

## Australian Privacy Foundation

### Committee Inquiry into a Comprehensive Revision of *Telecommunications (Interception and Access) Act 1979*

#### CONTENTS

APF's Standing as an Interested Party	1
Scope of Inquiry	1
Wider Context	2
Access regimes	3
s.313 of the <i>Telecommunications Act</i>	4
Use of the Access Powers	5
Progressive weakening of controls over interception	7
Blurring of Vital Distinction between National Security and Law Enforcement	8
The Metadata Furphy – Metadata Surveillance is Still Surveillance	8
Warrants and metadata	9
Data Retention Requirements	10
Proportionality principle	10
Need for government response	11

## APF's Standing as an Interested Party

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

The APF has been a regular contributor to inquiries and reviews concerning the telecommunications interception regime for more than 20 years. In addition to copies on official websites, many of our submissions are indexed at:

<http://www.privacy.org.au/Papers/indexPolicies.html#TelecommsIA>

We draw attention in particular to our submissions to previous Senate Legal and Constitutional Affairs Committee inquiries into Amendment Bills in 2002, 2004, 2006, 2007, 2008, 2009 and 2010, and to the 2005 Review of the Regulation of Access to Communications under the Telecommunications (Interception) Act 1979.

## Scope of Inquiry

While the terms of reference appear to confine the review to the Telecommunications (Interception and Access) Act 1979 (hereafter, TIA Act) itself, both of the reports referenced address the issues of the relationship between the TIA Act and other relevant laws including the ASIO Act 1979, the Telecommunications Act 1997, the Privacy Act 1988, the Intelligence Services Act 2001 and the Surveillance Devices Act 2004.

We accordingly submit that the Committee should not be feel constrained from addressing these relationships to the extent that they are relevant.

## Wider Context

Ideally, the Committee should look at the wider context of government surveillance in Australia. The specific concerns that have been raised recently, in the wake of the Edward Snowden revelations concerning US NSA activities and relationships with foreign (including Australian) intelligence agencies, involve surveillance allegedly carried out by the Australian Signals Directorate (formerly the Defence Signals Directorate) under the Intelligence Services Act. The JPCIS Report touched on the issue of collection of intelligence on Australian persons (Recommendation 39).

A full picture of the circumstances within which Australian government agencies are able to monitor the activities or communications of persons in Australia, or Australians overseas, and the safeguards which apply, requires consideration of a wide range of legislation and of surveillance practices.

While some of this may seem to fall outside the terms of reference for this inquiry, it is directly relevant at least to the extent that safeguards in the TIA Act may be rendered worthless if they can be avoided or circumvented by conducting surveillance under other sources of authority, or by using relationships with overseas agencies. Recent revelations have provided some evidence that the relationships between agencies in the 'five eyes' countries (US, UK, NZ, Canada and Australia) may be particularly problematic and needs to be subject to much greater accountability, and transparency.

The wider context also necessitates a review of the various requirements for private sector organisations to collect and hold information about the activities of their customers or clients. The best known and most extensive of these are the reporting requirements under tax legislation, facilitated by the use of the tax file number; and the 'know your customer' and reporting obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act of 2006 (AML/CTF Act). We note that a statutory review of the AML/CTF Act has just commenced but this is an in-house review by the Attorney-General's Department, with obvious consequential limitations.

We note that a broad range of politicians, organisations and governments in Europe and North America, including the Council of Europe (a key intergovernmental body that seeks to strengthen law enforcement) and German premier Angela Merkel) clearly express our disquiet regarding pervasive data collection and sharing. That concern is particularly pertinent because there are indications that data collection by the US NSA has in fact not been notably effective in either the detection nor prosecution and conviction of people who pose a threat to public safety. (In that respect see for example the January 2014 report by the US Privacy and Civil Liberties Oversight Board report on the 'bulk telephone records program operated by the National Security Agency' under s 215 of the *USA PATRIOT Act* and review of the operation of the Foreign Intelligence Surveillance Court')

We also note that the Inspector General of Intelligence & Security (IGIS), the national government agency that serves as a watchdog over intelligence bodies under the Inspector-General of Intelligence and Security Act 1986, has in a recent submission recurrently:

- emphasised the importance of privacy
- highlighted the need for proportionality, i.e. an appropriate balance between privacy and what is essential for law enforcement or public administration
- recognised that there is a difference between what is administratively convenient and what is necessary for public safety

IGIS for example clearly indicated that privacy was not subservient to intelligence activity. It stated that inclusion of an objectives clause in the Act would recognise:

the need to balance the privacy of users of the telecommunications services in Australia with ASIO's investigative requirements for security and foreign intelligence purposes.

