Unintended consequence of government "metadata" legislation that enables domestic and family violence[1]

By Kylie Hillard, 2 May 2016

Data retention legislation in Australia enables an account holder to access the data on their own phone or computer account for a two-year retrospective period, and, to access the data of other people connected to that account. When that account holder is also a perpetrator of domestic and family violence, they are able to track where a victim goes, who the victim contacts if the victim seeks help, where a victim may have sought refuge accommodation, when a victim is at home, the daily activities of victims, which route they take to work, and more. This unintended consequence of Australia's "metadata" retention legislation not only enables perpetrators to commit domestic and family violence, but endangers the safety (and lives) of their victims. Legislative amendment and possible procedural safeguards can minimise the risk of harm.

Why is "metadata" a problem?

1. With the introduction of the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* ("the Bill") there came significant outcry from the community about 'big brother' watching us amidst concerns about invasion of privacy. Among the issues raised was the right of individuals to access information on their own account, resulting in amendments to the Bill.
2. As part of my work as the Chair of National Advocacy for Soroptimist International Australia, we have considered this legislation and other matters, not only though a "gender" lens", but also a "domestic violence" lens.
3. Under the Act as passed coming into effect in October 2015, not only can an account holder access their own metadata information, but they will have the right to access information of anyone else who uses their account, as well as being able to access data for any other devices connected to that account.
4. Because many perpetrators of domestic and family violence hold computer, phone and other accounts, access to their victim's metadata information is an issue.

[1] This paper was presented at the Australian Women Lawyers Conference in Perth on 10 April 2016 and was presented in an adapted form at the Womens Legal Service Queensland Seminar in Brisbane on 9 September 2015, the National Indigenous Domestic Violence Conference at Carrara on 9 October 2015, the National and Domestic Violence Summit in Sydney on 27 February 2016 and a QAILS state-wide webinar on 15 February 2016. This paper was also adapted to a poster presentation that was provided at the STOP Domestic Violence Conference in Canberra between 7 to 9 December 2015.

5. For victims of domestic and family violence, this means perpetrators can track retrospectively over a two-year period who the victim sees, where they go, who they contact and which numbers they called most frequently, and more.
6. The access to this information could occur, even if the parties are no longer involved in a relationship due to the retrospective effect of the access to the data.
7. While the legislation provides for some limited protection of data, as the legislation currently stands, it creates a serious risk of harm to the safety of victims of domestic and family violence.

What exactly is "metadata" and how will it be accessed?

8. Under the *Telecommunications (Interception and Access) Act 1979 (Cth)* section 172 purports to define what metadata actually is and provides as follows:

> ***172 No disclosure of the contents or substance of a communication***
> *Divisions 3, 4 and 4A do not permit the disclosure of:*
> *(a)* ***information*** *that is the* ***contents or substance of a communication****; or*
> *(b) a* ***document*** *to the extent that the document contains the* ***contents or substance of a communication****.*

9. The Act as passed applies to the fact of the communication itself being made, but not the content, except to the extent it comes within the areas below. It is **not** your web browsing history and it is **not** the content or substance of a communication.
10. In relation to phone calls, it includes the phone numbers of the people talking to each other, how long talked, when, but not the content.
11. In relation to internet activity, the email address, when the communication was sent, but not the subject line of an email or its content.
12. And, the Act as passed provides for metadata covering six types of information that identifies:
    a. The subscriber to a communications service;
    b. Source of the communication;
    c. Destination of the communication;
    d. Date, time and duration of the communication;
    e. Type of the communication; and
    f. Location of the equipment used in the communication.
13. Once set up, it is contemplated that account holders will have a password that they can use to logon and access their metadata anywhere, any time, for a two year retrospective period.

