Australian Mobile Telecommunications Association (AMTA)

Communications Alliance

Internet Industry Association (IIA)

Response

to the

Senate Standing Committee on Environment, Communications and the Arts

Inquiry of the Adequacy of Protections for the Privacy of Australians Online

23rd July 2010

Confidentiality

1 Communications Alliance, the Australian Mobile Telecommunications Association and the Internet Industry Association ("the Associations") submit this response to the current Inquiry of the Senate Standing Committee on Environment, Communications and the Arts ("the Committee") on the Adequacy of Protections for the Privacy of Australians Online ("the Inquiry") on the basis that this response is recognised as being confidential in nature and is held in confidence by the Inquiry. The subject matter that is the focus of this submission concerns matters of law enforcement and government interaction that only occur on the basis of such confidentiality and as such this confidentiality must be maintained.

Motivation

2 The Associations") would like to take the opportunity of the current Inquiry of the Senate Standing Committee on Environment, Communications and the Arts ("the Committee") on the Adequacy of Protections for the Privacy of Australians Online ("the Inquiry") to focus on the specific privacy issues that are raised from the prospect of a legislated data retention regime in the telecommunications sector.

3 The Associations and their members have this focus due to the general responsibility that carriers and carriage service providers ("the industry") in Australia have to provide reasonable assistance to law enforcement and national security agencies (LEAs) to assist in the prevention of crime and the prosecution of criminals. The industry has a long history of close collaboration with LEAs and demonstrates that this responsibility is taken very seriously by the telecommunications sector. The industry has accommodated requests from LEAs wherever possible and typically the industry willingly cooperates to the maximum extent permitted under the Telecommunications Act 1997 and the Telecommunications (Interception and Access) Act 1979.

4 Part of the discussion of co-operation has included from time to time the potential for a legislated data retention regime to be introduced in Australia to ensure that LEAs have access to customer information on Australian citizens should the need arise in an investigation.

5 Any capture and storage of data generated by customers using a telecommunication service raises issues of data access, protection and privacy. Such issues are only more complex and difficult when the capture and storage of such data is mandated by government on every citizen of Australia on a 'just in case' basis – in other words there is no particular demonstrable need in relation to a data subject's information at the time of its capture and storage. Any such mandate requires close scrutiny from the privacy perspective (amongst others) to ensure that:

(a) it is justified in its introduction and will provide verifiable benefits, and

(b) if justified, it is limited in scope to match the demonstrable need; and

(c) on introduction it is accompanied by clear policies and safeguards as regards use, access and security,

so as to prevent overreach, disproportionate outcomes and other unintended consequences.

6 Therefore, the Associations would like to take the opportunity of the current Inquiry to reiterate our fundamental concerns regarding the future protection of the privacy of Australians online should a data retention regime in any of the forms advocated from time to time by the Attorney-General's Department be translated

into law.

Background

7 LEAs in Australia already have extensive mechanisms available under law to access data pertaining to the activities of end users of telecommunications services in Australia. This includes:

(a) voluntary disclosure by the service provider of information or documents where reasonably necessary for the purposes of enforcing criminal law and laws imposing monetary penalties, protecting the public revenue and safeguarding national security or in connection with the performance of the Organisation's functions (ss 174, 177 of the Telecommunications (Interception and Access) Act, 1979 ("the Act"));

(b) access to pre-existing information or documents pertaining to the affairs or personal particulars of end users of telecommunications services for the purposes of enforcing criminal law and laws imposing monetary penalties, protecting the public revenue and safeguarding national security or in connection with the performance of the Organisation's functions. Access to this information is gained by provision to the relevant service provider of notice of the authorisation by an authorised officer that the disclosure is reasonably necessary for the abovementioned purposes or in the case of the Organisation that the disclosure is made in connection with the Organisation's functions (ss 5, 175, 178 and 179 of the Act). LEAs can request access to the content of any communication;

