New South Wales
Council for Civil Liberties

NSWCCL SUBMISSION

Access to telecommunications data in civil proceedings

27 January 2017

Contact: Stephen Blanks

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Contact NSW Council for Civil Liberties

http://www.nswccl.org.au
office@nswccl.org.au
Street address: Suite 203, 105 Pitt St, Sydney, NSW 2000, Australia
Correspondence to: PO Box A1386, Sydney South, NSW 1235
Phone: 02 8090 2952
Fax: 02 8580 4633

The New South Wales Council for Civil Liberties (NSWCCL) thanks the Attorney General's Department and the Department of Communications and Arts for the invitation to make a submission concerning access to retained data in civil proceedings.

Since 2015, telecommunication carriers and internet service providers have been compelled to collect/retain mass telecommunication information (metadata) for two years. Following its *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014,*[1] the Parliamentary Joint Committee on Intelligence and Security (PJCIS) recommended that retained data stored solely to comply with the metadata scheme, should not be accessed by civil litigants (subject to future regulations). This prohibition is set to commence as of 13 April 2017. In a very limited page and a half consultation paper, the Department of Communications and the Arts and the Attorney-General's Department have asked key stakeholders whether there are areas of civil law that should be exempt. In this submission we are confining our comments to the third of the questions asked in the consultation paper, namely:

> Are there particular kinds of civil proceedings or circumstances in which the prohibition in section 280(1B) of the Telecommunications Act 1997 should not apply?

NSWCCL views the current metadata scheme as an affront to civil liberties and opposes its extension into civil proceedings.

1. Context

The implementation of the data-retention scheme has been controversial from its conception. It has been opposed by privacy experts and civil libertarians and divided the community. However a large part of the general public has been willing to forgo privacy rights to address the fear of serious crimes and terrorist attacks.[2] This cavalier approach to civil rights under the mantra, 'you only need to worry if you have something to hide', is an alarming example of government demagoguery exploiting Australia's poor civic education system. It encapsulates Williams' observation, that the very lack of protection in Australia has ironically lulled Australians into a sense of false-security that their rights are not being undermined.[3] Though the public generally accepted the 'hypothetical' risk of their privacy being breached, they will not tolerate when the risk materialises. Australia is not alone in implementing such a scheme, with many international counterparts already having implemented or planning to implement variants of this controversial metadata scheme.

The NSWCCL acknowledges the continual pressure on governments to ensure national security in the face of serious terrorism threats, however we continue to believe that these responses must be balanced against democratic values.[4] Storing the data of every individual is undoubtedly invasive. It

[1] Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015).
[2] See, eg, Australian National University, *Attitudes to national security* (10 October 2016) <http://politicsir.cass.anu.edu.au/research/projects/electoral-surveys/anupoll/national-security>.
[3] 'Legislating for a Bill of Rights Now' (2001) 36 *Papers on Parliament* 23-37.
[4] See, eg, Joint CCLS submission to PJCIS inquiry into Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 - October 2014; Joint CCLS submission to PJCIS inquiry into Counter-Terrorism Legislation Amendment Bill (No.1) 2014 - August 2014; Submission of the Civil Liberties Councils across Australia to the

poses an immediate threat to the right to privacy and freedom of association. This threat will escalate further as accessibility and reliance on the internet grows.

Commissioner Andrew Colvin has asserted that in 2014 telecommunication information was used "in 92 per cent of counterterrorism investigations, 100 per cent of cybercrime investigations, 87 per cent of child protection investigations and 79 per cent of serious organised crime investigations."[5] Though criminal law enforcement agencies may 'use' metadata in such high quantities, it remains highly contentious whether this information is actually valuable to investigations. Doubt about the pragmatism of metadata follows from the general international experience of similar schemes. Data from a German study, in conjunction with the European Digital Rights Organisation, asserts that metadata only made a difference in 0.002% of criminal investigations;[6] this mirrored other inadequate results in nations such as Denmark and the USA.[7]

Indiscriminate surveillance treats every Australian as a suspect, not knowing when their information is being accessed elicits, "The feeling that their private lives are the subject of constant surveillance."[8] A feeling of constant surveillance not only adversely impacts on human dignity but also overlooks that police are often aware of terrorists or terrorist sympathisers, as was the case in the Sydney siege. Consequently the storage of everyone's data is excessive and redundant. NSWCCL contends that such blanket encroachments on the right to privacy are disproportionate to the resultant reduction in serious crimes threatening national security.

