



## NSWCCL SUBMISSION COMPREHENSIVE REVISION OF THE TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 2014

The New South Wales Council for Civil Liberties (CCL) welcomes the opportunity to make a submission to the Senate Legal and Constitutional References Committee (the committee) on the comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (the Act). We share the widespread view that such a comprehensive and integrated review is very overdue and urgently needed.

*Given the unique power of the state, it is not enough for leaders to say: Trust us, we won't abuse the data we collect. For history has too many examples when that trust has been breached. Our system of government is built on the premise that our liberty cannot depend on the good intentions of those in power; it depends on the law to constrain those in power.*

Barak Obama, January 17, 2014 Speech on NSA phone surveillance

NSWCCL is one of Australia's leading human rights and civil liberties organisations. Founded in 1963, NSWCCL is a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. To this end the NSWCCL attempts to influence public debate and government policy on a range of human rights issues by preparing submissions to parliament and other relevant bodies. 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).

### **1. Recommendations by the Parliamentary Joint Committee on Intelligence and Security (the PJCIS).**

1.1 CCL made two submissions to the PJCIS inquiry. Sections 6-9 (pp. 6-10) and 14-16 (pp14-18) of the principal submission and sections A and B (pp. 1-4) of the subsidiary submission bear on the current inquiry, the latter particularly if data retention is included in the scope of the inquiry. We refer the Committee to those two submissions, which remain relevant to the current inquiry.

1.2 CCL also made a brief submission to the Committee concerning the review of the Telecommunications (Get a Warrant) Bill, 2013. That submission is also relevant.

## **2. The importance of privacy.**

2.1 Privacy is no trivial matter. Intrusions on it have effects. They harm the individuals whose privacy is invaded. But even more importantly, society suffers. Privacy is a fundamental human right, in that it is central to the maintenance of democratic societies and is essential to human dignity. In its absence, there is no freedom of expression and information, and no freedom of association.

2.2 It is essential for each person to have a realm where they are free from other human eyes watching them; where they are free from others forming judgements about what they can and cannot do. Privacy gives us the freedom to define ourselves and our relations with others. It is essential for human development.

2.3 But this is not only a psychological necessity. Privacy is necessary for the development of dissent, for the formation of challenges to orthodoxy. A human being who lives in a world where he thinks he is always being watched is a human being who makes choices, not as a free individual, but as someone who is trying to conform to what is expected and demanded of him or her. Politically, that is why tyranny loves surveillance—because it encourages conformity. It means people will only do that which they want other people to know they are doing—in other words, nothing that is deviant or dissenting or disruptive. It breeds orthodoxy.

2.4 Intrusion upon privacy lays the victim open to victimisation and discrimination. Covert intrusions leave a person vulnerable to misinterpretation and mistaken data-matching. The knowledge that words and actions may be being monitored restricts autonomy and hampers personal growth and the development and enjoyment of relationships. In the hands of the unscrupulous, covert surveillance leaves victims open to blackmail.

2.5 Accordingly, privacy is recognised under international human rights law.<sup>1</sup>

## **3. Attacks upon privacy.**

3.1 The revelations by Edward Snowden as to the scope, volume, analytic capacity and international sharing of systemic internet/telecommunications surveillance by NSA and other intelligence agencies are astonishing. The massively increased willingness of Australian agencies to monitor, collect, store and analyse and share unprecedented volumes of data requires exposure and debate.

---

<sup>1</sup> Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights Article 17.

- 3.2 Reported Australian interceptions have been steadily rising. The large number of warrants issued for interceptions and access to stored communications and the huge numbers of authorisations for access to communications data require addressing.
- 3.3 This increase gives the impression that those involved suppose that it does not really matter if privacy is invaded, provided it is the police, ASIO or other enforcement agencies that are doing the snooping. It cannot be emphasized enough that eavesdropping, interception, or accessing private communications are, in themselves, wrongs. They are wrong whether they are done by private individuals, by anti-corruption bodies, by police or by ASIO. They cannot be justified merely because they are useful.
- 3.4 Because they are wrong in themselves, their use should be limited. They must never be a substitute for ordinary policing. It is not proper that agencies only have to demonstrate that an interception ‘would be likely to assist in connection with the investigation by the agency of a serious contravention in which the person is involved.’ The circumstances must be that the applicant agency *cannot reasonably use* other methods to obtain the information it needs. And then they can only be justified where the most serious of offences or security threats are involved--where there is a risk to life.

