New South Wales
Council for Civil Liberties

Presentation for screening of CITIZENFOUR at Avoca Beach Picture Theatre

Pauline Wright, 24 March 2015

The NSW Council for Civil Liberties is delighted to have this opportunity to speak to you here tonight at the much-loved Avoca Beach Picture Theatre for this special screening of the powerful documentary **CITIZENFOUR** by award-winning director Laura Poitras. We thank Beth and Norman Hunter and their dedicated team at the Theatre for having us here to discuss **CITIZENFOUR**, in the context of the Federal Government's contentious data retention bill and in the spirit of enlivening an open public debate.

As you are all no doubt aware, **CITIZENFOUR** has just won the Oscar for Best Documentary and explores Edward Snowden's revelations about mass data collection and surveillance by the US intelligence agencies and their FiveEyes allies. It also explores Snowden's reasons for his actions – with full knowledge of the likely devastating personal implications. In doing so, it provides powerful insights into the astonishing dimensions and significance of metadata collection and analysis.

The NSW Council for Civil Liberties

The NSW Council for Civil Liberties is one of the oldest human rights organisations in Australia, having been formed in 1963 primarily to combat abuse of power by police. In recent times, it has been heavily involved with the issues arising from telecommunications surveillance, making submissions to the Parliamentary Joint Committee on Intelligence and Security, analysing bills produced by the Government, and hosting a viewing of this documentary in Parliament House for the benefit of our politicians in Canberra.

The current laws

I am assuming most of you know about the Federal Government's proposed Data Retention Bill[i] which is due to come before the Senate very shortly. The Government says that there is nothing significantly new about it. On one view, that is correct. The Government has for a considerable period now been able to access your metadata without a warrant. The importance of metadata is covered in the documentary and I won't go into it now. But this is an extraordinary circumstance.

The current regime distinguishes between: first, "live intercepts" of telecommunications data. Live intercepts are where a government functionary listens into your telephone call, for example. The Government needs to suspect you of a serious offence in order to make this serious incursion into your private sphere. The second category is stored communications such as emails and SMSs. Again, the Government needs to get a warrant, although here the bar is much lower. The Government only needs a real suspicion of an

indictable offence, some of which are quite trivial, such as larceny (ie stealing or common theft). The third category is metadata. For this information, no warrant is required. The agency can effectively self-authorise the incursion into your space.

There are real problems with the warrant regime. The NSW Crime Commissioner, Peter Singleton, recently gave evidence about the warrant system (in NSW) saying:

> *There are regular audits of the law enforcement agencies as to form—do we tick all the boxes? Are our applications in the correct format? Have we made the reports to the relevant authorities on time? There are no proper checks as to the truthfulness of affidavits that are put forward to get warrants, and no auditing of the substance of that kind of matter, and I draw that to your attention in case you wish to explore it*[1]

Further to that, the data being collected, in other words the boxes that are being ticked, are grossly inadequate for the community to form a proper opinion about the effectiveness of the warrants that are being issued. The NSW Council for Civil Liberties has repeatedly requested that warrants and the collection of information about warrants be meaningfully amended so that citizens can properly appreciate their effectiveness. This can be done without taking more police time, or drowning officials in red tape. These are achievable changes.

But it is much more alarming where no warrants are required at all. In 2013, there were 319,874 self-authorisations for access to metadata in Australia. There is very little oversight of this regime. The scope for harassment by law enforcement or other agencies is of course very real here. The Commonwealth Parliament found cases of people having their metadata accessed by obsessed and infatuated officials with no connection to the investigation of any crime[2]and corporations have long accessed metadata to more efficiently market their products and services to particular demographic sectors.

The Data Retention Bill

The police and security services now say that the current regime is not enough. They want telecommunications companies to store the metadata of every individual so that it can be accessed at a later time.

CITIZENFOUR is a timely documentary that may help us, and hopefully members of the Senate, better understand what is at stake if the Government's current *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* is made law in Australia – whatever our personal views of Snowden and his actions. Notwithstanding NSWCCL having screened **CITIZENFOUR** in Canberra for a screening to better inform politicians of the ramifications of mass data collection and retention, the ALP unfortunately joined with the Government to vote in favour of the Bill in the House of Representatives last week and it

[1] Draft Hansard, PJCIS hearing, Wednesday September 26, 2012

[2] http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook44p/Surveillance

will be going to the Senate as soon as this week. It will have to be passed by the Senate if it is to become law.

