a much more controversial issue.

The data that is being collected includes IP addresses, email addresses, phone numbers, and location data.

Although these individual datasets already reveal a lot of your online presence, the real deal is data matching. Once an experienced analyst brings the different datasets together using a common field, a picture of your activities can emerge through the fragments in each dataset.

It's easy to ignore that so much information about us is collected and stored. SnitchHunt was created to educate the public about how our everyday activities are being recorded and what this may mean for us. SnitchHunt puts you in the shoes of a data analyst working for the federal police, using this data to solve the challenges.

There are 2 versions of SnitchHunt. The first is a version designed to be easily done in an evening workshop. The Short Quiz is not scored and requires no registration.


The Hard Quiz is designed to be challenging and takes some time to complete. The Hard Quiz is scored so requires registration of a team name to begin. There are hints to step players through the difficulties but clicking on them results in points lost to you or your team.

You will need to dig into, correlate and pivot on the various metadata sets to catch a whistleblower.


But first we'll learn a little more about the different datasets.

SnitchHunt

IP Address:	115.203.183.254
Search Terms:	fracking australia
User Id:	a4c34410-eebb-4443-bdc0-cc780595eb6d
Full Name:	Laura May
Username:	william02
Email Address:	william02@gmail.com
Address:	31 / 8 Jackson Freeway South Kimberlyfort, SA, 3149
Employer:	
Job Title:	
Source TCP Port:	30035
User agent:	Mozilla/5.0 (compatible; MSIE 5.0; Windows NT 5.2; Trident/3.0)
Date and Time:	22/07/2015 11:26:15



IP Address:	115.203.183.254
Sender email:	hesssonia@smalllake.com.au
Recipient email:	gomezkeith@gmail.com
Email subject line:	Environment
Port:	5885
Date and Time:	07/05/2015 23:20:45



Datasets

Email metadata



Email metadata that is provided to government without warrant includes data from emails sent to and from Australian email providers, including recipient and sender address, time and date, regardless of whether the email was successfully delivered.

It is worth remembering that while metadata is provided to law enforcement agencies without a warrant, access to content is available where a warrant has been granted.

IP Address:	64.29.168.217	IP Address of the router that connects your devices to the internet.
Sender :	kristopher12@smalllake.com.au	
Recipient:	daniel43@ford.biz	
Email subject line:	BAWG Presentation for April 24, 2001 BIC	This is content under the Data Retention Scheme: only available with warrant
Port	3926	
Date and Time:	18/03/2015 10:12:27	

Phone account data

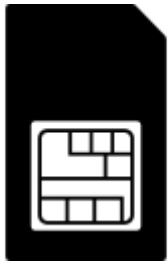


Every phone has a number called an IMEI that is unique to that device. This number is part of your customer records with your phone company along with your basic personal information like name, address and email.

People can be identified by taking information from one dataset and using it search a different dataset. Mouse over the fields for more information on where this data comes from and compare with the other datasets here to see which fields occur in more than one dataset.

Subscriber IMEI:	70487327344081	International Mobile Equipment Identity is a unique number used to identify individual devices to the GSM network
Subscriber Address:	293 Olson Circus Harrisville, TAS, 2819	
Subscriber Email:	blakejohnson@jordan-foley.info	
Subscriber Name:	Crystal Harris	
Subscriber Number	0463-330-779	
Date and Time:	2014-02-13 07:49	

Phone usage metadata



Your IMEI can be used to track your geographical location and find all the records for that device. These records show when calls were made, how long they lasted, when texts were sent, who they were sent to or received from and the locations of each party during the call or text.

The government also has warrantless access to when (and where) you log into and out of your voice mail messages.

Subscriber IMEI:	15336857825067	International Mobile Equipment Identity is a unique number used to identify individual devices to the GSM network.
Subscriber Number:	0	
Dialled Number:	-5741	
Cell Tower Location:	Andre Ground	The Global System for Mobile Communications uses cell towers to relay information to and from your phone. More
Date and Time:		

Google search data



While the Australian government doesn't have direct access to your browsing history, foreign governments collect this data and access can be provided to local authorities. Search engine data varies depending on the information you have provided in your use of the internet and your privacy settings.

IP Address:	225.251.112.80	This is the IP address of the device not the web page. More
Search Terms:	fault	
User Id:	37a83b2b-a317-47bb-b939-cb33a49a5c4f	
Full Name:	Kelly Rodriguez	
Username:	hooperdennis	
Email Address:	hooperdennis@gmail.com	
Address:	9 Lori Route East Jeffreybury, VIC, 2822	
Employer:	Jordan Ltd	
Job Title:	Community development worker	
Source TCP Port:	15078	Port numbers can be used to identify particular services used such as FTP, HTTP or IRC. More
User agent:	Mozilla/5.0 (Windows NT 6.1; sl-SI; rv:1.9.1.20) Gecko/2016-04-17 19:38:23 Firefox/3.6.16	The browser/version used & device type is sent with web activity to customise content. More
Date and Time:	14/01/2015 10:02:32	

Data Matching

Data matching means taking information that appears in more than one data set and finding matching records for it.