IGIS further stated that it has

a particular interest in whether proposed changes place sufficient weight on maintaining the privacy of individuals, and whether proposals reflect the concept of proportionality – that is, that the means for obtaining information must be proportionate to the gravity of the threat posed and the likelihood of its occurrence. The exercise of ASIO's TIA powers will, almost always, not be apparent to the subject. Further, the use of ASIO's powers is not usually subject to scrutiny by a court or through legal processes as can often occur for law enforcement agencies. As ASIO's use of TIA powers is often highly intrusive, these powers should only be considered for use when other, less intrusive, means of obtaining information are likely to be ineffective or are not reasonably available.

Any proposal to apply a consistent proportionality test will need to be examined carefully to ensure that it does not compromise privacy objectives.

That recognition of the importance of privacy and wariness about overreaching by governments is evident in past submissions by the Australian Foundation and by bodies such as the Law Council and Law Institute of Victoria that are representative of the legal community as a whole.

We note with concern that in many instances submissions from central agencies such as the Attorney Generals Department, in this matter and in relation to the earlier proposed metadata retention regime, do not appear to appreciate the fundamental importance of personal information security, privacy and confidentiality to individuals, business and the community, both in and of themselves as primary rights, and also as the foundation for other fundamental rights and freedoms, such as freedom of speech, freedom of association and freedom of belief. This raises questions as to the degree to which they have exercised the necessary balancing consideration between operational effectiveness for certain forms of law enforcement and intelligence gathering, on the one hand, and the potential for excessive, ineffective and blanket surveillance programs to undermine the very values which they are charged with upholding, on the other.

## Access regimes

There are currently three primary regimes for access to information about telecommunications under the TIA Act:

- Access to 'contents and substance' of telecommunications during passage (i.e. in real time):

Warrant regime under TIA Act Part 2:

- by ASIO under Part 2-2
- by other specified 'interception agencies' under Part 2-5

- Access to 'contents and substance' of 'stored communications' (e.g. emails, SMS, message bank) by 'enforcement agencies':

Warrant regime under TIA Act Part 3-3,  
supported by provisions for preservation notices in Part 3-1A

- Access to other telecommunications data – including call records and other so-called 'metadata':

Non-warrant 'authorisation' regime under TIA Act Part 4:

- by ASIO under Division 3
- by other enforcement agencies under Division 4
- on behalf of foreign law enforcement under Division 4A

The application of the warrant regimes to 'contents or substance' of communications is indirectly specified in the TIA Act in that the authorisation of access to other data regimes in Part 4 expressly excludes 'contents and substance' leaving it implicit that access to such 'real time' information is controlled by Part 2. Part 3 covers stored communications which by definition includes both substance and content and other information.

Consideration should also be given to whether the current definitions in the TIA Act adequately protect all communications using new technologies which are analogous to out-dated concepts of 'voice calls' or 'messages'. It is important that the TIA Act is updated to ensure that consistent levels of protection are afforded to broadly analogous methods of communication. Specifically, consideration should be given to the protection offered to communications which may be between more than two parties but not 'public', e.g. within closed user groups.

## **s.313 of the *Telecommunications Act***

Consideration should also be given to s.313 of the *Telecommunications Act 1997* (Cth). Evidence has emerged in recent years that this 'general assistance obligation' section has been used by some agencies as a way of accessing information (including communications data) from carriers and carriage service providers (including telcos and ISPs), in circumstances where they should arguably be using one of the TIA access regimes, or where use of s 282 of *Telecommunications Act* has been questioned.