The only dissenting voices in the House of Representatives were the three members not part of the ALP or Coalition – the Greens' Adam Bandt and independents Andrew Willkie and Cathy McGowan. The ALP agreed to vote in favour of the Bill after a deal was agreed between Prime Minister Tony Abbott and Opposition Leader Bill Shorten to amend it to better protect journalists' sources, including requiring a warrant issued by a judge and the creation of a 'Public Interest Advocate' who will be able to argue against police access to a journalist's metadata for the purpose of identifying their sources. One limitation is that because of secrecy provisions, the PIA won't be able to discuss the proposed police access with the journalist.

And while the amendments mean that in some cases a judge will have to determine whether the public interest is served in the disclosure of the journalist's source, such agencies such as ASIO and ASIS will not be subject to this constraint. Labor also insisted that the legislation include a "presumption against issuing the warrant," setting a higher bar for agencies seeking access.

The amendments were a step in the right direction, but they do not go far enough. This Bill should not become law.

NSWCCL and other civil liberties councils around Australia consider that the only kind of data retention regime that would be compatible with a robust democracy is one which targets suspects and not the whole community. We are dismayed by the failure of the Government to give any serious consideration to the far less intrusive and dangerous alternative of a targeted data and surveillance scheme. The available evidence suggests that a targeted scheme would be at least as effective as the proposed mass regime in terms of keeping the community safe from serious crime, and it would protect our privacy. We are citizens, not suspects, and should be treated accordingly.

The issues in the Bill are very complex – the implications hard to understand. The growth and transformation of telecommunications technology and personal 'metadata' is so fast that non-geeks must make a deliberate effort to get a meaningful understanding of what is being proposed and its implications.

CITIZENFOUR is centrally relevant to the core issue behind the proposed new law: should democracies collect and hold mass telecommunications data on everyone for subsequent access by government and its agencies? What is the cost to privacy and other freedoms? Will it make us safe from terrorism and major crime?

Understanding the nature of metadata

The Government, as I said, insists its plan to collect and retain telecommunications 'metadata' on most Australians is nothing new; does not involve sensitive 'content' and has no major threats for personal privacy, freedom of the press, free speech or the right to dissent. In short – it is of no great significance to the ordinary citizen.

None of these assurances is true. By its massive increase in scope, the metadata collection regime has enormous implications in terms of privacy and other core freedoms. Information technology experts say we should not be talking in terms of what is 'metadata' and what is ordinary data. They say it's all data and if it's data it can be retrieved, unlocked and understood.

This will be the first time Government determines exactly what telecommunications data must be collected and kept for all users of the net and mobile phones. Previously, data was collected by telecommunication providers for business purposes.

Many of the parliamentarians who will decide if mass data retention becomes the norm in Australia are not likely to fully understand the technology detail and therefore what is at stake. In fact, it is possible some members of the critical parliamentary committees reviewing this bill may not understand as much as they should. The Attorney General of Australia was unable to explain what was meant by 'metadata' when the Bill was first mooted[3] and only a few days ago the Prime Minister displayed his ignorance of what was involved when he spoke of his experience with metadata retention as a journalist in the 1980's, a time before mobile phones, the internet and emails![4]

The scope and informative value of 'metadata' is vastly greater than it was even a few years ago and certainly when the telecommunications legislation was originally passed in 1979, and it is constantly and rapidly expanding. Every aspect of a person's life can be deduced from 'metadata'.

Experts insist, as I said, that there is no longer any meaningful distinction between 'metadata' and 'content' data. The submission of internet service provider iiNet to the Senate Inquiry on the Comprehensive Revision of the *Telecommunications (Interception and Access) Act 1979* (Cth) stated that:

> *Contrary to the Attorney-General Department's submission to this Committee, access to telecommunications data is not necessarily less…intrusive than access to the content of a communication. We draw the Committee's attention to recent research from Stanford University which should put to put to bed the fallacy that the community should only be concerned about access to telecommunications content and not "metadata" or telecommunications data. Telecommunications data when accessed and analysed may create a profile of a person's life including medical conditions, political and religious views and associations:*

---

[3] On 6 August 2014 Attorney General George Brandis struggled to explain live on Sky News the details of his government's data retention policy. See article http://www.smh.com.au/digital-life/digital-life-news/george-brandis-in-car-crash-interview-over-controversial-data-retention-regime-20140806-101849.html