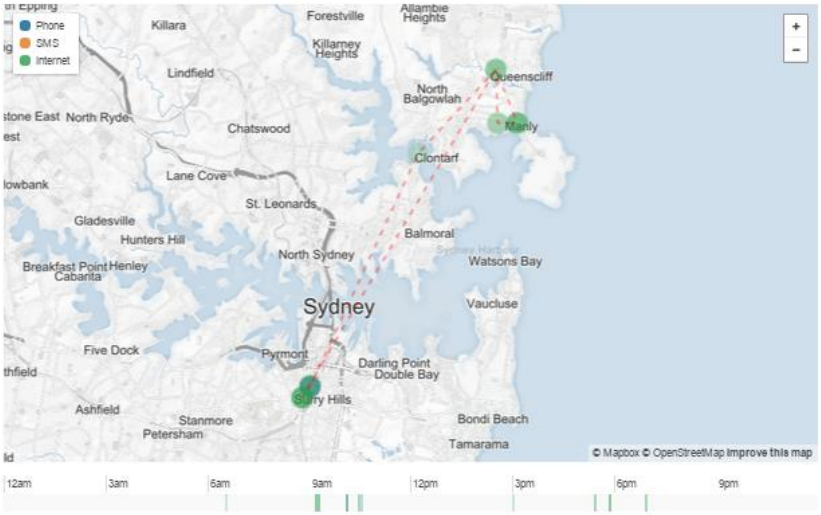
What's the big deal about people having your data?

14. Some have argued that metadata information was already being retained by service providers and relevant entities, that there was nothing new in what is being retained under the Act.

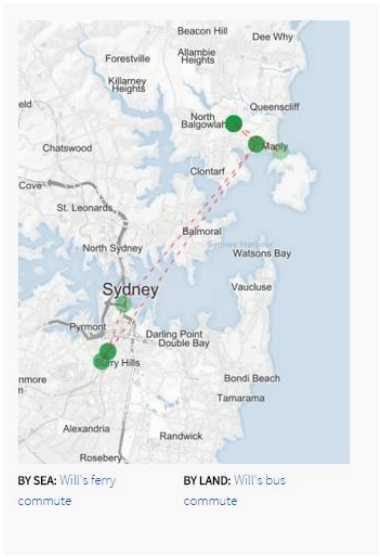
15. Some have argued that national security and policing benefits take precedence over personal privacy rights.
16. It has also been said that metadata provides merely an ‘envelope’ of the information, not the information itself.
17. But, what are the consequences of your data being released? If you have nothing to hide, what is there to worry about? What information can you obtain from an ‘envelope’ without the content of the communication?
18. Domestic and family violence is becoming more invasive through the use of technology enabling perpetrator to follow, stalk, harass and harm their victims in new and different ways via technology and mobile phones.
19. However, rather than advising clients not to use a phone, a phone is a necessary tool to empower and keep victims safe and connected to the outside world, however, domestic violone centres and support workers frequently advise victims about safe use of their phone.
20. And, now, with the access to metadata, the process to obtain information is made easier.

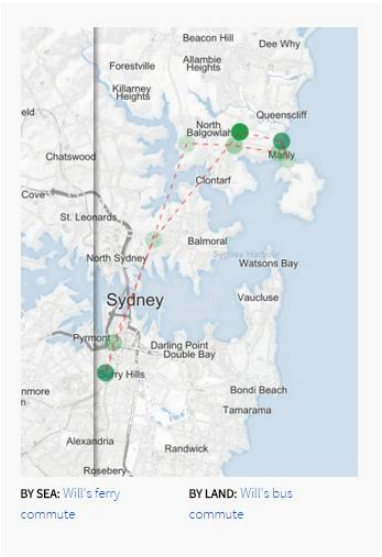
How a perpetrator of domestic and family violence can track victims using “metadata”

21. Your mobile phone “pings” telephone towers hundreds of times every day. That data was collected by Will Ockenden “How your phone tracks you everywhere” and “What you found” and he put it out to the public to work out what his activities were.
22. The outcome and conclusions people draw are truly disturbing in their overall accuracy, and when reduced to an image representation, it is concerning to see as you realise how much information about yourself is being kept.
23. From analysing the data, it is possible to work out which suburbs you travel to and areas that you frequently visit:



24. And by some simple investigation, it shows how you get to and from work, and which public transport route was used:

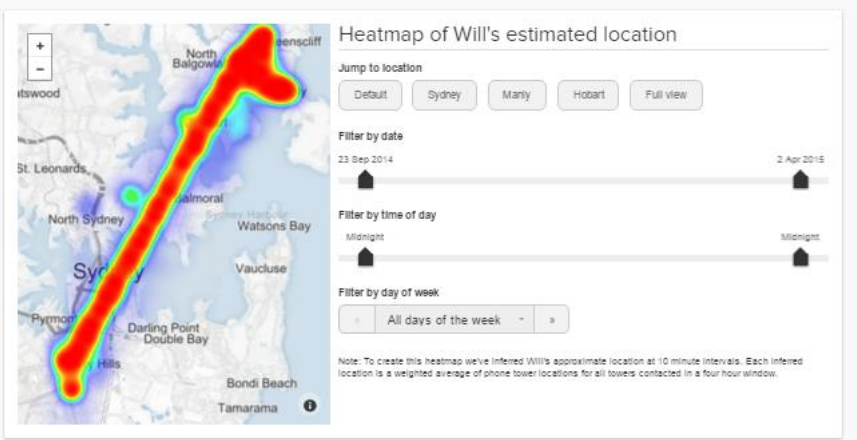




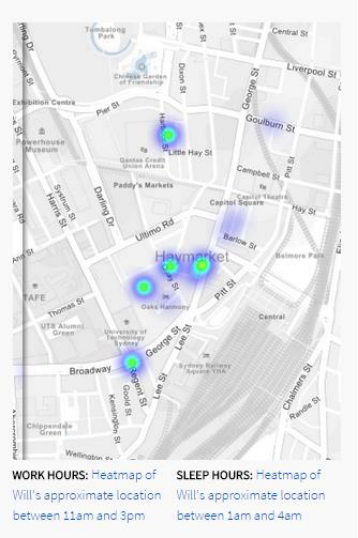
25. This is particularly concerning when considering that the perpetrator need only work out the public transport routes, and wait for their victim to come by and to then follow them.

26. And, because the legislation has a two year retrospective effect, a perpetrator can track down and work out where a victim went in that time - where they went to seek help, who they contacted, where they may have sought refuge.

27. The data also shows patterns of behaviours, how long you remain somewhere, and the frequency of trips. This image shows how long you stay at a particular place and the frequency with which a particular path is used. Again, it makes it easier to identify where a victim travels:



28. Disturbingly, the data enabled viewers to identify when Will was at home and likely to be asleep. This means that a perpetrator of domestic and family violence can work out the times of day when a victim is more likely to be home or not, and go to their home to either wreak havoc while they are out, or while they are home.



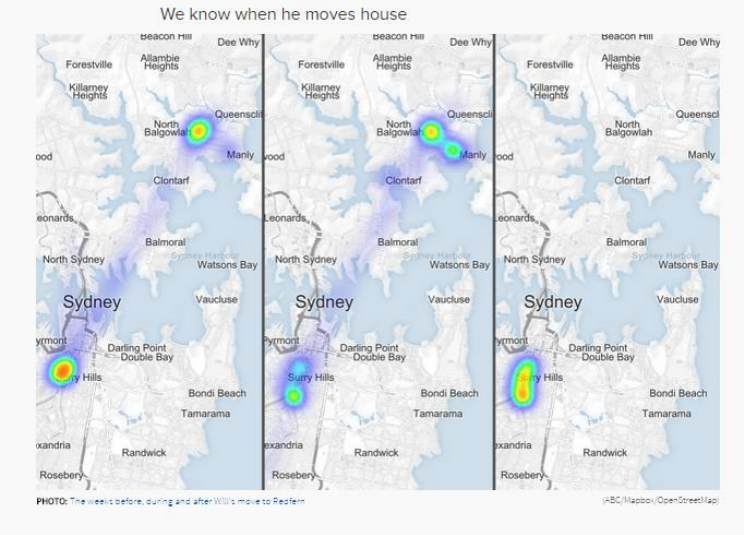
WORK HOURS: Heatmap of Will's approximate location between 11am and 3pm

