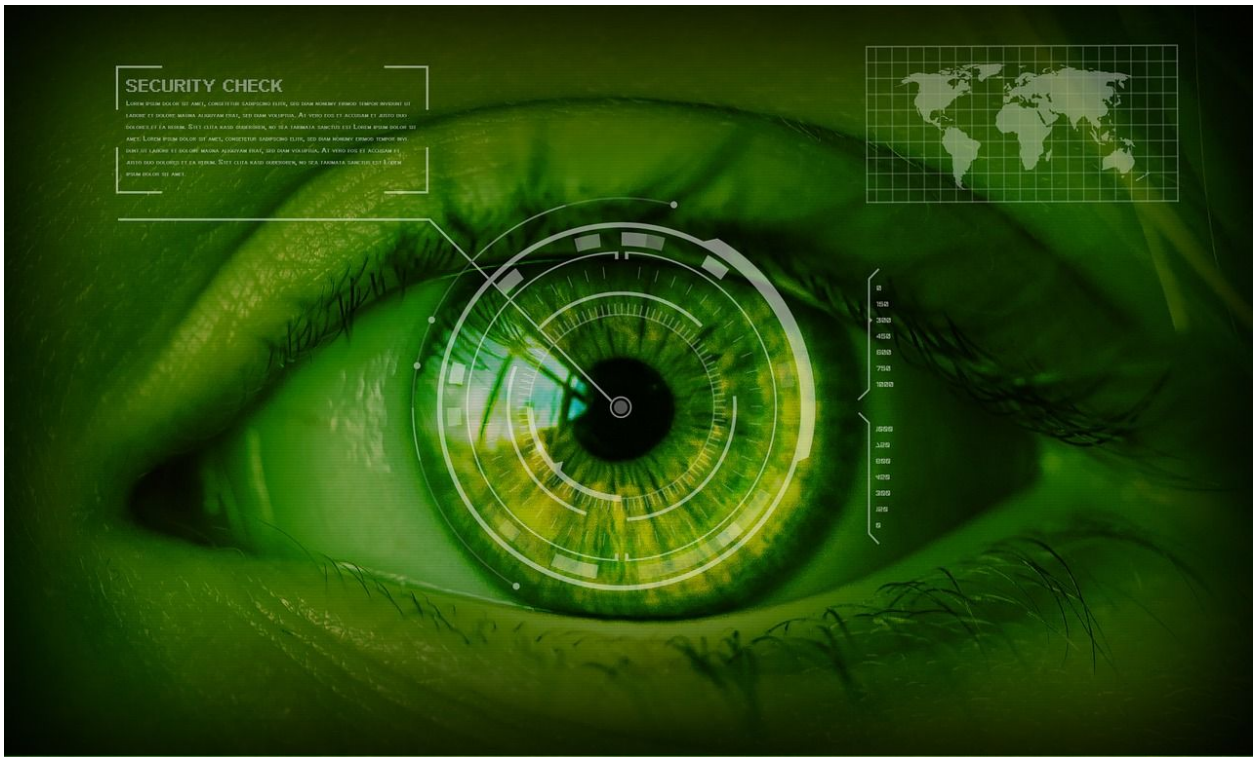
Submission to the departmental Inquiry into the use of retained metadata in civil proceedings.



Introduction

This submission is written by Rosie Williams BA (Sociology). Rosie is an open data, privacy and data ethics advocate. Rosie authored the 'CensusFail Submission' which was referenced in the Inquiry report and included a survey with input from over 400 people.

Rosie Williams organised a public information session on the topic of the use of metadata in civil proceedings hosted by Open Knowledge Australia on January 11 which was attended by 50 people and a follow up event specifically for those writing submissions to the Inquiry on January 18 where people could ask further questions & discuss strategies.

Historical background to the Inquiry

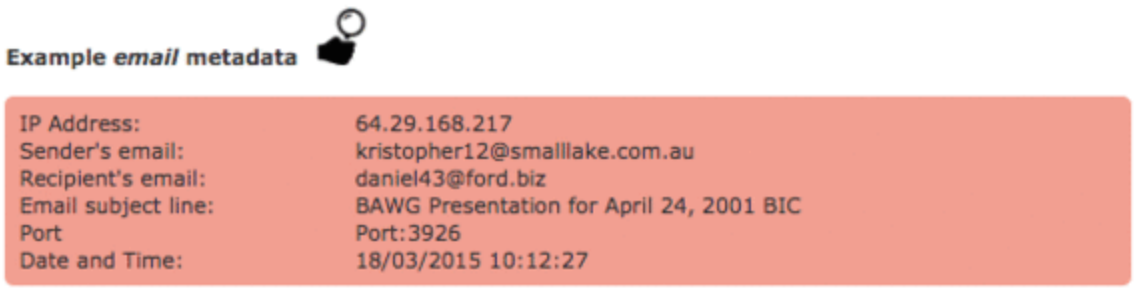
In March 2015, the Australian parliament passed legislation to introduce a data retention scheme into Part 5-1A of the Telecommunications Interception Act. The scheme standardises the data collected by Internet Service Providers and telecommunications organisations including a mandated storage period of retained metadata of two years.

