NSW Council for Civil Liberties Inc.

Postal address: PO BOX A1386 SYDNEY SOUTH NSW 1235
Office address: suite 203, 105 Pitt Street SYDNEY NSW 2000
Phone: 02 8090 2952 Fax: 02 8580 4633
Email: office@nswccl.org.au Website: www.nswccl.org.au

New South Wales Council for Civil Liberties

Subsidiary submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS)

CCL appreciates the invitation of the PJCIS for us to make a subsidiary submission.

We were asked specifically to respond to two matters: a letter from the Attorney General to PJCIS outlining what is proposed with respect to data retention and giving two examples of its usefulness, and to police submissions that they are not asking for new powers, but for the same powers in a new context.

A. The Attorney General's letter

The Attorney General's letter is concerned with only one part of the Discussion Paper: the proposal to require providers to retain data concerning telecommunications for two years, and to make that data available to agencies and organisations (the data retention proposal). It is made clear, as it always has been clear, that the retention of data is not the retention of the *content* of communications, but of what is sometimes called metadata.

Nevertheless, the privacy implications of the proposal are substantial. Ms. Roxon quotes, as a precedent, European Directive 2006/24/EC, and it is made plain that the same requirements are what are proposed for Australia. 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.

> 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, helplines, 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. Blanket data retention has proven to be superfluous, harmful or even unconstitutional in many states across Europe, such as Austria, Belgium, Germany, Greece, Romania and Sweden. These states prosecute crime just as effectively using targeted instruments, such as the data

NSW Council for Civil Liberties Inc.

Postal address: PO BOX A1386 SYDNEY SOUTH NSW 1235
Office address: suite 203, 105 Pitt Street SYDNEY NSW 2000
Phone: 02 8090 2952 Fax: 02 8580 4633
Email: office@nswccl.org.au Website: www.nswccl.org.au

New South Wales Council for Civil Liberties

> preservation regime agreed in the Council of Europe Convention on Cybercrime. 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 Euro, 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.[1] (Emphasis added.)

Ms. Roxon's letter does not consider these matters *at all*. There is *still* no attempt at balancing even the costs of the loss of professional confidentiality—the lives that will be lost unnecessarily for example—against the supposed gains from law enforcement agencies having access to the data. There is no discussion of proportionality, of alternatives, of harm minimisation. Apparently it is left to the PJCIS to do the balancing.

We appreciate that members of the PJCIS have demonstrated their concern over proportionality, in their discussions with police forces in particular.

It would appear, though it is not plain, that it is proposed that access be granted to all the sixteen law enforcement agencies that have access to telecommunication interception warrants, together, presumably, with ASIO. That is a lot of investigating detectives. Even if there is no outright corruption, there will surely be misuse.

CCL urges PJCIS to reject the proposal. But if it goes ahead, as we noted in our original submission, 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.

We applaud also the following remarks of the NSW Crime Commissioner, Peter Singleton:

> 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.[2]

---

[1] http://www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf

[2] Draft Hansard, PJCIS hearing, Wednesday September 26, 2012.

NSW Council for Civil Liberties Inc.

Postal address: PO BOX A1386 SYDNEY SOUTH NSW 1235
Office address: suite 203, 105 Pitt Street SYDNEY NSW 2000
Phone: 02 8090 2952 Fax: 02 8580 4633
Email: office@nswccl.org.au Website: www.nswccl.org.au

New South Wales Council for Civil Liberties

B. Police evidence

We took on notice a question: how we respond to the assertion, made during hearings, that the police are not asking for more powers, but for the same powers in the new context brought about by changes in technology. 'You would not have been here earlier, but we had evidence from the Australian Federal Police and from state police commissioners that was characterised, in its first instance, by our witness saying that they were not seeking additional powers…. [P]reviously we have had representatives of law enforcement, intelligence and security agencies making that strong point to us—that they are not seeking additional powers but rather the application of those powers to areas where, for example, new technology has developed and the like. I would be interested to hear from the New South Wales Council for Civil Liberties, if you accept that there is no attempt here to seek additional powers.'