**Recommendation 1: That the Committee recommend that warrants under the TIA Act should only be issued where they are likely to assist in an investigation of an offence involving a risk to life and where there are no other reasonable methods available to the agency to obtain the information it needs.**

#### **4. B-Party warrants.**

- 4.1 A B-party warrant enables an officer to intercept the telephone calls and other communications of innocent persons, about whom there is not a shred of suspicion, in the hope of obtaining information about another person. There is no restriction on who the B-party will be. It could be spouse, child, lawyer or clergyman. All the conversations of the B-party may be monitored, not just those with the suspected transgressor.
- 4.2 B-party interception can easily be misused, for example, to catch whistle-blowers by targeting journalists. They could be used to eavesdrop on discussions between lawyers and their clients.
- 4.3 CCL opposed the introduction of B-party warrants in 2006. We strongly recommend that they be abolished.
- 4.4 B-Party warrants were introduced on the ground that they were needed to deal with the threat of terrorism. But it was not long before function creep took over, with an explicit and open recommendation (in an annual telecommunications report) that they be used more widely. After a certain amount of outrage about this, the recommendation was dropped, and this year, for the first time, the number of these warrants that were issued decreased.

#### **Recommendation 2: That the Committee propose that B-Party warrants sections of the TIA Act be repealed.**

- 4.5 The use of B-party warrants inevitably produces a great deal of information which is unrelated to the commission of any offence. There are penalties for the release of such material. But if B-party warrants are to continue, there should be a requirement that such materials are destroyed within a short time of their collection. The ombudsmen and the Inspector General of Intelligence Services (IGIS) should be required to certify the processes by which the destruction is initiated.

#### **Recommendation 3: That if B-Party warrants are to continue, the ombudsmen and the IGIS investigate and report periodically on the progress of the destruction of material relating to non-targeted persons collected under them.**

## 5. Stored communications.

5.1 Stored communications are transmissions between persons such as emails, SMS and voicemail messages, which, at least in the past, did not involve live interaction between communicators.

5.2 The TIA Act distinguishes between ‘live’ interception warrants and stored communications warrants. In respect of interception warrants, law enforcement agencies must be investigating serious *offences*, being offences carrying a sentence of seven years or more. There are further criteria, excluding a number of offences. These restrictions are important protections of privacy. There is also a long list of other offences included by stipulation.

5.3 For stored communications warrants, however, the threshold is a serious *contravention*—an offence for which the penalty is three years’ detention or a fine of 180 penalty units. There are no further restrictions to the kind of offence included. The range of offences which carry three years’ penalty is immense and the number of persons convicted of such crimes is large. For example, under the Federal Criminal Code, ‘causing a loss’ carries a sentence of five years.

5.4 The threshold for a serious contravention also includes offences under state laws. Here are some offences in NSW which meet the requisite threshold to justify a stored communications warrant:

*Malicious damage to property*, which includes graffiti, carries a five years penalty. There were just under 10,000 charges for this kind of offence in one year in the Local Court of NSW alone. (That excludes the Children’s Court).

*Larceny*, which includes shoplifting. The maximum penalty is five years’ imprisonment. There were 6,000 charges in 2011 in the NSW Local Court for this offence (excluding motor vehicle offences and the Children’s Court cases.) Three thousand of these were from retail premises.

*Assault occasioning actual bodily harm*. The maximum penalty is five years’ imprisonment. The offence includes anything more than causing momentary discomfort. There were over 10,000 charges for this kind of offence in the NSW Local Court in 2011.

There are dozens of other examples. The list is likely to expand as the competition between political parties to appear tough on crime continues.

5.5 The Attorney General’s Department’s rationale for the lower threshold in respect of stored communications warrants is questionable. It successfully argued that covert access is less privacy intrusive than real-time listening, because communicators have the opportunity to review or to delete communications before sending them.

5.6 This reason does not seem compelling to CCL as a matter of logic. An ability to reflect on a communication before sending it may make access to it all the more privacy intrusive. Further to that, the amount of stored communications has greatly increased in recent times such that people now communicate a great deal more by emails and text messages, to the point where they carry out conversations by these means. Emails have become more like telephone conversations. The content can be as trivial or as profoundly personal as a live conversation. They can be conversations between a parent and a child in trouble; between a counsellor in an agency and a person who is contemplating suicide; contain medical details; involve messages of love and affection. They can contain scraps of information which, looked at out of context, will be misleading. They may contain criticisms of persons which will cause great damage if made public.