2. Danger of including civil proceedings

Prior to the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 ('Amendment'),*[9] it was not an offence for communication service providers to release communication information if it was authorised under law or in connection to the operation of an enforcement agency (for example a warrant).[10] Since the *Amendment,*[11] s 280 has also been altered to no longer allow disclosures from subpoenas, notices of disclosure or court orders in civil proceedings if information is retained solely for the purposes of complying with Part 5-1A of the *Telecommunications (Interception and Access) Act* or not for the purposes of s 280(c).[12]

Parliamentary Joint Committee On Intelligence And Security inquiry into the National Security Legislation Amendment Bill (no 1) 2014; NSWCCL Submission: The Comprehensive Revision Of The Telecommunications (Interception And Access) Act 2014.

[5] Commissioner Andrew Colvin, AFP, Committee Hansard, Canberra, 17 December 2014, p. 3.

[6] European Digital Rights Shadow evaluation report on the Data Retention Directive (2006/24/EC) 17 April 2011 <https://edri.org/files/shadow_drd_report_110417.pdf> 14.

[7] Torben Olander, 'In Denmark, Online Tracking of Citizens is an Unwieldy Failure', *Tech President,* 22 May 2013. Available at: <http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy>; Privacy and Civil Liberties Oversight Board: Report on the Telephone Records Program January 23, 2014; Peter Bergen, David Sterman, Emily Schneider and Bailey Cahall, 'Do NSA's Bulk Surveillance Programs Stop Terrorists?' (2014) *New America Foundation.*

[8] *Digital Rights Ireland and Ors* (C-293/12) and *Kärntner Landesregierung and Ors* (C-594/12), 8 April 2014 [37].

[9] *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth).

[10] *Telecommunications Act 1997* (Cth) s 280(1).

[11] *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth).

[12] *Telecommunications Act 1997* (Cth) s 280; *Telecommunications (Interception and Access) Act 1979* (Cth) pt 5-1A; *Telecommunications Act 1997* (Cth) s 280(c).

Setting aside the contentious value of metadata in criminal cases, there has been some suggestion that civil proceedings, particularly concerning international child abductions and family violence, could benefit from the use of metadata. This is controversial not only because it directly violates the original purpose of the scheme, but also because it may produce disturbing repercussions if retained data was sought, for instance via subpoena. Implications include revealing journalists' sources, opening up the floodgates to an inundation of entities seeking access to data, in particular intellectual property owners seeking to enforce their rights. There is also the fear that over time the government will continue to expand the metadata scheme, like the frog in slowly boiling water. Expansion risks mission creep and infringement on civil liberties. Specific examples of this are discussed below:

2.1 Whistleblowers

Whistleblowers, are vital to hold authority accountable. This requires a safe outlet for the information or it may no longer become available. Under article 3 of the Media Entertainment and Arts Alliance code of ethics,[13] journalists must protect their anonymous sources by not revealing their identity. Through the use of journalists' metadata, the right to freedom of expression and right to a free press would be jeopardised by circumventing article 3 and exposing whistleblowers.[14] This potential fear has already been realised in a recent cyber 'snitch hunt' co-hosted by University of Melbourne.[15] Using only a 'leaked' document, pre-teens relied on metadata to track whistleblowers to their address. The winning team managed this feat in less than an hour. The scope of data collected is evidently so in-depth that this information must be limited as much as possible so as to not fall into the wrong hands. In early 2016, it was demonstrated that police may be tempted to exploit this information. The Australian Federal Police admitted to earlier warrantless email checks on Guardian Australia journalist Paul Farrell to find out who leaked information to him for his Australian asylum seeker policies article.[16] Despite leaking sensitive information being a potential crime,[17] The Age Company Limited and Liu debacle demonstrates how a civil defamation claim could be used to reveal sources.[18] In that case The Age would have been forced to reveal its sources for Ms Liu's defamation claim, if it had not agreed to forgo the qualified privilege defence. By including metadata in civil cases, the government further jeopardises the safety of whistleblowers. Noting with approval the implementation of public interest safeguards,[19] the NSWCCL still fears the potential risk of allowing further access to wide-scale surveillance in the civil jurisdiction. By