(c) access to specified information or specified documents that come into existence during the period for which the authorisation is in force (which cannot be longer than 90 days) pertaining to the affairs or personal particulars of end users of telecommunications services for the purposes of enforcing criminal law and laws imposing monetary penalties, protecting the public revenue and safeguarding national security or in connection with the performance of the Organisation's functions. Access to this information is gained by provision to the relevant service provider of notice of the authorisation by an authorised officer that the disclosure is reasonably necessary for the abovementioned purposes or in the case of the Organisation that the disclosure is made in connection with the Organisation's functions (ss 5, 176 and 180 of the Act);

(d) access to stored communications by way of a stored communications warrant (Chapter 3 of the Act); and

(e) access to the content of communications by way of interception warrant (Chapter 2 of the Act) which warrants may pertain to a particular service or person.

8 In addition to these existing powers of access, the Associations have been engaged in an ongoing dialogue with relevant federal government departments over the past five years regarding their views on the establishment of a legislated data retention regime for Australian carriers and ISPs (collectively carriage service providers or CSPs). As a result of this dialogue the Associations have made a number of submissions on the introduction of a legislated data retention regime which have included comments on matters related to privacy as well as other issues such as a demonstrable need for such a regime, cost and cost allocation of such regime, data sets, who carries the obligation for retention of stipulated data sets, security of data retained, access to data retained, application of such a regime to off-shore application providers, impacts of anonymising technologies

including encryption on the usefulness of retained data and volume of data concerns to name just a few.

9 Further by way of background it is noted that in these previous discussions there has been a focus by some members on the difference between a data retention regime and a data preservation regime with a view to making known a preference for the latter. To explain what is meant by these terms in this context:

- **Data "retention"** – is the collection of all data of specified types traversing a telecommunications network. Typically, only a selected set of data is "retained" by CSPs for billing or related business needs, and then only held for a brief period. When mandated by law enforcement, such retention occurs regardless of sender/recipient or investigative purpose, for eventual review by authorities as the need arises. Mandatory retention proposals can vary according to the length of time for which data will be retained and whether the data retained will include just "traffic" information (sender/recipient, header or subject line and file size) or communication content as well. The line between what is or is not the retained "content" of a communication is frequently blurred.

- **Data "preservation"** – very much resembles the traditional intercept with a set duration: preservation occurs where authorities request a communications service provider by warrant or court order to retain all communications but only for a specific individual or set of individuals and for a finite period specified in the order. Preservation requests can often be supplemented by data that has been retained by the service provider as part of its legitimate business needs, but unlike mandatory data retention, LEAs do not 'require a business case' under a preservation regime.

10 With regard to the above explanations it can be seen that the impacts on privacy are minimised in a meaningful way under data preservation as such a regime only applies to and affects citizens who are implicated in or connected with an LEA investigation whereas the retention regime affects every user of a telecommunications service in Australia irrespective of their circumstances or on the basis of a possible future LEA perceived need.

11 There are three key threshold questions to determining the appropriateness of any new mandate for a legislated data retention regime:

1. what information do authorities hope to retrieve, and what is the need for it?
2. what authority or process is necessary to enable CSPs to provide data pursuant to a lawful request?
3. what is the impact of the measure on both individual rights and the economic viability of the service. And, how does this impact balance against the need for the information and the potential for its successful retrieval whilst addressing the legitimate expectations of security in the Australian landscape?

12 As discussed above, CSPs have a strong track record of working closely with LEAs under current national statutory arrangements. This cooperation often includes real time interception of communications and access to retained traffic data that is routinely collected for legitimate business purposes. Thus, the first key question above has been fulfilled by the existing track record of telecommunications and ISP industry assistance to law enforcement on retention requests.

13 Only data preservation offers a proven track-record of support to LEA needs without an excessive impact on privacy and industry competitiveness. It is for this reason that data preservation is the preferred method of the Associations for investigative cooperation, and as a less intrusive and less costly alternative to data retention. It also has the advantage of being currently available under the

provisions of the prospective data authorisations which if not sufficient in their current form could certainly be amended to address whatever gaps exist between currently available measures and a demonstrated need which is balanced against the legitimate privacy and security expectations of telecommunications users in Australia.