The current consultation implies that data retained for the Data Retention Scheme is a subset of all data collected by ISP's and that access to data outside the Data Retention Scheme should be preserved for civil proceedings and data collected and stored solely as a requirement of the Data Retention Scheme should be kept available for law enforcement purposes under the criminal code and accessible without a warrant:

“Currently, civil courts can issue subpoenas for telecommunications data, but only if the data is being collected for operational reasons by the service provider, rather than under the national security-related mandatory data retention scheme.” (Hayden Cooper, 5 Jan 2017)

This distinction comes into play when for example, data concerning an individual from two years ago is sought but that data is not data the telco needs for its own purposes and is only retained due to the Data Retention Act. To further the example, if the ISP or telco has no reason to store the subject lines and contacts of the emails you send and receive through them, if they are only hanging onto those from two years ago due to the Data Retention Scheme then they will not be available for use in civil cases in the future *unless* this Inquiry decides on the basis of the submissions it receives that it should make that data available. I will argue that they should not.

To understand what kind of information is included as retained metadata you can visit the educational tool SnitchHunt (which shows how metadata can be used to identify and track down whistleblowers) or check out the examples below:



International context

Australia has no Bill of Rights that specifies a right to privacy so that when new regulation or legislation is considered there is an instrument which can provide protection of civil liberties including privacy.

A demonstration of why a Bill of Rights would be useful to Australians is the reversal of the Data Retention Directive:
"Under the directive the police and security agencies will be able to request access to details such as IP address and time of use of every email, phone call and text message sent or received. A permission to access the information will be granted only by a court. On 8 April 2014, the Court of Justice of the European Union declared the Directive invalid in response to a case brought by Digital Rights Ireland against the Irish authorities and others." (source)

"In 1995, conscious both of the shortcomings of law, and the many differences in the level of protection in each of its States, the European Union passed a Europe-wide directive which will provide citizens with a wider range of protections over abuses of their data.[fn 1] The directive on the "Protection of Individuals with regard to the processing of personal data and on the free movement of such data" sets a benchmark for national law. Each EU State must pass complementary legislation by October 1998." (source)

An Australian Bill of Rights would help mitigate the tendency for scope creep which is where legislation is passed for one purpose (eg terrorism) but then extended or re-purposed for ends that were never intended and have not been subjected to proper democratic consultation or inquiry (eg copyright infringement). Allowing data retained for the purposes of investigating terrorism or paedophile cases to be available for family law disputes or debt collection is an example of the kind of issue that a Bill of Rights could assist in protecting Australians from.

Problems with existing legislation relating to data & privacy

Definition of Personally Identifying Information
The recent decision in the Grubb/Privacy Commissioner v Telstra case has implications for this Inquiry. The decision handed down by the Federal Court on Jan 19, 2017 has left open the question of whether phone metadata stored by Telstra falls under the Privacy Act.

Ben Grubb, (a technology journalist) sought to access his own telephone metadata held by Telstra under the Privacy Act, and was refused. The case came out of a desire by Grubb to see if he could access the same information that the government is able to access without a warrant including cell phone tower locations that his phone communicated with. As Salinger reports: "Ben also worked on a seemingly simple premise: "the government can access my Telstra metadata, so why can't I?""

Telstra refused to provide access to this information claiming that location information generated when Grubb's phone pinged cell towers was not 'personal information' under the definition in the Privacy Act and so they didn't have to supply this data. Grubb appealed this decision through the Office of the Information Commissioner and Administrative Appeals Tribunal found that: "That data is no longer about Mr Grubb or the fact that he made a call or sent a message or about the number or address to which he sent it. It is not about the content of the call or the message" (AAT in Salinger 19 January, 2017).

The Privacy Commissioner disagreed with this explanation, finding that cell tower locations recorded from an individual's device could be linked with other data to identify an individual and so qualified as falling under the definition of 'Personally Identifying Information'. Telstra appealed this ruling in the Federal Court and the decision was handed down on January 19th in favour of Telstra on the basis that it is not yet been decided whether the type of information used by the government to identify, track and prosecute people is actually about those people.

To be fair to the Administrative Appeals Tribunal, they did not put it quite like that. The AAT provided extensive explanation as to how it might be possible for information not to be considered to be personally identifying if it had originally been collected for purposes other than identifying an individual.

I am not a lawyer but I question the failure of logic that follows from a set of data being retained for the specific purpose of identifying, tracking or prosecuting an individual and the decision of the AAT to claim it may not fall under the definition of PII covered by the Privacy Act.

How can criminal or civil litigants proceed with cases using metadata if that metadata is not considered to be 'about' that individual? How can the government force organisations to collect and maintain data of such an intimate personal nature as the location, subject, contact and

other personal information and not consider that information to be covered by the Privacy Act and also available to the people without whom, the data would not exist?

The definition of what is or is not metadata for the purpose of Data Retention Scheme
The existing legislation has not defined metadata. Metadata required for retention under the data retention scheme needs to be defined explicitly so that it can not be expanded down the line. Australians would hate to see a situation where data that is now considered content - for example our browsing histories ends up being included under a future demand for metadata because the definition of metadata has not been made clear.