It is important to note that s.313 can be used by an even wider range of agencies than can use powers under the TIA Act. And that it is really two separate wings, for crime prevention and one for law enforcement: it is not a single provision, contrary to popular discussion. The crime prevention wing has no limitation on who may wish to assert what should be done in respect of the obligation it creates, although it creates no requirement to comply with such assertions either. The law enforcement wing requires giving help requested by "officers and authorities of the Commonwealth and of the States and Territories", though the latter appears to have been interpreted to extend to entities empowered under state law.

The recent content-blocking use of the s 313(1) and s 313(2) crime prevention wing (below called "313(1)"), while controversial, is a distraction in this discussion. The other 313(3) and 313(4) law enforcement purpose wing ("313(3)") is about traditional interception for law enforcement purposes, detection and prosecution of offences committed. 313(1) is unbounded as to who may make suggestions for what should be done, which is broader than 313(3), which is in turn broader than the TIA Act.

Three unusual features of s 313(1) are not found in 313(3):

- the open-endedness of the s 313(1) exhortation to "do your best"(!),
- the unusual 'crime prevention' focus, where we consider prospective future offences, potentially of any type and at any future time, rather than law enforcement's focus on evidence of specific past offences for prosecution, and
- the lack of any accountability for the 313(5) and (6) immunity, a removal of liability for collateral damage (of whatever type) unintentionally caused by speculative good faith 'preventive' activities, not tied to a specific request for assistance by a class of agencies as in 131(3),

Together these mean that 313(1) is potentially open to use as part of a practice of informal suspicionless, warrant-less 'persuasive' pressure on ISPs or carriers from almost any agency or authority, or indeed anyone at all (unlike 313(3)) who decides to knock on their door with a helpful suggestion as to what "doing your best" might mean here.

By their nature these demands would be informal, difficult for the public or customers to detect, and unlikely to be reported on, because they do not represent the exercise of a formal power: unlike 313(3) for law enforcement, 313(1) for crime prevention does not as noted above formally create a power for anyone to request help, nor an obligation to give it. Note also that it is not appropriate to use the full arsenal of coercive and aggressive law enforcement tools for crime prevention, which is typically not the core business of law enforcement agencies, and by its nature is speculative, not subject to judicial review, and largely lacking in credible studies about efficacy.

(A recent case dismissing the effectiveness of a specific CCTV program for crime prevention purposes, after examination of the evidence, has a useful discussion of this difference, between the level of intrusion justified by crime prevention and the greater level appropriate for law enforcement.

It concludes that the intrinsically speculative and unprovable effectiveness of crime prevention efforts must be matched by caution and full consideration of unwanted side effects, compared to the more robust tactics and agencies appropriate for law enforcement: *SF v Shoalhaven City Council* [2013] NSWADT 94, at: <http://www.austlii.edu.au/au/cases/nsw/NSWADT/2013/94.html>. There are few if any cases on the current issue under the TIA Act, or the federal Privacy Act for that matter, so the discussion, though in a NSW not a federal tribunal, is of assistance on the general question.)

Anecdotal evidence suggests however that there is some of this 'persuasion' going on, and many carriers would be reluctant to antagonize authorities by refusal; but hard evidence is intrinsically elusive. In the US a large range of such informal discretionary surveillance activities was ultimately if reluctantly confirmed by ISPs and carriers after being revealed by Snowden's material, and it is possible that the same approach may gain hold here, enlivened by the ambiguity and informality of s313(1), and the license to cause harm without liability in s313(5) and (6), if done in good faith.

We cannot seek to prove any particular activity is going on at any particular level, due to the lack of formality and the lack of data, and joint incentives to secrecy (both parties don't want to scare the customers). But we can say that 313(1) is no way to leave a back door method for informal surveillance. Surveillance, including metadata surveillance, should be removed from its ambit, and kept in 313(3) TA, or in the TIA Act.

S 313(1) TA thus deserves amendment to add much greater constraint and specificity to limit its scope for being called on in aid of vague, open-ended, un-enforceable but potentially irresistible demands for 'crime prevention'-directed surveillance, data retention and/or metadata analysis.

## Use of the Access Powers

We offer our summary of the level of use of the various powers below.

They show a steady and substantial increase in all varieties, and confirm that metadata collection is occurring on a massive scale, unlikely to be tied to specific suspicions, not subject to warrants, and similar in form to other warrantless, suspicionless mass surveillance programs come to light in other countries. The scale of this latter activity, and its continued growth, is a matter of grave concern.