14 For the purposes of this response to the Inquiry, the Associations now focus on – without limiting themselves exclusively to – matters relating to the protection of privacy of telecommunications in light of the potential introduction of a legislated data retention regime.

15 The current proposed regime by the Attorney-General's Department is subject to strict confidentiality and as such the Associations are not at liberty to direct comment on that regime in such a way as to disclose the substance of draft proposals we have seen. However, given the existence of the Inquiry, it is appropriate to make some general observations about the tensions inherent in any regime that by its nature may include the capture, storage and retrieval of population wide telecommunications transaction data. For discussion purposes this submission will make its comments on the basis of a scenario of regulation were the provisions of the European Union (EU) Directive on data retention, DIRECTIVE 2006/24/EC, ("the EU Directive") is mirrored in Australia.

EU Directive Requirements

16 Essentially the EU Directive requires the capture and storage (for a minimum period of time) of necessary specified data for both telephony and internet based services including the:

- tracing and identification of the source of a communication;
- the tracing and identification of the destination of a communication;
- identification of the date, time and duration of a communication;
- identification of the type of communication (fixed, Mobile, internet);
- identification of the communication device used; and
- the identification of the location of mobile communications equipment.

Proportionality of the Proposed Data Retention Regime

17 Generally speaking, any obligation placed by a state authority on an industry to capture and retain data of its customers beyond what is required for legitimate business purposes and compliance with relevant laws/regulations can and ought to be questioned as to whether it is an appropriate and a proportionate measure within a democratic society. This is because such an obligation can result in the state placing a de facto surveillance function on private entities in a democratic society that are not designed to carry out such functions.

18 The data required to be retained under the EU Directive as set out above includes data derived from both internet and voice based telecommunications. Whilst the obligations and concerns regarding the protection of privacy of data remains the same for each category, the Associations concede that there are certain types of data that are already retained by their members for legitimate business purposes for compliance with such things as taxation record keeping requirements and as

such raise no additional issues to those that exist today. The same, however cannot be said of internet and service usage data. It is within this area that the Associations maintain a very high degree of concern as to the viability and proportionality of the proposed regime in the context of the protection of privacy – not only in the sense of protecting what is retained from non-authorised disclosure but also in the threshold sense of protection of the right of each individual citizen to privacy of their communications.

19 Any harm to these fundamental privacy rights which are part of all democracies must be proportionate not only to the aims of the proposed retention regime, i.e. the protection of all Australians through the prevention and prosecution of crime, but also to the ability and likelihood of the proposed regime to achieve this aim. It is thus required to determine how useful the proposed capture and retention of the stipulated data will actually be, and what harmful effects it will actually have. It is equally important to consider whether such an aim could not be achieved by other, less harmful means such as via a data preservation regime.

20 The Associations are concerned that this test of proportionality has not been performed sufficiently in the previous debates. Broadly speaking the test boils down to an assessment of the costs of the regime, i.e. social costs such as lack of privacy and potential abuse of retained data as well as monetary costs of implementation of a retention solution that have to be borne by either the tax payer in general or the consumers of telecommunication services via an increase in prices for those services, and the benefits of the proposed regime, i.e. how useful is the capture and storage of customer data to prevent and prosecute crime. The Associations contend that there is no clear evidence that the costs are outweighed by any additional benefits a legislated data retention regime (based on the EU Directive) may bring and, moreover, it is the Associations' strong view that the onus is on the government as the moving party of the regime to demonstrate that the test is satisfied given that this regime impacts on every user of telecommunications in Australia. The relevant government authorities so far involved in the proposal have failed to address this test of proportionality, especially with regards to providing evidence to the effectiveness of such a retention regime over and above mechanisms that exist today and the impact on an individual's privacy.