SLEEP HOURS: Heatmap of Will's approximate location between 1am and 4am

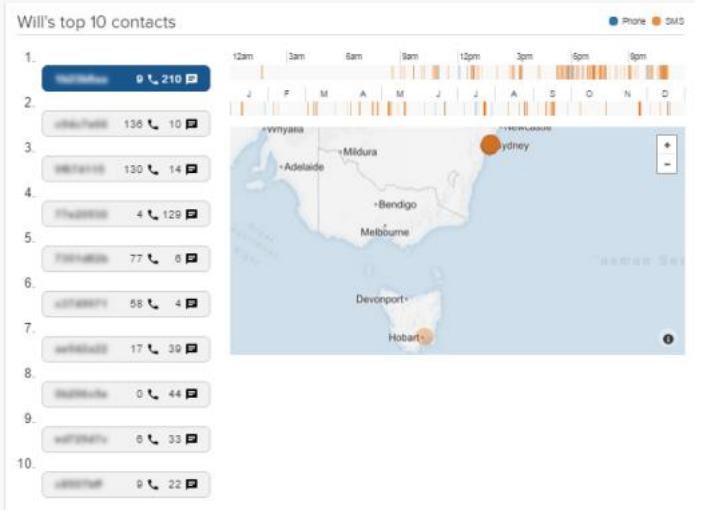
WORK HOURS: Heatmap of Will's approximate location between 11am and 3pm

SLEEP HOURS: Heatmap of Will's approximate location between 1am and 4am

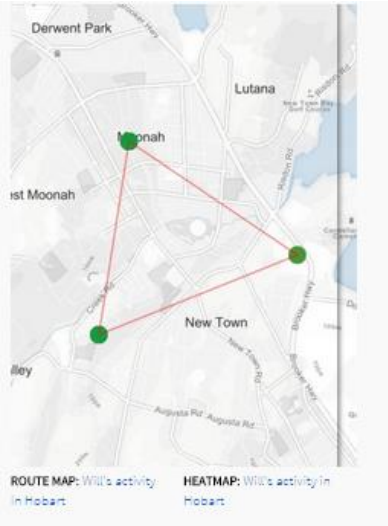
29. And, it shows when Will moved house, as can be seen in these images where the patches on the left show the previous house, the moving of the house in the middle, and the right showing the new house location:



30. It shows who Will connected to and the frequency of those connections (and who you a victim went to for help):



31. And it shows changes in behaviour, and in this case, viewers were able to ascertain where Will spent his holidays:

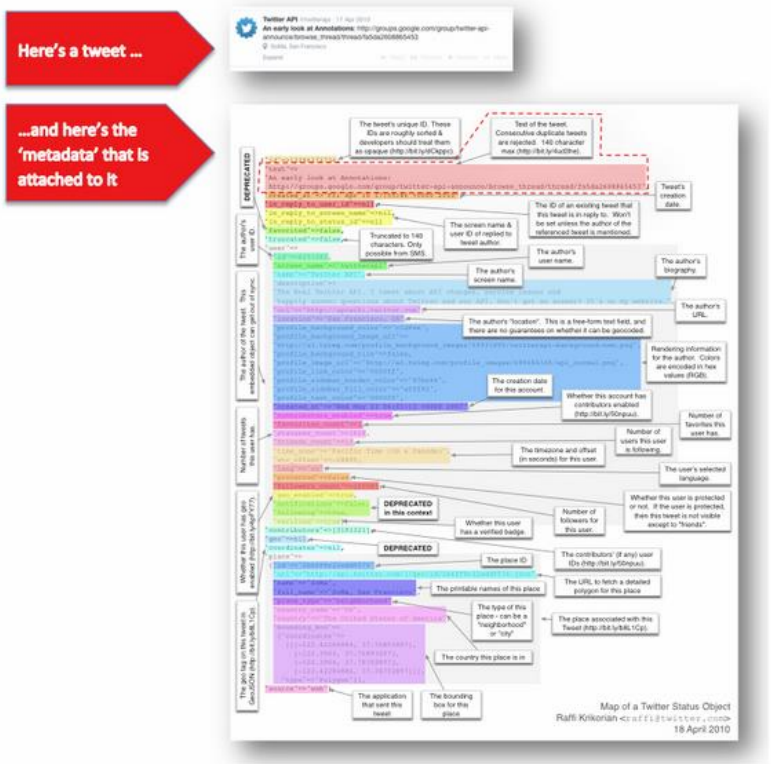


32. And this is just your phone metadata.

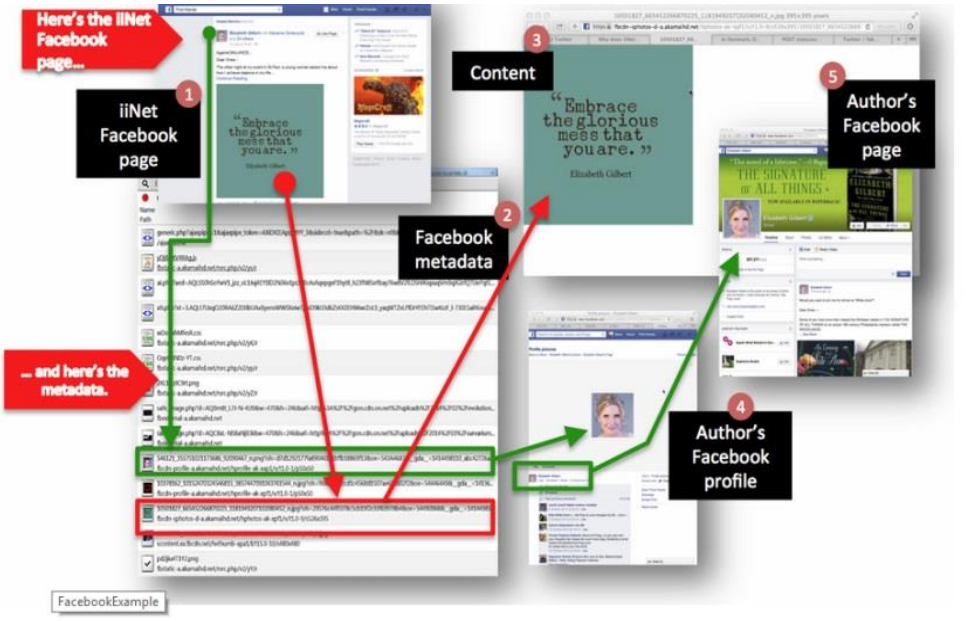
What about other mediums?