For example, when we browse the web or send an email using the same internet connection, the IP address of the router our devices use to access the internet is recorded along with other data about each activity.



Which datasets contain IP address of the device connected to the internet?



Which datasets contain email address?



Which datasets contain home address?



Which datasets real time location information?

Task

You are on the train heading home when your phone starts buzzing. You got a text from your boss, who is asking you to take a look at your work emails. You reluctantly open your mailbox only to find the following email:

From: Finn Coburn <finn.coburn@thepolice.com>

To: data-analysts@thepolice.com

Date: 2016-12-10 10:58

Subject: Fixing a leak at Minecorp

Good morning analysts,

Apologies for the email on the weekend. I am just off the phone with the chief and I need you to work on something asap.

It seems there is a whistleblower at Minecorp leaking to a journalist at MineWatch. Here is the article that just came out yesterday evening:

Anna Dupont: Whistleblower Reveals that Minecorp's WA Fracking Operation Uses Toxic Chemicals (next page)

May I remind you that the mines in Australia are all critical infrastructure, and those leaked docs cannot get into the wrong hands on the black market. Therefore, we need to identify the person of interest to put him/her under ~~scrutiny~~ ^{surveillance}. I need you to dig this guy up for me. As some of you are new hires here, let me reiterate again what is expected from you to do:

We need to know who has been in contact with the journalist. We have taken the data from the cell tower location at Bungana Drive near the mine and we need to match it against the calls to and from the journalist to see if we can narrow it down to a suspect.

#1. You will need to read the article to get the name of the journalist.

#2. You will need to dig into the phone subscriber data to get the full information on the journalist.

#3. You will need to use the journalists phone number search the phone usage data to find out who has been in contact with her.

#4. Once you have the results for calls made to cell towers around the mine, plug it into the phone subscriber data base to identify our potential suspect.

FINN COBURN
CHIEF DATA OFFICER
COMPUTER CRIME SQUAD
Tel: 16131
www.thepolice.com

Article

MineWatch, 9th December, 2016

We still remember vividly not long ago, Western Australia (WA) farmers told ABC News about their Fracking fears in WA 'food basket' Dandaragan, because their freehold farms which they have spent 40 years to build up will be at risk if frackers get on them.

"If the climate keeps drying as it has been, the only way we will be able to grow any crops is by irrigation. And if we foul the aquifers with these chemicals and the gas, then that option won't be open to us." - WA farmer Harry Minty.

Nobody wants to use contaminated groundwater. It is horrifying for anyone having to ventilate their home anytime they take a shower to prevent the build-up of methane in their home and facing the serious risk of losing the sense of smell and taste.

Who can assure Mr. Minty and many other WA farmers and residents that the environment and families are protected?

Firstly, let's take a look at what is fracking and why is it controversial. Fracking is the process of drilling down into the earth before a high-pressure water mixture is directed at the rock to release the gas inside.

Potentially carcinogenic chemicals used may escape and contaminate groundwater around the fracking site. The oil and energy industry suggests pollution incidents are the results of bad practice, rather than an inherently risky technique.



In WA, the Department of Mines and Petroleum (DMP) promises to strive to make WA the first choice for responsible development. DMP, in close cooperation with the Office of Environmental Protection Authority (EPA), the departments of Water, Environment Regulation, Health, and other agencies, ensures responsible practices and energy companies compliance with the legislation of petroleum activities including Hydraulic fracturing for onshore natural gas from shale and tight rocks. Environmental impact assessment and the controls from the fracking license issued by EPA are two of the primary controls to prevent, detect and correct bad fracking practices which negatively affect the environment.

A whistleblower says that the WA mine giant, Minecorp, has been using BTEX (benzene, ethylbenzene, toluene and xylene) chemicals for more than two years. It's confirmed that the Minecorp management is fully aware of such practice, but has no intention to change or disclose it to MDP or EPA.

The whistleblower says it is not surprising that the authorities do not interfere in Minecorp's illegal usage of BTEX chemicals or its poor wastewater storage and disposal processes and facilities. Minecorp has misled relevant authorities by submitting incorrect information to avoid any environmental impact assessment by EPA.

Our environment is important to all of us. Unfortunately, powerful and manipulative commercial organisations often make profits at the cost of environment and the health of the local community. Do we want to threaten places in WA into the future with polluting practices by mine giants like Minecorp? Do we want a legacy of toxic chemicals in our home?

All residents will be eagerly awaiting the responses and actions from EPA and the executives of Minecorp.

MineWatch encourages whistleblowers, and others with access to information they believe should be revealed for the public good, to contact us (see contact details below). You can remain anonymous if you so wish. Please note, we cannot guarantee to respond directly to anything you send here.

Anna Dupont
Investigative Journalist at MineWatch
Email: anna@minewatch.org.au
Phone: +61475212201
Twitter: @annaminewatch

Short Quiz

Q1. What's the name of the journalist at Minewatch?

Q2. What is the phone number of the journalist?

Q3. Which dataset would you search to find an address for the journalist?

Q4. Which field in the phone usage metadata gives the general location of the device?

Q5. Which field in the email & google search datasets gives a location for the device used to access the internet from it?