21 On the question of the need for such a regime we understand one of the concerns of the advocates of the regime is that data as is currently available today may not continue to be available in the future. The Associations submit that this is a natural evolution resulting from significant advances in technology and competitive business models leading to the delivery of not only completely new services and applications but also of existing services in new and innovative ways which results in changes to the types of data that are created, captured and retained for legitimate business purposes by CSPs. Therefore this statement whilst true does not necessarily address the test at all – it simply highlights a self-evident truth in that different telecommunications services and products produce different records. Similarly, different business or competitive needs produce different requirements in respect of data to be retained. However it will not stop legitimate business purposes leading to the retention of a variety of information. Data will continue to be retained and be accessible by LEAs via all the currently available lawful methods. If the de facto result of any mandated regime is that the industry needs to capture and store data about a citizens telecommunications in a manner to purpose fit law enforcement needs then such a regime implies a surveillance function performed by private organisations on lawful citizens' activities. Hence, the stakes are raised and the test to satisfy the balance of cost and benefit becomes more difficult to satisfy.

22 When considering the balance between security and privacy, the Associations submit the current context must be kept in view which is that information retained by CSPs is minimised to the maximum extent possible having regard to the

legitimate privacy expectations of customers, the current state of privacy laws in Australia, legitimate business needs and the consent of the customer.

Large Social Costs – Intrusion into Privacy and Lack of Data Security

23 The potential monetary and social costs to society are reasonably easy to identify but difficult to quantify. It is known from the experiences of other jurisdictions around the world that the monetary cost in terms of data capture, storage and retrieval is considerable regardless of the nature of the regime however without specificity of requirements it is difficult to capture the exact magnitude of the costs. Ultimately, the tax payer or end-user of a service subject to the requirement will incur that cost. (The Associations have commented on the monetary costs in previous submissions.)

24 The social costs in terms of the impact on individual rights are arguably just as significant. The proposed data retention regime will mean levels of surveillance and intrusion into a consumer's privacy of a magnitude that have never been seen before in Australia.

25 The intrusion into privacy is particularly pronounced where it relates to the capture and storage of internet browsing sessions (i.e. to trace and identify the destination of a communication) as the logging of these sessions blurs the line between mere traffic data storage and the capture of information that may reveal the content of a communication, e.g. it is quite obvious that web pages like www.ivf.com.au or www.aidshep.org.au relate to fertility and aids or hepatitis issues respectively.

26 However, as experts argue even the collection of pure traffic data does not constitute a lesser intrusion into privacy: "Contrary to popular opinion, access to traffic data cannot be considered less privacy invasive than the surveillance of the content of telecommunications. The information value and usability of traffic data is extremely high and at least equals that of telecommunications content. First, traffic data can be processed much more effectively than content data. Traffic data can be analysed automatically, combined with other data, searched for specific patterns, and sorted according to certain criteria *[although with some difficulty as stated below; NB this comment is added by the Associations]*, all of which cannot be done with content data. An interest purely in the contents of telecommunications does not occur in practice. Traffic data provides a detailed picture of the telecommunications, social environment, and movements of individuals. The information value of traffic data can, depending on the circumstances, be equal to or exceed that of communications contents. It can therefore not be said that traffic data is typically less sensitive than content data, and it is not justified to apply a lower level of legal protection to traffic data than to content data." [1]

27 Apart from the intrusion into privacy that occurs through the storage of traffic data as such, when analysing potential costs to society from extensive data retention regimes, consideration has to be given to "who will have control over" these vast amounts of private data and their protection from abuse. Hence, the additional risk to security and privacy are factors of social cost that must be considered. The retained data itself can become a target for inappropriate and unauthorised access by and of unlawful means. It would appear that the smaller the amount of customer data stored by service providers the better in terms of privacy protection and, thus, social costs. This is the current premise of privacy laws in Australia.