Lack of instruction on destruction of data
There needs to be a directive to destroy metadata that has been retained under the data retention scheme. There is no current requirement as to what telcos and ISP's need to do with the data they retain under the Data Retention Act. This data should be destroyed once there is no longer a requirement for the organisation to retain it. This data should also be stored in Australia and be subject to Australian laws.

Lack of protection for individuals on breach of privacy
Currently Australians do not enjoy a right to sue for breach of privacy. There is also no sufficient requirement for Australian organisations to notify affected individuals or the Privacy Commissioner when a data breach has occurred. Legislation was brought in late in 2015 but has been delayed to the new parliamentary year.

As things stand, Australians have no right to be informed when a data breach involving our personal information has occurred and can seek no remedy for the harm any such a data breach has caused.

Groups affected and scope of the request for submissions

The Attorney-General's information on the Data Retention Scheme lists terrorism and pedophilia as case studies that demonstrate the usefulness of the scheme. The Attorney-General had previously stated that metadata retained under the Data Retention Scheme would not be used in copyright infringement cases but has recently removed this advice. It is widely believed among privacy advocates in Australia that it is the intent of the Inquiry to extend the data retained for the investigation of serious crimes to copyright infringement cases.

What the Attorney-General's information fails to mention are the special interest groups that are impacted by the retention and warrantless access to retained metadata and the significance of these groups.

The Whistleblower Handbook (2011) revealed that according to extensive research carried out by PriceWaterhouseCoopers that "whistleblowers detected and exposed more wrongdoing in the corporate world than every investigator and auditor working for every law enforcement regulator agency combined."

It is widely understood that whistleblowers, particularly in Australia, face enormous challenges in bringing to light corruption and misbehaviour that affects Australians. Whistleblower groups need to be specifically consulted with regard to how retaining metadata for a number of years and providing warrantless access to that data for either criminal or civil proceedings may affect them. Journalists and media organisations who deal with whistleblowers also need to be consulted to understand how the retention of metadata under the Data Retention Scheme affects their work and interests.

Likewise, advocates for victims of domestic violence also should be consulted to see what concerns they may have about how the storage and use of people's personal communications for warrantless access by the government may potentially impact them.

It is concerning that in requesting public input to evaluate exclusions on the use of retained metadata in civil proceedings the Attorney-General has sought only for advice on how parties might be affected by not having access to metadata rather than requesting feedback on how providing access may negatively affect different interest groups. This bias in the consultation toward parties wishing to use metadata for civil proceedings is evidence that no proper social licence has been attempted by the government.

Conclusion/Recommendations

In consideration of the aforementioned points, it is recommended that data retained by telcos and ISP's under the Data Retention Scheme not be made available for use in civil proceedings, and specifically not be used in copyright infringement cases which is a direct contradiction of the original publicly stated intention of the Scheme.

It is recommended that input from whistleblower and domestic violence advocates be specifically sought in order to understand how the use of data may impact upon them.

It is recommended that the Australian government introduce legislation for mandatory data breach notification.

It is recommended that the Australian government provide legislation under which Australians can seek legal remedy when our data is subject to breach.

It is recommended that the Australian government require telcos and ISP's to destroy data stored under the Data Retention Scheme after the expiry period.

It is recommended as has been proposed by Ben Minerd in his submission that the Attorney-General provide regular public reporting and transparency on how retained metadata is used.

It is recommended that data retained for use in criminal or civil proceedings fall within the definition of Personally Identifying Information or be excluded from the Data Retention Scheme.

It is recommended the Australian government create a Bill of Rights which includes privacy as a right.

References/Appendixes

SnitchHunt Rosie Williams & Gabor Szathmari

Mobiles, metadata and the meaning of personal information Anna Johnston, 2017

Ben Minerds Submission (to this Inquiry)

Telecommunications Interception Act 1979

Push for Australians' web browsing histories to be stored by David Wroe, Ben Grubb

FOI'd AFP presentation Josh Taylor

Australians phone & email records to be used in civil lawsuits by Bianca Hall

Fighting Terrorism or Piracy? Data Retention Floodgates Opened by Claire Reilly

Brandis Rushes to Release Telco Metadata for Civil Proceedings by Stilgherrian

Consultation Paper from the Attorney General (pdf)

Privacy Showdown: Divorce lawyers could see your web history by Quentin Dempster

Data retention laws: Experts warn against opening up metadata to civil cases as telcos renew bid to change laws by Hayden Cooper

Concerns metadata could be used in civil cases, including divorce by Hayden Cooper ABC 7:30 Report

Easier access to your data starts here from Paul Farrell The Guardian

Electronic Frontiers Australia info on use of metadata in civil proceedings

Data Retention information Attorney-General

Wrap up of Opening Pandora's Box Whistleblower.network

http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security

Privacy and Human Rights

https://en.wikipedia.org/wiki/Telecommunications_data_retention

https://en.wikipedia.org/wiki/Data_Retention_Directive