5.7 These interactions will be inhibited or made practically impossible if it becomes known that there are snoopers “listening” to these conversations.

5.8 The reasons for restricting access to stored communications have become the same as those for restricting interceptions. There is a case for logical consistency: the threshold for stored communications warrants should be raised to seven years.

**Recommendation 4: The Committee recommend that the threshold for stored communications warrants be raised to be equivalent to that for interception warrants.**

## **6. Communications data ("metadata")**

6.1 Communications data is information about a transmission without any of the content of the transmission. It may include details about where and when a transmission took place, with what device, and who sent it. It will include the same details about the recipient—when it was received, and where.

6.2 Although the intrusion on privacy imposed by accession to a single transmission datum may appear slight by comparison with interception of a telephone call, repeated access to metadata is as great an intrusion as an interception or access to a stored communication.

6.3 According to the annual report under the TIA Act by the Attorney-General's Department for 2012-2013, there were 319,874 authorisations for access to existing metadata information or documents in the enforcement of a criminal law—an increase of 29,516 over the previous year (more than 10%). There were a further 10,766 authorisations for access in the enforcement of a law imposing a pecuniary penalty. There were, in addition some 7,532 authorisations for access to prospective data. The total of the actual days in which these last authorisations were in force was 206,807. The average was 30 days per authorisation. These figures are mind-boggling.

6.4 Before accessing metadata, an agency is required by the TIA Act to calculate that the invasion of privacy was justified in each case by the importance to the public of solving a crime or recovering money. The figures are so great for some of the agencies (103,824 by the NSW police, 63,173 by the Victorian Police, 22,900 by the Australian Federal Police—and that is just for existing data) it is a reasonable assumption that no such calculation is made.

**Recommendation 5: That the Committee recommend that before accessing metadata, an agency should be required to obtain a warrant, which includes a proper justification of the access.**

## **7. Mandatory data retention**

7.1 The PJCIS was undecided about whether there should be a mandatory data retention regime. Recommendation 42 includes proposals for how such a regime should operate, if it is adopted.

7.2 CCL opposes the adoption of such a regime.

7.3 As CCL argued to the PJCIS, the privacy implications of the proposal are substantial. It was made plain at the time that what is proposed for Australia is the same as that in European Directive 2006/24/EC. We agree with the following passage, from a letter written to the European Commissioner for Home Affairs which was endorsed by 106 organisations including the highly respected organisations Human Rights Watch, Reporteurs Sans Frontières and Liberty UK.

We believe that such invasive surveillance of the entire population is unacceptable. With a data retention regime in place, sensitive information about social contacts (including business contacts), movements and the private lives (e.g. contacts with physicians, lawyers, workers councils, psychologists, help lines, etc.) of 500 million Europeans is collected in the absence of any suspicion. *Telecommunications data retention undermines professional confidentiality, creating the permanent risk of data losses and data abuses and deters citizens from making confidential communications via electronic communication networks. It undermines the protection of journalistic sources and thus compromises the freedom of the press. Overall it damages preconditions of our open and democratic society.* In the absence of a financial compensation scheme in most countries, the enormous costs of a telecommunications data retention regime must be borne by the thousands of affected telecommunications providers. This leads to price increases as well as the discontinuation of services, and indirectly burdens consumers.

Studies prove that the communications data available without data retention are generally sufficient for effective criminal investigations...There is no proof that telecommunications data retention provides for better protection against crime. On the other hand, we can see that it costs billions of Euros, puts the privacy of innocent people at risk, disrupts confidential communications and paves the way for an ever-

increasing mass accumulation of information about the entire population.<sup>2</sup> (Emphasis added.)

7.4 In balancing the invasion of privacy against the gains from law enforcement agencies having access to the data, the costs of the loss of confidentiality must be included. In the submissions to the PJCIS and the Committee by law enforcement agencies and their supporters, we have read no discussion of proportionality that shows an understanding of why privacy matters, of alternatives, of harm minimisation. We appreciate that members of the PJCIS have demonstrated their own concern over proportionality.