[13] Media Entertainment and Arts Alliance, '*MEAA Journalist Code of Ethics*' (February 1999), Media Entertainment and Arts Alliance <https://www.meaa.org/meaa-media/code-of-ethics/>.
[14] *Universal Declaration on Human Rights,* GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948) art 19; *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 19.
[15] James Purtill, 'How pre-teens using metadata found a whistleblower in two hours', *Australian Broadcasting Corporation; triple j hack* (online), 12 December 2016 <http://www.abc.net.au/triplej/programs/hack/how-team-of-pre-teens-found-whisteblower-using-metadata/8113668>.
[16] Amanda Meade, 'Federal police admit seeking access to reporter's metadata without warrant', *The Guardian* (online), 14 April 2016 <https://www.theguardian.com/world/2016/apr/14/federal-police-admit-seeking-access-to-reporters-metadata-without-warrant>.
[17] See, eg, *Public Interest Disclosure Act 2013* (Cth); *Australian Security Intelligence Organisation Act 1979* (Cth) s 35P.
[18] See, eg, *Liu v The Age Company Pty Limited (No 2) [2015]* NSWSC 276 (23 March 2015).
[19] *Telecommunications (Interception and Access) Amendment (Data Retention) Act (Cth)* 2015 div 4C.

endangering whistleblowers and by-proxy the media, mission creep threatens the backbone of every functioning democratic society, a free press.

2.2 Opening the floodgates

By allowing metadata access for civil cases, the Government gives scope to protect not just public interests but also private interests. The Polish experience of data retention demonstrates that retained data is inevitably exploited by parties who attempt to 'fish' for information, leading to an increase in overall litigation.[20] As information will be stored for two years, civil litigants could access unprecedented levels of information pertaining to contacts and locations, which in turn could encourage further civil action. The implementation costs of the metadata scheme are already expected to be as much as $319.1 million, based on Government estimates generated by PricewaterhouseCoopers; more litigation will only further increase this already exorbitant price.

Metadata information is so valuable due to the depth and breadth of the stored data. Journalists have some level of protection via safeguards, however they are not the only ones with access to sensitive information. Professionals in the legal and medical industry have access to highly confidential material. Much can be inferred from the fact of communications between them and clients/patients, yet access to their metadata is not protected. Former Law Council of Australia president, Stuart Clark AM, has likened this information to police recording 'who comes in and out of a psychiatrist's room.'[21]

2.3 Copyright enforcement

The current metadata scheme has been justified as a means of preventing terrorism and serious crimes threatening national security.[22] Without restrictions on the access to metadata in civil claims, there is potential for copyright holders to sue internet service providers for customer information. This in turn would allow the actions for copyright violations, in a similar fashion to the attempts by Dallas Buyers Club. Allowing metadata in civil cases involving copyright breach is contrary to the assurances provided by Attorney-General George Brandis and Prime Minister Malcolm Turnbull. George Brandis is quoted saying, "Breach of copyright is a civil wrong. Civil wrongs have got nothing to do with this scheme."[23] Whilst acknowledging the devastating impact that piracy has on the likes of the film and music industry, the NSWCCL contends that many Australians would not support privacy rights violation for the purposes of enforcing copyright.

3. The purported benefits of allowing data to be used in civil proceedings.

3.1 The PJCIS argument

The PJCIS proposes that metadata be able to be used in certain cases to facilitate the provision of justice. The PJCIS instances cases involving family violence or international child abduction,

[20] Katarzyna Szymielewicz, Data Retention in Poland: The issue and the Fight, *Panoptykon Foundation*, 2012.
[21] Will Ockenden, Interview with Stuart Clark AM (Radio Interview, 24 March 2015).
[22] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.
[23] Australian Broadcasting Corporation, 'Metadata', *Q & A,* 3 November 2014 (George Brandis QC) <http://www.abc.net.au/tv/qanda/txt/s4096883.htm>.

suggesting that in such cases the ban on the use of metadata in civil proceedings ought to be relaxed.

It is notable that that the Family Law Council argues that in order to protect vulnerable children, international child abduction should not be criminalised.[24] They argue that doing so would encourage people to 'go underground'. Allowing the use of metadata in such cases would have a similar effect. Metadata also offers limited benefit when abductors switch to foreign carriers not obliged to collect/retain telecommunication information.