## Interception warrants

	2012-2013	2011-2012	2010-2011	2009-2010
Number of telecommunication interception warrants issued*	4232	3755	3488	3584
Average period TIW in force (days)	56	55	56	52
% of warrants issued by non-judicial issuing authorities (nominated AAT members)	79%	83%	85%	81%
Number of named person warrants issued	895	701	628	550
Number of B-Party warrants issued	120	149	111	120

\*This is not specified in the Annual Reports, but calculated by adding other figures in AR (no warrants issued by Federal Court Judges, Family Court Judges, Federal Circuit Court Judges and nominated AAT members). *Note that the total number given in the table 'Application for telecommunication interception warrants' (table 3 of 2013 AR) does not equal the aggregate of warrants by issuing authority (table 2 of 2013 AR).*

### Issuing Authorities: Most warrants are issued by AAT members

(Source: TIA Act Annual Report 2012-13, pg. 10-11)

Number of eligible judges and AAT members who can issue warrants:

<i>Issuing Authority</i>	<i>Number Eligible</i>
Federal Court Judges	11
Family Court Judges	8
Federal Circuit Court Judges	34
Nominated AAT Members	37

### Law enforcement:

No of prosecutions and convictions where lawfully intercepted information was given in evidence

	2012/13	2011/2012	2010/2011	2009/2010
Prosecutions	6746	5928	3168	3079
Convictions	2700	2267	2034	2180

## Stored Communications

	2012/13	2011/2012	2010/2011	2009/2010
Total applications for stored communication warrants	561	483	298	285
Total number subject to conditions or restrictions	40	23	8	2

### Law enforcement:

Based on evidence from stored communication warrants, law enforcement agencies made:

	2012/13	2011/2012	2010/2011	2009/2010
Arrests	132	106	91	113
Prosecutions	152	191	33	48
Convictions	65	69	33	49

## Telecommunications Data

Part 4-1 of the TIA Act enables enforcement agencies to authorise the disclosure of telecommunications data by telecommunications carriers or carriage service providers in certain circumstances.

Telecommunications data, also referred to as metadata, communications data and communications associated data, is information about the process of a communication, as distinct from its content.

### Existing information

*Total number of authorisations made for access to existing information or documents in the enforcement of a criminal law – section 186(1)(a)*

	2012/13	2011/2012	2010/2011	2009/2010
No. of authorisations made by a Law Enforcement Agency	312,929	280,973		
No. of authorisations made by	6254	7866		

a Commonwealth Agency				
No. of authorisations made by a State or Territory Agency	691	1519		
Total	319 874	290 358	243 631	282 195

### Prospective data authorisations

	2012/13	2011/2012	2010/2011	2009/2010
Number of authorisations made	7532	5811	4836	3804
Average actual no of days in force	30	28	27	30

With any authorisation regime (including warrant schemes) it is impossible to judge whether a high approval rate is a positive (reflecting the effect of the need for approval on the frequency and care with which applications are made) or negative (reflecting a lack of scrutiny or care by the approver). The public essentially has to rely on trusting the approvers.

This is one reason why the progressive transfer of authorisation powers from independent judges to employed tribunal members and public servants is a matter of serious concern.

At least in the case of the warrant regimes under the TIA Act, statistics are published on the approval rate. But even this level of transparency is missing for the hundreds of thousands of annual authorisations under Part 4.

We note that between July 2012 and June 2013 there were 319,874 authorisations by Australian governments for access to telecommunications information. Those authorisations included Bankstown City Council, Ipswich City Council, Knox City Council, Wyndham City Council, the RSPCA in three states, Australia Post, the Clean Energy Regulator, Workcover NSW, WA Department of Fisheries, Australian Health Practitioner Regulation Agency, Tax Practitioners Board, Medicare, Department of Immigration & Citizenship, Harness Racing NSW and the national and state police forces. It appears that much of that access does not relate to national security or serious crime.

It is of increasing concern among the legal community, civil society organisations, industry and public administration that the number of bodies that are gaining access to telecommunication data under the TIA is increasing, particularly as there has been no clear demonstration that such access is effective and proportionate.