**Recommendation 6: The Committee recommend against the introduction of mandatory data retention.**

7.5 CCL urges the Committee to recommend against mandatory data retention. But if it goes ahead, as we noted in our original submissions to the PJCIS, safeguards should include logging all views of the data, demonstrated adequate encryption and security protections, certified destruction regimes so data older than 2 years are properly deleted, and at the very least, mandatory notification of any misuse of the data or any unauthorized access. Penalties should be consistent with the damage caused to society as well as the damage to individuals whose data is misused or whose privacy is breached.

**Recommendation 7: That if mandatory retention is adopted, the Committee ensures that appropriate safeguards are in place including: logging all views of the data; demonstrated adequate encryption and security protections; certified destruction regimes so data older than 2 years are properly deleted; and mandatory notification of any misuse of the data or any unauthorized access. Penalties should be consistent with the damage caused to society as well as the damage to individuals whose data is misused or whose privacy is breached.**

---

<sup>2</sup> [http://www.vorratsdatenspeicherung.de/images/DRletter\\_Malmstroem.pdf](http://www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf)



## **8. The single warrant.**

- 8.1 The innocuous looking recommendation 9 turns out, when the explanation in the body of the PJCIS report is examined, to mean the same as recommendation 10. The intention is that agencies will be able to seek a single telecommunications warrant permitting them to intercept live communications, stored communications and communications data. The act will thus be simplified--in other words, there will only be one kind of warrant, available for all purposes from preventing mass murder to solving a shoplifting crime.
- 8.2 It is not clear whether the single warrant will also cover all of person, device, attribute based and data surveillance, or whether these will have to be requested separately—though the logic of “simplifying the Act” would imply that it would. And it is not clear how B-person warrants will fit in to this. If the natural interpretation is correct, a single warrant will enable an organisation to target a number of people (including people against whom no suspicion is held), multiple devices, multiple services, and unlimited stored communications and data.
- 8.3 It is said that this change will simplify reporting. The only way this could happen is if there will no longer be separate reporting of the numbers of uses of each of the different kinds of surveillance, but only a single number comprising all of them. This, the PJCIS avers, will make it easier for the general public, law practitioners, law enforcement agencies and the justice system to understand and apply the law.
- 8.4 This is insulting.
- 8.5 It is also remarkably Orwellian. The public is to be given less information, yet somehow it will understand better. Delineating between indicators is vital for the public’s monitoring and evaluation of government agencies. Proper monitoring and evaluation of agencies is in turn critical for rational, evidence-based decision-making and the assignment of public resources.
- 8.6 Unless an application for a single warrant specifies all the persons of interest and any others to have their services intercepted, all the devices, and the kinds of interception to be used in each case, a calculation as to the balancing of public and private interests will be impossible. If all the relevant information is required before a warrant is issued, then it is hard to see that there will be a simplification.

**Recommendation 8: That the Committee recommend that the government not move to a single warrant.**

**Recommendation 9: That the Committee ensure that if a single warrant is adopted, the TIA Act is amended so that that there are adequate reporting requirements to enable**

the public to properly monitor and evaluate compliance with, and effectiveness of, the interception/access regime.

**Recommendation 10: That the Commonwealth Ombudsman be tasked with reporting to parliament on compliance with and effectiveness of the interception/access regime every 6 months.**

## **9. Sharing information**

### *Disclosure between agencies.*

9.1 Every time surveillance material is given by one agency to other agencies, the invasion of privacy is, ipso facto, increased. Further, the chance that surveillance materials are misused, leaked, misunderstood or inappropriately matched with other data increases every time the materials are transferred. And again, these materials may be highly sensitive in nature, may intrude on the privacy of people other than those who are (or were) targets. It should follow that the temptation to make it easy for people to transfer information within and between agencies should be resisted. There should remain legislative barriers to such transfer, to ensure that agencies, and officers of an agency, should not be able to receive information which they would not be entitled to seek for themselves. We agree with the Law Council that information obtained under a section 180 transfer should not be able to be disclosed for a purpose that would not itself be capable of providing grounds for a section 180 authorisation.