[4] "When I was a journalist there were no metadata protections for journalists and if any agency, including the RSPCA or the local council, had wanted my metadata they could've just gone and got it on authorisation," Prime Minister Abbott was reported as having said. In response, head of the Media Entertainment and Arts Alliance (MEAA) Paul Murphy said the Prime Minister's personal experience was not relevant. "For Tony Abbott to compare his time as a journalist to now is ludicrous," he is reported as having told the ABC. "Agencies are now given access to an unprecedented amount of data about our lives and work. The volume and type of data now available was beyond imagining in 1980." See http://www.abc.net.au/news/2015-03-18/metadata-laws-will-create-digital-fingerprints-ed-husic-says/6330012

> *The researchers initially shared the same hypothesis as their computer science colleagues, Mayer said. They did not anticipate finding much evidence one way or the other.*
>
> *"We were wrong. Phone metadata is unambiguously sensitive, even over a small sample and short time window. We were able to infer medical conditions, firearm ownership and more, using solely phone metadata," he said.'*

In its submission to the Leader of the House in the Senate dated 3 March 2015, the Law Society of NSW made the point that accessing an individual's metadata can be just as intrusive, if not more telling, as the content of the communications, because metadata can reveal that person's associations and movements, sensitive personal information, including health information and even a person's sexual orientation[5]. The Law Society cited mathematician and NSA whistle-blower William Binney, reputedly one of the best analysts in history, who left the agency in 2001 amid privacy concerns. Binney said:

> *When you take all those records of who's communicating with who, you can build social networks and communities for everyone in the world.*

It is a serious issue ordinary citizens should be concerned about, when Government treats all citizens as potential suspects and collects and holds their sensitive personal data for at least two years 'just in case'.

The right to privacy

Further, it's not at all clear that this very expensive increased surveillance which fundamentally undermines our privacy is either necessary or proportionate. No solid evidence has been produced that would justify the mass surveillance of minors and citizens on the chance that two years later some evidence might come up that could help an investigation.

Australia is a signatory to the International Covenant on Civil and Political Rights ("ICCPR"), which requires that state intrusions on the right to privacy must be necessary and proportionate. Article 17 of the ICCPR provides that:

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*

2. *Everyone has the right to the protection of the law against such interference or attacks.*

[5] See copy of the Law Society of NSW submission at http://www.lawsociety.com.au/cs/groups/public/documents/internetpolicysubmissions/942145.pdf

The right to privacy is not a trivial thing. It matters, and has significant implications for the nature and quality of personal life, family life and the wider society. Intrusions on it have effects. They harm the individuals whose privacy is invaded. But even more importantly, society suffers. If the confidentiality of communications cannot be assured, then the capacity for legitimate whistle-blowers to bring important information about official or corporate misbehaviour or corruption to public notice is severely compromised. This does not augur well for any democratic society.

Given the highly sensitive nature of metadata, the Government has failed to justify how its collection and retention in the way proposed by the Bill is necessary or proportionate. The experience of other countries has been that that data retention had no impact on either the effectiveness of criminal investigations or the crime rate. For example, in February 2011 the Legal Services of the German Parliament cited data suggesting only a very marginal increase in crime clearance rates from data retention, saying:

> *This marginal increase in the clearance rate by 0.006% could raise doubts about whether the provisions in their current form would stand their ground under a proportionality review. In any case, the relationship between ends and means is disproportionate.*

Implications for ordinary people

Journalists have argued that the proposed data retention regime will seriously constrain journalists and an effective free media and intimidate legitimate whistle-blowers. A State that spies on all its citizens, constrains its journalists and intimidates legitimate whistle-blowers will have trouble sustaining a robust democracy.

After fierce lobbying by journalists, the Bill has been amended to require a judicial warrant for a journalist's telecommunications data among other things. This is a welcome development, but what of other confidential relationships, such as between a solicitor and their client? The Bill does not stop data about people's communications with their lawyers being collected, retained and accessed. And similar privacy concerns might also arise for Catholics having contact with their priests, which is something which has traditionally been protected at common law.

The President of the Law Institute of Victoria, Katie Miller, said last week[6]: "In many cases it is very important to keep confidential and protect even the fact that a lawyer is in contact with particular people" and that the mass retention of communications data between lawyers and their clients could "threaten the necessary trust between lawyers and their clients, allow an issue of sensitivity to be inferred or revealed, and undermine the ability of lawyers to advocate on behalf of their clients".