CCL replies: the distinction between seeking more powers and the application of existing powers to new areas is a distinction without a difference. The agencies want to be able to do things that at present they are not permitted to.[3]

The argument, such as it is, would apply to the data retention proposal. It might conceivably apply to the proposal that ASIO be able to target third party computers. It does not apply to:
changes in thresholds for warrants/reduction to a single threshold;
the introduction of single warrants under the Telecommunications (Interception and Access) Act and under the ASIO Act;
introducing person search warrants;
giving certificates of immunity from civil and criminal liability to ASIO officers and their contacts; or
the warrant renewal proposal.

The description of changes as the application of existing powers to new areas is an invitation to invalid argument. In each case, the change requires to be justified; it is not valid to suppose that because such powers exist elsewhere, they are properly extended. The argument is irrelevant.

We have examined evidence from the agencies that have given it.

The NSW Crimes Commissioner argues that because it is acceptable that business organisations are required to keep details of transactions for several years, it is acceptable for details of all telecommunications to be kept for two years.

[3] We note that our original submission refers to 'extension of powers'.

NSW Council for Civil Liberties Inc.

Postal address: PO BOX A1386 SYDNEY SOUTH NSW 1235
Office address: suite 203, 105 Pitt Street SYDNEY NSW 2000
Phone: 02 8090 2952 Fax: 02 8580 4633
Email: office@nswccl.org.au Website: www.nswccl.org.au

This exhibits the same fallacy. Data might include records of a young person emailing Twenty10[4],, of a desperate housewife calling Lifeline[5], of an academic googling research on police corruption, of a reporter corresponding with a whistle-blower—you need argument that justifies the retention of such data. The reasons that there are for retaining business data do not apply elsewhere.

C. The proposal that ASIO officers and their contacts be given certificates of immunity from civil and criminal liability.

1. What is wrong with the proposal.

Professor George Williams comments on ASIO's questioning and detention powers:

> ASIO is a covert intelligence-gathering agency. It is not a law enforcement body. As such, it is not subject to the same checks and balances and public scrutiny as a police force.
>
> If ASIO is to be granted coercive police-like powers, it should be subject to the political and community scrutiny and controls that apply to a police force. However, this is not compatible with its intelligence gathering work. These powers, even if they could ever be justified, are simply not appropriate to ASIO.[6]

And on the bill that gave it those powers:

> Similarly, the Parliamentary Joint Committee on ASIO unanimously stated that it 'would undermine key legal rights and erode the civil liberties that make Australia a leading democracy'.

That is the point we were making about certificates of immunity, and which was a matter of contention with some members of the PJCIS.

Members of PJCIS may not be aware of recent controversy in the United States about the activities of the Federal Bureau of Investigation in setting up sting operations in which potential terrorists have been assisted in obtaining what they thought were bombs, and in the most recently reported case, actually encouraged to use them.

---

[4] This is a Sydney agency which assists gay and lesbian youth with accommodation and other problems.

[5] An agency that provides telephone counselling to people in distress.

[6] Address to the Ken and Berenice Buckley Dinner, October 19, 2012. The full text is available on CCL's website.

According to a recent article in the New York Times, the FBI have been acting in accordance with a model

> in which, in the process of flushing out people they believe present a risk of terrorism, federal law enforcement officials have played the role of enabler. Agents and informers have provided suspects with encouragement, guidance, and money and even, the subjects of the sting operations are led to believe, the materials needed to carry out an attack. Though these operations have almost always held up in court, they have come under increasing criticism from those who believe that many of the subjects, even some who openly espoused violence, would have been unable to execute such plots without substantial assistance from the government.[7]

In the most recent case, a 21-year-old Bangladeshi man is alleged to have tried to remotely detonate what he believed was a 1,000-pound bomb in a van he parked outside the building in Lower Manhattan on Wednesday. But the entire plot played out under the surveillance of the Federal Bureau of Investigation and the New York Police Department as part of an elaborate sting operation. The man tried to make contacts and recruit people to form a terrorist cell to help him carry out an attack, according to a criminal complaint in the case. But one of these recruits was an F.B.I. informer, who later introduced him to an undercover F.B.I. agent who *helped him with the plot*.

In an earlier case in 2009, several men, urged by an unusually persistent government informer, planted what they believed to be homemade bombs in front of synagogues in the Riverdale section of the Bronx. Four men were convicted, but the judge who oversaw the trial also criticized the law enforcement agents who helped push the plot forward: "*The government made them terrorists.*"[8]

It is not only the FBI and not only in America. And it is not only fake bombs.

