The Secretary
Joint Select Committee on Cyber-Safety
R1-109 Parliament House
PO Box 6021
Canberra ACT 2600

Inquiry into Cybercrime Legislation Amendment Bill

This submission responds to your invitation of 8 July 2011 to comment on the *Cybercrime Legislation Amendment Bill 2011* (Cth), hereafter the *Bill*.

Overall the *Bill* is a positive and progressive response to challenges facing Australian law enforcement agencies, communication service providers and data custodians/owners in a global digital environment. Although aspects of the Bill are highly commendable and for example potentially reinforce the Australian human rights and commercial regime through the protection of data there are elements in the proposed legislation that raise concerns.

Those concerns are of sufficient gravity for the Bill to be amended and, it is respectfully suggested, for the Joint Select Committee on Cyber-Safety on behalf of the Australian community to articulate expectations about how the legislation will be implemented. Merely because something is convenient for a law enforcement or national security officer does not mean that it is necessary, viable or desirable.

Basis of the Submission

This Submission is made by Bruce Arnold and Skye Masters.

It is made on an individual basis rather than on behalf of the University of Canberra.

Mr Arnold is a lecturer in the Law Faculty at the University of Canberra, where he teaches Intellectual Property Law, Information Law, Competition & Consumer Law and Contract Law. He is the General Editor of *Privacy Law Bulletin*, Australia's leading privacy law journal, and has written the introductory chapters in the new LexisNexis Butterworths legal practitioner guide regarding data protection and privacy (in press).

His writing on telecommunication regulation, cybercrime, privacy and other matters has been widely cited in academic and other works, including leading law journals, government publications, the *Australian Financial Review* and the *Wall Street Journal*. He has been a member of advisory and policymaking committees of the Internet Industry Association, auDA (the Australian domain name regulator) and ISOC-AU (the Australian branch of the Internet Society). He has advised Australian internet service providers and consulted to bodies such as the Department of Foreign Affairs & Trade. As an official in the former Australian Department of Communications, Information Technology & the Arts he provided reports to the Online Ministers Council and Cultural Ministers Council, and was involved in discussions with telecommunication service providers about interception and data retention frameworks.

He has no commercial or other involvements that would be reasonably construed as a conflict of interest regarding this submission.

Ms Masters is a research assistant in the Law Faculty at the University of Canberra.

Recent and forthcoming publications include articles on data retention in relation to the Council of Europe Convention, the High Court's decision in *Hogan v Hinch* and questions of jurisdiction in relation to internet-based data profiling.

She has no commercial or other involvements that would be reasonably construed as a

conflict of interest regarding this submission.

The authors of this submission are thus equipped to provide an informed assessment of the proposed legislation from a legal, administrative and technical perspective.

An assessment of the Bill

As indicated above, aspects of the *Bill* (notably the emphasis on a technologically neutral regime for data protection that extends beyond Australian government networks and devices) are commendable.

Overall the *Bill* is a forward-looking and and sensible proposal that addresses Australia's relationships with other nations and the practicalities of law enforcement and national security activity in a world where digital technologies have facilitated offences that may be restricted to a single jurisdiction or may instead occur across borders.

Some elements of the *Bill* however raise concerns. We submit that it is both desirable and possible for the Committee to address those concerns through a statement of principle and through suggestions for modification of the *Bill*. Enhancement of the proposed legislation will reinforce the legitimacy of the Bill and of the agencies that seek to use the legislation.

That reinforcement is important given disquiet among the legal community and the Australian community at large about –

- large-scale interception/retention of electronic communications;[1] and
- potential misuse of Australian law by national security and law enforcement personnel in countries where there is less respect for process, less accountability and indeed less commitment to justice than in Australia.

(Concerns regarding misuse regrettably have a substantive basis, given criticisms by overseas courts and legislatures of the behaviour of their police and other officials or the constitutionality of national statutes that implement the Council of Europe *Cybercrime Convention*).[2]

A targeted approach

We strongly endorse the Bill's reliance on a targeted approach to data interception and retention, ie in implementing the Convention –

- Australian law enforcement personnel will be required to make requests that are specific to a particular individual;
- those requests will be effective for a short period;
- there is independent oversight of the requests by, for example, the Inspector-General of Intelligence & Security;
- Australian telecommunication service providers will not be required to provide law enforcement personnel with comprehensive access to all data of all customers on a long or short-term basis.

The Government has not made a persuasive case about the need for (and practicality of) retention of traffic records and communication content of all service provider customers in the long or short term. It is neither administratively nor commercially feasible for the Government to require telecommunication service providers to preserve and provide copies of the traffic

[1] The Committee's attention is drawn to submissions – well-founded or otherwise - by the Australian Privacy Foundation, Law Institute of Victoria, Victorian Privacy Commissioner, Pirate Party, Electronic Frontiers Australia and others that are noted in the recent Senate Committee report on *The Adequacy of Protections for the Privacy of Australians Online*.

[2] The Committee's attention is drawn for example to the German Federal Constitutional Court, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (Judgment of 2 March 2010), English text accessible as Press release no. 11/2010 of 2 March 2010 at http://www.bverfg.de/pressemitteilungen/bvg10-011en.html

data and communication content of all customers on an ongoing basis. A 'blank cheque' approach is not required by the Convention. The proposed statute complements but should not be expected to replace existing legislation.

We suggest that the Committee notes the fundamental undesirability of regulatory creep, ie warns that acceptance of targeted access to data about specific people should not be the basis for future extension of the legislation to require retention of data about *all* customers. A basis of the Australian justice system is that although investigation of people is necessary for the purposes of law enforcement and national security that investigation must always be bounded by law and must be on an exception basis rather than encompassing *all* members of the population or all members of ethno-religious and other minority groups.