For example, the fact that information has exchanged (whether by email, text or telephone) between the client and the lawyer or the lawyer and associates of the client, experts or

[6] See article by Katie Miller http://www.afr.com/technology/data-retention-bill-changes-fall-short-law-institute-of-victoria-20150322-1m3w12

potential witnesses, could disclose a defence case, a litigation strategy or case theory. All of this could be identified based on witnesses or experts contacted by the lawyer.

It is a fundamentally important principle, long recognised under common law, that clients should be confident that their communications with lawyers are private and will not be disclosed to any person. Without that confidence, people will be afraid to tell the whole story to their legal representatives for fear of the opposing side finding out details that might be used against them. If lawyers don't know their client's whole story, they won't be able to properly represent their interests and this would undermine the whole justice system.[7]

Lawyers' associations across the country are urging the Government that if the Bill is to become law, it must be amended so that a warrant is required to access lawyers' telecommunications data as well as those of journalists. They also argue that it should be amended to restrict access to metadata to criminal law enforcement agencies for preventing, detecting or prosecuting major crimes including terrorism.

But the view of the NSW Council for Civil Liberties is that amendment will not solve the fundamental problems posed by this Bill[8]. Because it is not targeted at people who are suspected of having committed a crime and applies to everyone everywhere no matter their age or background, it treats all of us as suspects, not citizens. It is a sow's ear and no amount of embroidery will transform it into a silk purse. There are some things that just cannot be polished!

CITIZENFOUR

CITIZENFOUR is an important film which will give audiences some powerful insights into the significance of mass collection of telecommunications metadata across the nation.

It is timely that you have the opportunity to watch this highly relevant documentary before our Senate decides on whether they should vote for a data retention regime to capture the communication metadata of Australians. After seeing this film, I urge you to talk to your local MP and contact Senators, make them aware of the issues and help them to influence the Senate vote.

Following the screening, you are welcome to stay for a short Q & A session. Joining me will be NSWCCL member, John Mifsud, a security technologist based on the Central Coast, who has designed data security systems for international corporations such as Citibank to ISO and Australian Standards.

I hope that you will enjoy **CITIZENFOUR**.

[FILM SCREENING]

---

[7] See the Law Institute of Victoria's supplementary submission on the Bill dated February 2015 at http://www.liv.asn.au/getattachment/de4c7bb2-0310-4f1b-a485-a3b78199d7ba/Supplementary-Submission-on-Data-Retention-Bill.aspx

[8] See link to NSWCCL's submission at http://www.nswccl.org.au/_mass_data_retention_bill

[Q & A SESSION]

What can you do?

Only with increasing community pressure on the Opposition and crossbenchers can we stop the passage of this bill. The Bill will be before the Senate this week – so you'll need to act quickly**.**

- Write to, email, and call Opposition and crossbench Senators
- Write to, email and call your local MP

We need to persuade Senators that:

- The only data retention regime that is compatible with a robust democracy is one which targets suspects.
- They must resist the rushed timetable of the bill.
- This bill should not proceed until the PJCIS inquiry into 'Access to the telecommunications data of journalists and their sources by law enforcement and security agencies' has reported and its recommendations considered by the community and the parliament.
- No agencies should have access to such extensive and revealing personal data of citizens without an independent warrant process.
- We want them to take a more principled stand on this issue and take seriously the chilling impact of mass surveillance.

If you are interested in finding out more or helping us in our work, you can join or make a donation to NSWCCL. Membership forms are available in the foyer afterwards or go online to join or make a donation: www.NSWCCL.org.au.

Thank you for coming along tonight and thank you once again to Beth and Norman Hunter for hosting this important screening.

---

[i] The *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 was i*ntroduced to Parliament on October 30 and redrafted on the advice of the Joint Committee on Intelligence and Security (which tabled its report on February 27). The proposed legislation would:

- Require telecommunications companies to retain customer's phone and computer metadata for 2 years
- Define which types of data must be retained, such as phone numbers, length of phone calls, email addresses and the time a message was sent, but not the content of phone calls or emails and explicitly exclude internet browsing
- Detail which agencies are able to access the data
- Give security agencies access to the data when they can make a case that it is "reasonably necessary" to an investigation
- Still require security agencies to obtain a warrant before accessing the actual content of messages or conversations
- Introduce an independent oversight mechanism, allowing the Commonwealth Ombudsman access to agency records, in a bid to boost privacy protections
- Give the Parliamentary Joint Committee on Intelligence and Security oversight of the use of metadata by the AFP and ASIO
- The Government is negotiating with telcos about who will pay for the new system