**Recommendation 11: The Committee ensure that the number of agencies to which information may be transferred should be strictly confined.**

**Recommendation 12: That the Committee recommend that the TIA Act ensure that an agency (*the first agency*) cannot transfer information obtained under the Act to another agency (*the second agency*), where the reason(s) the second agency is seeking the information would not justify its original disclosure to the first agency under the Act.**

**Recommendation 13: That the Committee ensure that there be no power to make regulations to extend the agencies which can receive surveillance information under the TIA Act.**

### *Destruction of irrelevant material.*

9.2 The chances of surveillance materials being misused, leaked, misunderstood or inappropriately matched with other data increase with every year in which they are kept. Materials should routinely be destroyed when they concern persons who have never been, or are no longer, of interest. Other materials should be considered for destruction on a regular basis, with the defeasible presumption that they will be destroyed after two years.

9.3 Circumstances which would tell against destruction might be:

- (a) there is a warrant permitting the continuing investigation of the person;
- (b) the information is to be used in court proceedings or a judicial inquiry; or
- (c) informing the former target will prejudice an ongoing investigation.

**Recommendation 14: The Committee urge the government to ensure that processes be required by which materials obtained under the TIA Act which are not or are no longer of interest in relation to the solving or prevention of a serious crime are routinely destroyed, and by which other all surveillance materials are routinely destroyed after two years, unless a further warrant is obtained authorising their retention.**

*Disclosure to innocent targets.*

9.4 There is a general principle of privacy protection that people are entitled to know what information is held about them. Accordingly, the Australian Privacy Principles 5.1 and 5.2 require APP entities inter alia to inform people about the fact that information is held about them, and what the authorisation is for the entity holding the information.

9.5 Law enforcement agencies and intelligence and security organisations are not covered by the Privacy Act. However it is desirable that as far as is reasonable, they should take account of the same principles.

9.6 In 2005, CCL argued that innocent people who had been subjected to telecommunication surveillance, like people who had been subjected to a covert search of their premises, should in due course be informed of the fact, and given the assurance that all the private information held about them had been destroyed. The obligation would be to disclose the surveillance after two years, unless a further warrant is obtained to permit keeping it secret. Warrants might be given on the following grounds:

- (a) there is a warrant in force permitting the continuing investigation of the person;
- (b) the information is to be used in court proceedings or a judicial inquiry; or
- (c) informing the former target will prejudice an ongoing investigation.

9.7 Such a warrant would be limited to two years, with the possibility of renewal.

9.8 This was not a novel idea. It should be readily acceptable to the law enforcement agencies. It would bring several benefits. It would enable a person who has been harmed by an improper interception to seek redress. It would enable innocent targets to clear themselves of the suspicion that led to their being spied upon in the first place. People who believed, but could not prove, that the police or ASIO agents had acted wrongly would be able to ask for the Ombudsman for an investigation. The

threat of adverse findings might well make agents and police wary of misuse of their powers.

**Recommendation 15: The Committee recommend that unless a warrant is obtained permitting otherwise, innocent people who have been subjected to telecommunication surveillance should within two years be informed of the fact and assured of the destruction of the materials.**

## **10. Oversight: Protecting the rights of targets and the public interest.**

10.1 In any kind of covert operation, the rights of the target need to be protected. Although the TIA Act includes a number of important safeguards there is no arrangement by which this can be done adequately, with the target, ex hypothesi, being absent.

10.2 Protection is needed to ensure that warrants are not being rubber stamped, that the impact of the invasion of privacy is properly evaluated (including the impact on the community, not just on the targets), that surveillance is used for proper purposes and not, for example, for fishing expeditions, to secure financial benefits to government or private enterprises, in an effort to obtain information that would discredit people, or to hound people. It is needed to ensure that surveillance does not go beyond what is warranted.

10.3 We applaud also the following remarks of the NSW Crime Commissioner, Peter Singleton to the PJCIS inquiry:

I would say that there is at least one area of weakness in our current safeguards system, and it is with respect to auditing what we do. 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.<sup>3</sup>

10.4 In Queensland for some time, and more recently in Victoria, a significant protection has been provided by Public Interest Monitors. In brief, a Monitor has the entitlement to attend all hearings of applications for warrants for covert operations including surveillance, to present submissions and to question the applicant and any witnesses. The Monitor also makes reports to the relevant ministers and to the parliament.<sup>4</sup>

---

<sup>3</sup> Draft Hansard, PJCIS hearing, Wednesday September 26, 2012.