As Kylie Hillard has pointed out, perpetrators of domestic violence can use the retained metadata to track their victims, determine from whom they have sought help, where they have taken refuge, when they are at home, their daily activities, their routes to work. Allowing a party to the proceedings to access this information creates an unacceptable risk. '[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.'[25]

A concern to reduce such violence should lead to a reduction in the retention of metadata, not making it more freely available.

3.2 Verifying evidence

Just as in a trial metadata can be used to verify or discount evidence concerning an accused's location at a given time, so it could sometimes be significant in a civil case, perhaps to confirm that a litigant was in contact with another party. Here, though, the benefit is slight, civil litigants are seeking to gain access to new information, not to protect existing access. Allowing civil litigants to access metadata also has major ramifications for privacy rights. NSWCCL submits that the public interest in privacy and the benefits of privacy for the individuals involved far outweigh any benefits of indiscriminate access to metadata.

4. Recommendations

For the retention and use of metadata to be justified, it must not only be beneficial, but both proportionate to and necessary for that benefit. It is not clear that metadata retention is necessary even for the reduction of terrorism and other serious crimes. At least here a legitimate purpose is being explored. But the requirements of proportionality include that the least invasive means must be used for the end to be achieved.[26] There are far less intrusive options available than monitoring everyone.

---

[24] See, e.g., Family Law Council, *Parental child abduction a report to the Attorney-General prepared by the Family Law Council* (1998) 37-38.

[25] Kylie Hillard, 'Unintended consequence of government "metadata" legislation that enables domestic and family violence' (Paper presented at the Australian Women Lawyers Conference, Perth, 10 April 2016).

[26] Human Rights Committee, *General Comment No. 27: Article 12 (Freedom of Movement),* CCPR/C/21/Rev.1/Add.9 (2 November 1999).

Recommendation 1. The existing legislation should be repealed, and a targeted data surveillance scheme instituted instead.

A less invasive and more acceptable approach to metadata surveillance is to use a targeted scheme, as the NSWCCL has previously advocated.[27] By targeting only those reasonably suspected of being involved in serious wrongdoing, a targeted data surveillance scheme balances liberal democratic values and the prevention of illicit behaviour. Though targeting individuals poses its own risks, such as discrimination, we believe that an ad-hoc approach would succeed if it relied on judicial authorisation with a Public Interest Monitor involved with each hearing. Limited surveillance would not only reduce costs but would also lower the temptation for hackers to try and access stored metadata about every Australian.

The use of the judiciary is important for the separation of powers, but, importantly, allows for controls on the extent and duration of surveillance. A Public Interest Monitor, such as those required in Queensland and Victoria, would provide a guarantee that decisions do not become perfunctory, and that access to metadata was only obtained in cases where it was indispensable.

Along with a warrant requirement, the NSWCCL believes there is a strong need to be transparent in the surveillance process, ensuring that those who had been monitored on unfounded suspicions would be notified (in the absence of strong justifications otherwise).

Recommendation 2. The period for which information is stored should be reduced from two years to six months.

The Explanatory Memorandum to the Data Retention Bill 2014 asserts that in the majority of cases data is accessed within six months of its collection. This would reduce the privacy invasion, and also lighten the burden on providers, who must separate information that is stored for operations and what is stored solely for the metadata retention scheme.

Recommendation 3. Civil proceedings should continue to be excluded.

As argued above, permitting the use of stored metadata in civil cases would threaten freedom of the press. It would greatly increase the risk to whistleblowers, making it less likely that wrongdoing and dangerous activities will be exposed. It would clog up the courts. It would pose a serious risk of misuse of the information. It would be contrary to solemn assurances given by the Attorney-General and the current Prime Minister, in 2014.

Conclusion

The NSWCCL maintains that the current scheme to collect and retain metadata is disproportionate to the threat of serious crime. It should not be made worse by permitting litigants in civil cases access to metadata.

[27] Joint CCLS submission to PJCIS inquiry into Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 – 20 January 2015.

This submission was prepared by Caleb O'Brien and Dr. Martin Bibby on behalf of the New South Wales Council for Civil Liberties.

Yours sincerely,

Therese Cochrane
Secretary
NSW Council for Civil Liberties
Mob 0402 013 303

Contact in relation to this submission Stephen Blanks: email Stephen.blanks@nswccl.org.au; tel. 0414 448 654