28 The current regulatory regime allows various parties to lawfully access information held by CSPs. Under the EU Directive in most Member States, access is limited to

[1] pp. 370-371, Patrick Breyer, *"Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR",* European Law Journal, Vol. 11, No. 3, May 2005

situations involving serious crime or requires a court order. Under the current Australian landscape as set out in Para 6 a wide range of agencies and even professional associations can lawfully access the data beyond strict law enforcement and national security agencies. In addition many other bodies have their own pieces of governing legislation that provide them with powers of access to retained data (such as ATO, Fair Trade, ASIC, professional associations etc). This raises the question of whether all these same parties would be granted access to the expanded data sets established under any formal data retention regime or whether access to extended data sets would only be available for investigation of serious offences, national security or child protection.

29 In this context, consideration must be given to the potential interaction of this proposed regime and existing legislation and laws that enable third parties with access to data by way of subpoena, search warrant and any other lawful request process. The result of this regime is that there will be more intrusive customer data than ever before retained by the telecommunications industry.

30 The Associations contend that this is part of the clear policies and safeguards that must be implemented as part of any legislated regime in order to identify legitimate levels of access to retained data, and must be complemented by the identification of appropriate processes and oversight to ensure that the policies and safeguards are applied consistently and with appropriate controls including authorisation, authentication and audit trails. Relevant Australian and international standards may require extensive measures to be introduced and or adjustment to ensure that what is accessible by lawful LEA requests is not also accessible to non-authorised parties not responsible for investigating and prosecuting serious offences, breaches of national security or child exploitation.

31 Again the Associations emphasise that in the context of the EU Directive the number of organisations and their level in state hierarchy that would gain access to the stored data under the proposed Australian regime seems to be significantly larger than in the European context. The number and nature of organisations having access or being able to request access to the data is, amongst others, a function of the definition of the purpose for which the data is made accessible.

32 The Associations submit that under the proposed retention regime, rights of access to retained data are broadly defined as being for all matters relating to crime, protection of public revenue or in fact in relation to any offence that has a pecuniary penalty. It is noted that the EU limits access to retained data primarily for purposes of investigations related to serious crime and often with judicial oversight.

33 As the ruling by the German Constitutional Court on this issue demonstrates, the Associations' concerns are shared by other jurisdictions which are further advanced in the law making process on data retention. The Court ruled in March 2010 that the German Law on Data Retention in its current form, i.e. past transposition of the EU Directive, is unconstitutional as the provisions of the law "guarantee neither adequate data security nor an adequate restriction of the purposes of use of the data. Nor do they in every respect satisfy the constitutional requirements of transparency and legal protection."[2] In its ruling the Court took into account that the general basis of data capture, i.e. the capture and storage without occasion and by way of precaution (blanket data retention), requires a special duty of care and security.

34 On the background of the discussion of the purpose of use, it should also be understood that the value of information will change over time. The Associations are very concerned that data retention of the kind envisaged will be attractive to others outside the law enforcement and national security communities, e.g. the

[2] See http://www.bverfg.de/pressemitteilungen/bvg10-011en.html

music and film industries are lobbying the European Parliament and national legislators to extend the (so far limited) scope of access to retained data provided for by EU Directive and national law to assist those industries in the prosecution of illegal downloading. This obviously signals the potential for retained data to be applied to purposes beyond the scope of the original policy justification.

35 The Associations point to the practical/financial implications of extended capture and retention requirements that derive from the obligations of the Privacy Act. The current Privacy Act requires that holders of personal information supply details upon request to individuals. Extended storage of customer service and usage data and increased retention times will increase the amount of information that must be supplied to individuals – in an intelligible form – and thus the cost to consumer's in accessing their data and to industry in complying with the Privacy Act.

36 The Associations require that the proposed regime contain a caveat which expands upon the current concept of immunity to incorporate "acting in good faith", and further, provide immunity and exceptions to reporting obligations under the Privacy Act.