We suggest that the Committee should consider whether it is appropriate for every local government in Australia to have ready access to the telecommunication information of people who have not been convicted of a criminal offence and are likely in many instances to be involved in minor civil infractions rather than serious crime. The current regime is open to abuse by junior officials (and the contractors who provide services in many local government bodies). Bureaucratic convenience is not the same as essential and appropriate.

## Progressive weakening of controls over interception

APF has documented the progressive weakening of controls over interception of telecommunications in numerous submissions to previous inquiries over the past 20 years. Key changes have included:

- Progressively broader criteria for warrants, allowing for them to be granted in relation to lesser offences
- Progressively broader scope of warrants, for instance to allow for interception of 'B party' communications and all communications of 'named persons' rather than communications made using particular devices

- Introduction of a new regime for access to stored communications which has weaker safeguards than the regime for ‘substance and content’, notwithstanding that stored communications (such as voice messages and emails) can contain at least as sensitive and intimate contents as real time voice communications
- Provision for warrants to be issued by designated members of the Administrative Appeals Tribunal (AAT) most of whom are non-tenured, and therefore without the guaranteed independence of tenured judges.

Annual Reports show that the vast majority of interception and stored communication warrants are now routinely issued by AAT members rather than by federal court judges

As we have previously acknowledged, some of the changes made to regimes have been sensible responses to changing technologies, and to the nature of the threat environment. However, the effect has been a major dilution of the limits and safeguards applying to the power of governments to intrude into the private affairs of Australians. Figures published in various annual reports show that government agencies have taken full advantage of this dilution, progressively extending the volume and type of intrusion.

## **Blurring of Vital Distinction between National Security and Law Enforcement**

We refer to our submission to the Committee on the Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, at <http://www.privacy.org.au/Papers/Sen-TIISL-101028.pdf>, together with the supplementary submission, and the transcript of oral evidence to the Committee.

In that Submission, APF raised serious concerns about the erosion of deliberately and carefully constructed walls separating the roles of national security and law enforcement. We have not had the opportunity to review the final form of those amendments or to check if there have been any subsequent amendments, but we submit that the Committee should take this opportunity to revisit the issue of the respective roles of the very distinct intelligence and law enforcement agencies.

## **The Metadata Furphy – Metadata Surveillance is Still Surveillance**

In the recent debates worldwide over surveillance, governments have routinely offered re-assurance that access is ‘only to metadata’ – meaning to information such as the participants in a communication and the date/time/duration – and seeks to contrast this with the ‘content’ of communications which is asserted to be subject to more rigorous access regimes.

This distinction conveniently overlooks the fact that so called ‘metadata’ can be very revealing about the nature of communications and underlying behaviour and relationships – which is precisely where the possible value to the monitoring agencies is to be found.

When combined with the lesser safeguards applying to stored communications such as email and other messages, it is clear that the ‘judicial warrant’ safeguards only apply to a small and diminishing subset of potentially sensitive communications data.

In a recent widely reported study, researchers confirmed the factual basis for US judge Leon’s finding that metadata from one’s phone reflects ‘reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.’ They also showed potential drug use, medical conditions, political associations and after hours activities with strip clubs.

(See Mayer and Muchler, *Metaphone*, the sensitivity of Telephone Metadata, 12 March 2014, Stanford ‘Web Policy’, at: <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>)

The nature of capabilities around so-called Big Data tools has been explored in the recent book ‘Big Data,’ by Viktor Mayer-Schönberger, professor of Internet governance and regulation at the Oxford



Internet Institute at Oxford University, and Kenneth Cukier of the Economist. Their work confirms that the modern online set of small, cheap, pre-labelled metadata, and what can be done with it using the machine learning tools now being developed at an unprecedented rate, provides potentially much more information about a person, their movements, their associations and their interior life than the expensive, ambiguous, oversized blobs of sound, vision or text captured by “content” surveillance. Both may be useful to law enforcement, but the prospects for mass scale abuse are essentially now all about metadata, not content.

This distinction itself also makes less and less sense, as the click-stream from using online applications like Gmail or Facebook, even absent the actual content addressed, embeds substantial information about that content in the metadata.