The following extract is from the sentencing remarks in the Benbrika case *R v Benbrika & Ors* [2009] VSC 21[9]

> 34. In about May 2004, an undercover Victorian police officer who gave evidence under the name SIO 39 infiltrated the group. He pretended to be a Turkish Muslim called Ahmet Sonmez who had had experience with explosives and their use in agriculture, particularly in tree stump removal. He attended a number of dars classes

[7] http://www.nytimes.com/2012/10/18/nyregion/arrest-in-plot-to-blow-up-federal-reserve-bank.html

[8] ibid.

[9] http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/vic/VSC/2009/21.html

and similar gatherings where he began to befriend members of the jemaah. Whilst it could be concluded that he appeared to have been generally accepted into the group, some members, particularly perhaps Sayadi, were concerned at his eagerness and willingness to accept almost everything suggested to him without argument. Sayadi expressed these concerns to Benbrika who appeared to dismiss them or at least to play them down.

35 *In October 2004, SIO 39 offered to show Benbrika how an explosive could be made from a mixture of ammonium nitrate fertiliser and diesel oil. He obtained a small quantity of these materials and took Benbrika to a remote location in the bush to the north of Melbourne where he detonated a very small quantity of this material for Benbrika's benefit. The whole episode was video and audio recorded, and was subsequently put before the jury*.

36 Although, in discussions with SIO 39, Benbrika sought information as to how much explosive would be needed to destroy different targets such as buildings, houses et cetera, and where and how such explosive could be obtained, he did not ask SIO 39 to obtain explosive or, for that matter, anything else that might have been useful to the jemaah. Nor is there any evidence that Benbrika told any other members of the group of SIO 39's demonstration.

37 Argument was put that a conclusion should be reached that Benbrika was not serious about wishing to learn about explosives as, if he had been, he would have expressed greater interest than he did in SIO 39's demonstration and would have requested him to procure explosives for the group. Against this, however, must be weighed the fact that Benbrika was well aware, at all times during the indictment period, that ASIO was very interested in him and probably also in those around him. As well, other members of the group, notably Sayadi, had expressed doubts as to SIO 39's bona fides as far as his expression of support for the organisation was concerned. Benbrika's apparent nonchalance at SIO 39's demonstration and his failure to take up offers to procure explosives can be equally interpreted as caution on his part.

It is this kind of sting operation which we oppose, and the reason we do not want ASIO to be given the power to conduct major controlled operations, without the kind of oversight and potential public exposure which applies to Australia's police forces. If, as we suppose, such openness is not possible for ASIO without compromising its legitimate activities, then it should not be given the power to authorise controlled operations.

2. Problems in ASIO's history—distant and recent.

i. In its short life, ASIO has been the subject of adverse comment by two royal commissions. The first of these revealed serious misuse of ASIO by some politicians, and its apparent willingness of accede to the wishes of those politicians. Both showed grave

misunderstandings of its legitimate role. Some of our members and former office-bearers have seen their old files which reveal quite ludicrous concerns about their activities.

Since those times, changes have been made to ASIO, and it and the other members of Australia's intelligence community are now subject to the scrutiny of the Inspector General of Intelligence Services, and, importantly of the PJCIS. The latter stands as the sole bulwark defending the principle of the supremacy of Parliament, which is the foundation of parliamentary democracy.

ii. We do not now whether the members of the PJCIS have ever been told that they cannot be given access to security information.[10] It would be a matter of the gravest concern if they were. But we do know, from the PJCIS's own report, that attempts were made to restrict inquiries by the PJCIS into the prescription of organisations until after the times when the regulations proscribing them could be rejected by the Parliament. Here the Attorney General's Department showed a remarkable lack of commitment to the rights of citizens—to so basic a democratic right as the freedom of association. We assume ASIO knew about this attempt—at any rate, the PJCIS did not report its opposition to the attempt.

iii. There is the recent Ul Haque case. ASIO officers met Mr Ul-Haque and his 17-year-old brother in a railway station car park. They told Mr. Ul-Haque he was in serious trouble, bundled him into a car, took him to a local park and forced him to answer questions. They took his frightened brother along as well — an action described by Justice Adams as "highhanded". The officers were dealing with a young man of twenty-one years. 'It is obvious that any citizen of ordinary fortitude would find a peremptory confrontation of the kind described by the ASIO officers frightening and intimidating. Furthermore, *the fact that he was being taken to a park rather than any official place would have added an additional unsettling factor. I do not think it can be doubted that this was precisely the effect that was intended.*' (Emphasis added.)