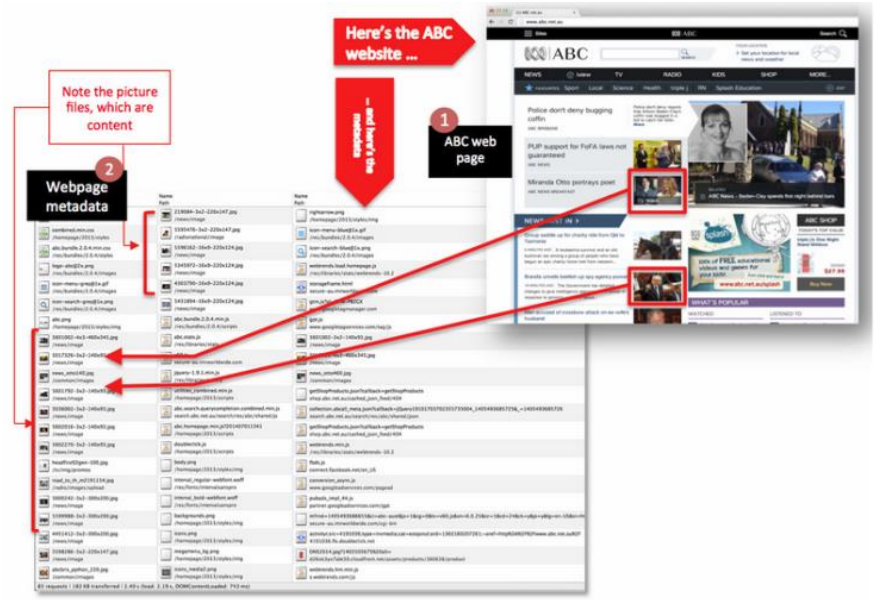
33. While not necessarily metadata required to be kept under the Act, other mediums and the coding reveals information about ourselves courtesy of “iinet” an article “Protecting your privacy: Our stand against mandatory data retention’”.

34. From a simple tweet you get a variety of information, including the geographical location, possible URL addresses, and much more:



35. And similarly, in facebook posts, which again may not necessarily be metadata required to be retained under Act, but it shows how information much can be obtained about you:





36. These examples demonstrate how much we share of ourselves on line and how we leave behind a digital footprint of ourselves, in addition to now, metadata information.

What does it mean for clients and victims of domestic and family violence?

37. From the perspective of domestic violence, we should be very concerned at the implications and consequences, and be alive on how to manage this risk.

38. Many of us know that technology, like the use of a mobile phone or smart phone, though a tool that can be used to enable and empower victims of domestic and family violence, it can also be used as a weapon or means by which domestic and family violence can occur.

39. It is widely accepted that technology and social media have become a larger forum by which perpetrators of domestic and family violence commit acts of domestic violence and essentially stalk victims.

40. Many of us may be aware of “Spyware” software – software that enables GPS tracking, recording of conversations remotely, copying of phone data, obtaining passwords to accounts, social media and more.
41. We may not be familiar with “MalWare” software – programs that ‘fake’ shutting down but which still monitor a person and record.
42. And, we may not be familiar with “spoofing” – posing or faking sending messages or emails by tricking or deceiving computer systems or other computer users, or by faking identify.
43. And, we may not appreciate that simply turning off the GPS locations and recently visited settings on your phone does not stop phone tracking.
44. But how does metadata change this?
45. It means that the changes to the metadata collection and the ability to access your own information for all account users, without the need at present for consent by other users, access for a retrospective period of 2 years will be a reality and it will likely be accessible by a password on your home computer at any time.
46. And by the time a victim of domestic and family violence seeks help, the damage is done, their digital footprint has already been created.
47. Survivors truly do “*map roads to new lives on the web by reaching out to Specialist Women’s Domestic Violence services and hotlines, researching intervention orders, and finding housing, employment opportunities, new schools and online support…*”: WesNET.
48. It is not such a sensational statement to say that government surveillance and “metadata” retention enables domestic and family violence.
49. It not only compromises the victims of domestic and family violence, but also those associated with them, those they contact, seek help from, and more

What can be done?

50. You can try:
    a. “VPN” device (Virtual Private Network) which limits the access to what you use (at least, unless government legislates against their use);
    b. Using encrypted messaging;
    c. “Tor”, a software program to help defend against surveillance;
    d. “Whatsapp”, a mobile messaging app that may or may not come under the Act; or
    e. Google’s web-based Gmail service said to excluded from data retention that may or may not come under the Act.
51. However, none of these are guaranteed to manage the risk of harm and you still need to advise clients on safe phone usage, and to obtain a separate phone account.

52. Given the massive cost of data retention (millions of dollars under), where the government will support the service providers to pay for the infrastructure to retain the necessary data, one wonders about the utility of the Act.
53. Surely organised criminal groups and those the Act is intended to target know of the these “work arounds”.