Questionable Benefits of Extended Data Retention Requirements

37 With respect to the effectiveness of capturing and retaining usage data in preventing crime, the Associations submit that "Traffic data retention can, in principle, be useful in preventing infringements on any right. As far as cyber-crime (i.e. crime committed by means of telecommunications networks) is concerned, however, it is mostly the monetary interests of individuals that are affected. Cyber-crime hardly ever poses a threat to society as a whole, or to the physical safety of individuals. The benefit of retaining traffic data lies mostly in the investigation of criminal acts committed in the past, whereas its effectiveness in preventing damage is marginal. An analysis of relevant empirical studies shows that strengthening law enforcement does not have any apparent effect on the decision-making process of potential offenders. The investigation and prosecution of crime has preventive effects only insofar as prison sentences prevent offenders from committing offences out of prison during their prison term, and where proceedings result in the restoration or compensation of damage suffered by victims of crime. It is not known how many cases traffic data retention would be of use in, in this regard. However, what is clear from general practical experience is that strengthening law enforcement does not have any apparent effect on crime levels. The existence of various ways of communicating anonymously, the use of which is likely to increase as a reaction to traffic data retention, raises fundamental doubts as to the benefit of data retention. There are a range of methods for preventing either the generation of "readable" traffic data or access to it by [European] authorities. For example, it is easy for criminal offenders to use mobile-phone cards that have been registered in the name of another person or even legitimately purchased in a country that does not require registration. Only if the world community cooperated closely would it be possible to prevent anonymous telecommunication from taking place. Realistically, however, such cooperation is not to be expected. In any case, criminal offenders cannot be expected to observe laws banning the use of anonymous telecommunications. Therefore, traffic data retention cannot stop more experienced criminals from preventing the generation of incriminating traffic data. In summary, data retention can be expected to support the protection of individual rights only in a few, and generally less important, cases. A permanent, negative effect on crime levels, even in the field of cyber-crime, is not to be expected. The potential use of data retention in fighting organised crime including cyber-crime, child exploitation and in

preventing terrorist attacks is marginal or non-existent."[3]

38 One might hence well ask what is to be gained by subjecting the whole law abiding population to unprecedented levels of continuous surveillance or tracking as this would be the outcome of a data retention regime. Indeed, the Associations can think of no surer way to accelerate the use of invasion and evasion technologies by criminals and terrorists than to subject the entire population to these measures. The use of encryption, anonymising technologies and VPNs (and sometimes simply in the quest for privacy as opposed to for any nefarious purpose such as identity theft) by these criminal or terrorist elements also renders much internet traffic data useless for the purposes of criminal investigations.

39 Furthermore, it is not clear how LEAs might benefit or even be capable of analysing the massive volumes of data subject to retention – arguably without a concomitant increase in technical, analytical and interpretive capability and human resources. Increasing the volume of data to the extent envisaged by a data regime could actually impact adversely on finding that information which is actually relevant to an investigation. To highlight this issue, the Associations point to a recent report by the renowned consulting company Frost & Sullivan who estimate that the number of records to be retained by a large telecommunication provider under such a data retention regime would amount to more than one billion records per day.[4]

Conclusion

40 Proportionality between interests of all stakeholders (industry, law enforcement and the general public) requires justification from law enforcement agencies for mandatory increases in the capture and storage of customer data, and ongoing consultation with relevant stakeholders. The proposed data retention regime needs to first establish that the requirement is based on a demonstrated need for such a mechanism relative to the data retention capabilities and outcomes that are currently available and relative to other viable options. It is the Associations' belief that greater rigor, above and beyond the justifications proposed to this point, is required in establishing a need for such a regime. In particular there appears to be no assessment of the relationship of the benefits of the regime when compared with the total social and monetary costs.

41 The Associations consider the requirement for this measure to be disproportionate to the law enforcement objectives it purports to achieve.

42 The Associations remain willing to work with the Government in achieving an alternative approach to reasonable assistance of LEAs which delivers outcomes without the perceptual difficulties, social costs, increased risks to personal privacy and the technical complexity inherent within the service usage elements of the proposal.

[3] pp. 369-370, Patrick Breyer, *"Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR",* European Law Journal, Vol. 11, No. 3, May 2005

[4] p. 7, Frost & Sullivan, *"The Challenges of Data Retention: Now and in the Future",* 2010