There is also no doubt that with the right tools, metadata is not anonymous, it is “personal information”, especially under the new Australian definition in the Privacy Act, which takes more account of the potential for re-identifying fragments of information than does the US concept of “personally identifying information” (PII) upon which some metadata thinking relies.

In short, while in the 1970s, ‘80s or ‘90s in relation to the simple analogue telephone system, there may have been a large difference between metadata (number and time called) and content, and the richness of the latter have been much more than the former, in the 2014 of digital networked phones and online interactive services with personal GPS, cameras, microphones and movement detection attached to insatiable longitudinal metadata logging, the inbuilt safeguards against abuse of metadata have disappeared, its central role in surveillance has overtaken that of content (whether divorced from that content or not), and its potential as a source of mass personal surveillance information has been confirmed.

It is no longer appropriate for this metadata-content distinction to be used as the basis for discounting the significance of mass surveillance practices using metadata. It is a furphy to assert there is any basis for seeing metadata as less intrusive, revealing or concerning than content. We understand from reports that the Northern Territory Police submission has noted that a shift away from traditional telephony services to Facebook, Twitter, Google Plus and others meant that data may be included in browser histories, and other police agencies are also keen to include browsing history in metadata.

## **Warrants and metadata**

Metadata and content should be treated similarly, and in particular, the traditional legal process for authorising breaches of an individual’s rights, namely the intercession of an independent judge assessing the specific case made in an application for a warrant should be applied to metadata surveillance. If this surveillance is on a huge scale, with no consideration taken of association with individual offences or threats, the requirement for a warrant may offer a useful discipline, even the bizarre “administrative” warrant associated with TIA Act: *Hilton v Wells* [1985] HCA 16. (US-style bulk ‘program authorisation’ warrants don’t count.)

If on the other hand the proponents of an ever expanding warrantless, suspicionless mass surveillance regime wish to make a case for setting aside centuries of legal protection, in the form of the search warrant, intended as a bulwark against the excesses of the executive and the development of the tools for an authoritarian state, then such a case should be made explicitly and publicly, with proper examination of the evidence for the effectiveness of warrantless, suspicionless metadata for prospective surveillance for serious, exceptional offences like terrorism.

Recent official confirmation that the US programs revealed by Snowden, the largest known metadata programs, appear not to have been effective in any identifiable terror incident, should form the foundation of the evidence-based aspect of any such discussion, in preference to the generally unsubstantiated assertions of its efficacy.

(The recent Australian arguments in favour of the case for mass warrantless, suspicionless metadata retention and surveillance are generally quite underdeveloped when it comes to rigorous

analysis of costs, risks, and effectiveness compared to other policing options, such as comparative cost, risk and effectiveness of properly targeted surveillance versus open-ended and indiscriminate harvest of bulk metadata. As with the underdeveloped arguments for the sketchy retention plans offered in 2012 and 2013, current arguments appear to still rely largely on assertion and rhetorical appeal rather than detailed evidence-based assessment of the full range of options, benefits, costs, risks to the community, and alternatives. It appears the proponents are convinced that mass warrantless metadata retention and surveillance programs are essential, but they do however have difficulty in explaining why in a way which would stand up to evidence based sceptical inquiry. Given the close agency identification with “the community” of agencies in other countries, and the risk of tunnel vision around such an enthusiastically supported program, it would be interesting to ask if the recent public failure of the equivalent US programs to deliver any identifiable anti-terror benefit, or benefits beyond those which traditional good policing and interagency cooperation would have delivered in say the Boston case, have been re-factored into Australian calculations.)

Finally, if the traditional Western civil protections against improper search, seizure or surveillance are to be set aside, not for exceptional matters like terror threats, as are often relied on as justification, but for open-ended fishing expeditions using the massive collections of metadata to search for minor offences, or to pursue parking infringements, then this too should be put on the public agenda for assessment and debate, rather than occurring by scope creep.

## **Data Retention Requirements**

The JPCIS Report correctly identified proposals to require communications providers to retain data for the convenience of intelligence and law enforcement agencies as a very significant privacy issue, and one which had been almost hidden in the terms of reference of their Inquiry.

Many submissions were made on this issue, and it remains important context for this review of the interception and access regime. Submissions made by key proponent agencies often appeared oblivious to the threats to personal information security, privacy and business confidentiality implicit in the proposals, or the practical constraints respect for such universal interests would require.