Where to from here – legislative or procedural changes?

54. A possibility is legislative reform prohibiting the respondent of a current domestic and family violence order from accessing information and / or criminalising efforts to access same, or, that they be required to show cause situation why they should not have access to the metadata.
55. A possibility is the introduction of a procedural requirement that an account holder to have the consent of other users to access information, however, one wonders whether a victim would have a free choice in signing consent in these cases, or whether reliance on a form being completed by a perpetrator is adequate.
56. Some may suggest that privacy laws and rights of individuals to access their data would be infringed – my response – we do that every day in legislating to protect the community, and infringe our rights to privacy by this Act in its present form in any event.
57. Some may suggest that national security that underpins the Act ought to be maintained – my response – national security remains important, but surely we should not have to wait for a victim to die at the hands of a perpetrator of domestic and family violence before we act.
58. Legislative change or procedural reform would not necessarily capture all perpetrators, but at least those who are subject to court order would be prevented from perpetrating the commission of domestic and family violence on their victims.

Post Script:

Scope creep

59. To date, over 60 organisations have applied for warrantless access to metadata which raises questions on exactly who’s data will be collected, who it will be available to and what it is going to be used for. Some of these organisations include racing industry bodies and transport organisations.
60. One wonders what level of security and control will be exercised over that access, and how much more scope creep will occur.
61. How much more data will be collected and by whom? Will the bounds of data collection be widened even more? Will it compromise the victims of domestic and family violence even further?

Links and Information Resources

http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5375

https://www.comlaw.gov.au/Details/C2015C00373/Download

http://www.ag.gov.au/dataretention

http://www.ag.gov.au/NationalSecurity/DataRetention/Documents/Dataset.pdf

http://www.ag.gov.au/NationalSecurity/DataRetention/Documents/KeepingourcommunitysafeFactsheet.pdf

http://www.ag.gov.au/NationalSecurity/DataRetention/Documents/DataRetentionGuidelinesForServiceProviders.pdf

http://www.abc.net.au/news/2015-08-16/metadata-retention-privacy-phone-will-ockenden/6694152?WT.mc_id=Innovation_News|HowYourPhoneTracksYourEveryMove_GPP|abc

http://www.abc.net.au/news/2015-08-24/metadata-what-you-found-will-ockenden/6703626

http://blog.iinet.net.au/protecting-your-privacy/#sthash.49Xrvz8n.dpuf

http://wesnet.org.au/

http://nnedv.org/

https://accan.org.au/news-items/hot-issues/1035-data-retention-facts

https://accan.org.au/files/News%20items/ACCAN%20Data%20retention%20factsheet%20FINAL.doc

http://www.businessspectator.com.au/article/2015/2/25/technology/its-not-what-who-you-connect-metadata-retention

http://www.attorneygeneral.gov.au/Mediareleases/Pages/2015/FirstQuarter/Government-Response-To-Committee-Report-On-The-Telecommunications-Interception-And-Access-Amendment-Data-Retention-Bill.aspx

http://exchange.telstra.com.au/2015/03/06/a-principle-of-privacy/

http://www.smh.com.au/federal-politics/political-news/telcos-confused-and-unprepared-for-new-data-retention-laws-20151012-gk6zq1.html

http://www.smh.com.au/technology/technology-news/metadata-retention-changes-explained-20151011-gk6m7p.html

http://www.sbs.com.au/news/explainer/what-metadata-and-how-do-you-maintain-your-privacy

http://www.itnews.com.au/news/australias-biggest-telcos-not-yet-collecting-all-user-metadata-410424

http://www.abc.net.au/news/2016-01-18/government-releases-list-of-agencies-applying-to-access-metadata/7095836

http://www.itnews.com.au/news/sixty-one-agencies-want-access-to-aussie-metadata-413770

http://mobile.pcauthority.com.au/News/413781,61-agencies-want-your-metadata--including-four-were-not-allowed-to-know-about.aspx