And despite having no authority to do so, the ASIO officers gave Mr Ul-Haque the distinct impression that he had to cooperate with them and answer their questions. If he did not, he reasonably assumed they might beat him up or take him to another sinister location.

Then the ASIO officers took him back to his home, kept him in his parents' bedroom and proceeded to interview him again until 3.45 the next morning. None of which impressed Justice Adams, who observed, 'To my mind, to conduct an extensive interview with the accused, keeping him incommunicado under colour of the warrant, was a gross breach of the powers given to the officers under the warrant.'

[10] Dr. Vivienne Thom, the Inspector General of Intelligence and Security, reports that she has access to every piece of paper in the security agencies' possession.

Justice Adams was not impressed by the evidence of the ASIO officers, and in his view, they had kidnapped and falsely imprisoned Mr. Ul-Haque and trespassed on his family's home.

From our point of view, a serious condemnation of ASIO is that the actions of these officers were defended.

iv. ASIO has been cooperating with the Government in condemning refugees to indefinite detention, conceivably for life, with no proof of any crime and with no opportunity to challenge their detention. We have yet to hear the opposition of the Director General to proposals to change the Migration Act in response to the High Court Judgment in the recent High Court Case Plaintiff M47-2012[11], so that the situation can continue.

v. Our information from barristers is that the Security Information (Civil and Criminal Proceedings) Act is appealed to unreasonably, to the point where barristers are unwilling to take some cases because they are prevented from offering a proper defense.

vi. Two of the issues before the present inquiry, the proposal that ASIO be able to access third party computers and especially the general proposal that agencies be relieved of the duty to keep records, are not promising. Dr. Thom writes: 'Comprehensive record-keeping in ASIO is essential to ensure ASIO complies with the legislation and to enable effective oversight. Any proposal to change the record-keeping regime must consider the accountability requirements'[12]. We assume that she would not have done so if the change did not have the support of ASIO's officers.

The point Dr. Thom makes, and which we made in our own submission[13] is obvious—oversight is impossible without these records. It does not speak in ASIO's favour that it supports the proposal.

We have, then, reason to believe that all is not well with ASIO; that its lack of commitment to the principles of liberal democracy lingers or is being reborn.

3. Conclusion.

[11] Plaintiff M47-2012 v Director General of security [2012] HCA46 (5 October 2012).

[12] Submission 185, p.8.

[13] Submission 175, section 15

NSW Council for Civil Liberties Inc.

Postal address: PO BOX A1386 SYDNEY SOUTH NSW 1235
Office address: suite 203, 105 Pitt Street SYDNEY NSW 2000
Phone: 02 8090 2952 Fax: 02 8580 4633
Email: office@nswccl.org.au Website: www.nswccl.org.au

We note comments made at our hearing that what is proposed is immunity from some ancillary offences only. In relation to Terrorist acts (T-acts), there are *legislated* ancillary offences under the Criminal Code including providing training or possessing things connected with a T-act, making documents likely to facilitate a T-act, doing anything in preparation for or planning a T-act. There are further ancillary offences under the proscription provisions—the funding, supporting and associating offences for example. Then, courtesy of section 11 of the Code, there are *second order* ancillary offences—inciting a person to make a document, conspiring to fund, abetting training, and so on. It is difficult to comment succinctly without knowing which offences it is proposed that the immunity should cover.

While we do not think that ASIO officers would engage in a real act of terrorism in order to obtain convictions, we do not think the organisation is immune from setting a sting of the kind in which the FBI have been indulging. And because of the secrecy provisions, it would be difficult to uncover wrongdoing. It would be impossible to obtain the information in a proceeding, as happened with the FBI. It would be difficult to expose wrongdoing if it were discovered.

ASIO should not be Australia's secret police force.

Martin Bibby
Executive member, NSW Council for Civil Liberties
October 22, 2012