The notion that it would be handy to hoard everything for years in case some use were found remains deeply concerning; not least because a trove of such commercial, political and psychological value would be an irresistible honeypot lure for users authorised and unauthorised, and recent events have demonstrated that no entity can credibly promise to keep such data secure. Its existence unused could also invite uses to be invented to justify its cost.

Clearly the degree of potential privacy intrusion depends only partly on the powers of access, and partly on the amount of information available to be accessed. There is in our view no justification for requiring communications providers (or any other businesses) to retain personal information beyond the period which can be justified for business purposes.

## **Proportionality principle**

One the greatest objections to the current surveillance regimes is that they are disproportionately privacy intrusive. They operate on the premise of a reversal of the usually accepted onus on government agencies to justify why privacy intrusion is necessary to meet other public policy interests, on a case by case basis.

The communications of ordinary individuals are being routinely monitored on the basis that it may be useful, or may reveal patterns which would justify further investigation (“fishing expeditions”). In free democratic societies, there can be no justification for such mass surveillance. It is important to avoid sliding into a way of thinking where every citizen is by default treated as a suspect.

The intoxicating temptation to aim to “collect everything” (regardless of benefit or risk) -- now a technical possibility thanks to the combination of massive extensions of programs in 5 Eyes members, and the advent of a breathless Big Data mindset which at worst wants to grab everything

first and let Machine Learning tools ask questions later -- should be recognised for what it is: a potential threat to not only privacy, personal information security and business confidentiality, but also to other key rights depending on these foundations, such as freedom of speech, association, religion and belief, the pillars we should be seeking to protect.

We draw the Committee's attention to a set of **International Principles on the Application of Human Rights to Communications Surveillance**, developed by a broad coalition of international more than 400 civil society NGOs, at <https://en.necessaryandproportionate.org/text>.

We submit that these principles should be adopted as a benchmark for a fundamental and broad review of the Australian communications surveillance regime.

We note also that IGIS has strongly emphasised the importance of proportionality and the protection of privacy. That emphasis by a national government body that works closely with the intelligence community is particularly significant.

In essence, IGIS is calling for **stronger** and better privacy protection. It has not found that law enforcement and national security are weakened by privacy. It – along with most people and the Australian Privacy Foundation – instead recognises that an overly broad statutory platform, persistent expansion, and exploitation by non-government bodies (eg the RSPCA) and local government (for example over parking infringements):

- erodes trust in government and in the communications environment
- imposes an inappropriate burden on business
- encourages the use of sledgehammers to break eggshells.

We look forward to both the committee and agencies engaging more robustly with the implications of these insights, and accepting a need to take action to restore the balance that appears to be at risk.

## Need for government response

We submit that most of the recommendations in Part J of the ALRC Privacy Report 108, and in the JPCIS Report in 2013, deserve serious consideration by government.

It is extremely disappointing that the government has still not responded formally, after 5 years, to the ALRC Recommendations in Part J of its 2008 report. Hopefully a response to the JPCIS report will not take as long.

This Inquiry does at least provide an opportunity to reinforce the earlier recommendations, in light of important revelations about the extent of government surveillance of communications, both here in Australia and worldwide.

It is no longer acceptable for governments to hide behind a veil of secrecy, on the excuse of 'national security', when it has become clear that powers granted to government agencies have been abused, in some cases involving unlawful activity.

## **Australian Privacy Foundation**

### **Background Information**

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, Subcommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, Subcommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies <http://www.privacy.org.au/Papers/>
- Resources <http://www.privacy.org.au/Resources/>
- Media <http://www.privacy.org.au/Media/>
- Current Board Members <http://www.privacy.org.au/About/Contacts.html>
- Patron and Advisory Panel <http://www.privacy.org.au/About/AdvisoryPanel.html>

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) <http://www.privacy.org.au/About/Formation.html>
- Credit Reporting (1988-90) <http://www.privacy.org.au/Campaigns/CreditRptng/>
- The Access Card (2006-07) [http://www.privacy.org.au/Campaigns/ID\\_cards/HSAC.html](http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html)
- The Media (2007-) <http://www.privacy.org.au/Campaigns/Media/>