<sup>4</sup> The monitor also has inspection powers similar to those of the Australian ombudsman with respect to law enforcement bodies, and to the IGIS with respect to control orders.

- 10.5 There are considerable benefits from this scheme. The Monitor, having records and experience of all applications, is able to discover evidence of misuse of powers under previous warrants, of fishing expeditions and of hounding of individuals. The appointment of a similar officer in each state and federally would reduce significantly the opportunities for misuse of the powers granted under this and other acts.
- 10.6 The Public Interest Monitor was created by the Borbidge Government of Queensland by the *Police Powers and Responsibilities Act 1997*.
- 10.7 The major concern leading to the decision to introduce the office was that the issue of warrants by a judge in his or her chambers, with only a police lawyer present, was unduly closed and secretive. The treatment of Matthew Heery provided an impetus. (Heery was subjected to surveillance for 600 hours, and was finally charged merely with burning a Telstra telephone bill that related to activities which were under investigation. He was acquitted. It was widely felt that the police had abused their powers.)
- 10.8 The powers of the Monitor are now governed by the *Police Powers and Responsibilities Act 2000*, the *Crimes and Misconduct Act 2001* and the *Terrorism (Preventative Detention) Act 2005*. Further powers are given to the Monitor by the Commonwealth Criminal Code.
- 10.9 The Queensland Acts require applicants for surveillance warrants, covert search warrants, additional powers warrants and preventative detention warrants (whether for interim orders, final orders or extensions of either) to inform the Monitor, under arrangements determined by the Monitor. The advice must include the time and place of the hearing of the application. The requirement is the same for all applicants, whether they are police officers or not.
- 10.10 The Monitor has the power to be present at hearings of these applications in the courts, where he or she may cross-examine or otherwise question the applicant and any witnesses. The judge is required to consider any submissions made by the Monitor, including representations made by telephone, fax or in any other reasonable way.
- 10.11 In the case of surveillance warrants and covert search warrants, the Monitor is required to monitor compliance with the laws in relation to matters concerning applications.
- 10.12 In the case of an emergency warrant, the Monitor must be advised within two days, when the applicant applies to the Supreme Court for approval of the exercise of the powers.

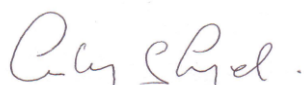
- 10.13 Similar arrangements apply when an application is made to revoke or vary a warrant.
- 10.14 Information obtained by surveillance or covert searches may be disclosed to the Monitor. (Reports on the covert searches are required within seven days of execution, and must be given to the Monitor as well as to the Supreme Court judge who issued the warrant.)
- 10.15 The Monitor is required by Section 160 of the Police Powers and Responsibilities Act to give annual reports to Parliament via the minister on the use and effectiveness of surveillance, covert search and preventative detention warrants.
- 10.16 It is essential that any body charged with oversight of the security organisations' use of surveillance, or use by law enforcement agencies, be given adequate staff and resources to do the job. It is apparent, for example, that the Office of the Inspector General of Intelligence Services is woefully under-resourced.

**Recommendation 16: That the Committee recommend the appointment of a federal public interest monitor, and one in each state and territory that does not have one, with powers along similar lines to the Queensland public interest monitor, with the duty to review applications for warrants under the TIA Act and the powers to request further particulars about any application for such a warrant and to address the issuing authority in respect of any such application. Should communications data (metadata) continue to operate outside the warrant system, appropriate internal mechanisms ought to be put in place to ensure that the public interest monitor has similar powers in respect of authorisations to access metadata by the Australian Security and Intelligence Organisation and other law enforcement agencies.**

CCL would welcome an opportunity to expand further or answer questions on any aspect of this submission.

This submission was prepared on behalf of the NSWCCCL by Dr Martin Bibby, Convenor of the Privacy and FOI Action Group with input from Jackson Rogers Assistant Secretary.

Yours sincerely



Dr Lesley Lynch  
Secretary  
NSW Council for Civil Liberties  
0416497508

-----  
**Contacts in relation to this submission**

Dr Martin Bibby Convenor of the Privacy and FOI Action Group [office@nswccl.org.au](mailto:office@nswccl.org.au)

Dr Lesley Lynch Secretary [lesley.lynch@nswccl.org.au](mailto:lesley.lynch@nswccl.org.au)