The recent Senate Committee report on *The Adequacy of Protections for the Privacy of Australians Online* noted that inadequate information about the Government's data retention proposal has "resulted in confusion, mistrust and fear" and there are "very real possibilities" that the data retention regime is:

> unnecessary, will not provide sufficient benefit to law enforcement agencies, and is disproportionate to the end sought to be achieved. … The fact is that much of the information intended to form part of the scheme does not need to be collected for any other purpose, so the only reason to retain it is the mere possibility that it may prove useful to law enforcement. This seems to the committee to be a significant departure from the core principles underpinning Australia's privacy regulation.[3]

The Law Institute of Victoria had earlier noted concerns regarding both data retention and the way the proposal was being developed by the Attorney-General's Department. It recognised that comprehensive data retention by ISPs is "inconsistent with and represents a significant departure from the National Privacy Principles" and would "in reality be unworkable for law enforcement agencies", which should more appropriately rely on current procedures for the issuing of warrants. It argued that:

> The data retention proposal is inconsistent with the ALRC's recommendation that data be collected only where "necessary". The LIV considers that it is not "necessary" for the enforcement of laws that all internet and email usage be logged and retained. It might be helpful for law enforcement agencies to access such information; however it is not necessary … the internet and email usage of a person suspected of committing crimes can be obtained under current legislation, particularly through the issuing of warrants.
>
> The large-scale collection of information by governments because it *may* be helpful to some government functions, rather than because it is necessary, constitutes a serious threat to online privacy. The power of the internet should not be used by governments to achieve measures of control that would not be possible without the internet. By way of illustration, the LIV suggests that neither government nor community would tolerate proposals to place telephone intercepts on all phone lines in Australia and record all conversations, or to open all mail, in case such information may be of use to law enforcement agencies. Such proposals would be unacceptable in a democratic society. There is no demonstrable reason why internet communications should be treated differently to other communications.[4]

Cost

Compliance by telecommunication service providers with data access and preservation requirements imposes costs on those providers. The scale of those costs has not been

---

[3] Senate Environment & Communications References Committee, *The Adequacy of Protections for the Privacy of Australians Online* (April 2011), p68.

[4] Law Institute of Victoria submission to Senate Committee inquiry into *The Adequacy of Protections for the Privacy of Australians Online* (nd), p2.

publicly indicated by the Attorney-General's Department in for example its very brief discussion paper released in February this year.[5]

Over the past decade industry and independent observers have expressed concerns regarding administrative and infrastructure costs associated with responses to requests by law enforcement agencies, particularly in instances where agencies have unrealistic assumptions about the delivery of information in particular formats.[6]

The Bill's emphasis on cost-neutrality (with providers not facing unrecouped costs or gaining a profit) is commendable and we endorse the amendment of section 313 of the *Telecommunications Act 1997* (Cth).

Supervision

Accountability is a precondition for any endorsement of the proposed regime.

Item 33 modifies the reporting requirements in the *Telecommunications (Interception and Access) Act 1979* (Cth), the TIA Act. We suggest that reporting on foreign preservation notices and revocations be broken down by jurisdiction. This will provide observers with some sense of how the notices are being used or abused but will not provide sufficient detail to aid offenders or suspected offenders in subversion of legitimate law enforcement and national security activity.

Foreign jurisdiction by jurisdiction itemisation does impose a cost on the Australian Federal Police and associated entities. That cost is, however, trivial. It is an appropriate cost given recognition that "reporting obligations are an important element of the oversight regime contained in the TIA Act". Reporting is for accountability rather than something that is undertaken for its own sake.

As a corollary we suggest that the amended section 185 of the TIA Act require retention by the enforcement agency of notices for a period of ten rather than three years. Again, there is a cost for the enforcement agency but the case is low and acceptable.

The longer retention of notices addresses potential concerns that notices are being misused or are inappropriate (concerns that may not be identifiable in the short term). It reminds law enforcement personnel that surveillance takes place within a justice framework and that application for and implementation of notices should not take place on a 'tick and flick' basis.

The history of official surveillance in Australia and other liberal democratic states suggests that routinisation and convenience are dangers: officials, often with the best of intentions, come to take exceptional measures for granted. A longer period of retention of notices (notices, rather than the data covered by those notices) serves to reinforce a recognition that accessing the communication of alleged offenders is special and is not to be undertaken lightly merely because the request originates overseas.

Authorisation

Consistent with concerns regarding regulatory creep and routinisation we suggest that Issuing Authority should be more restricted than that identified in section 6DB of the TIA Act.

The Act provides for authorisation by a judge, federal magistrate, a magistrate or member of the Administrative Appeals Tribunal (AAT). The inclusion of a non-Commonwealth magistrate and of AAT members is not necessary. It is inappropriate. Authorisation is a serious matter. It

[5] The paucity of information in that document is particularly disappointing and reflects a lost opportunity to address community concerns regarding accession the *Convention*.

[6] It was once necessary for an author of this submission to explain to an Australian Federal Police representative that providing the requested "printout" of all SMS or email traffic of all Telstra and Optus customers would require more semi-trailers than could be comfortably parked outside the AFP headquarters.

relies on trust in foreign police systems, a trust which has been recurrently placed in question by official investigations and negative judicial judgments within those jurisdictions. (Put simply, overseas courts, tribunals and legislatures on occasion have been highly critical of the competence or bias of their investigators and decision-makers).

One response might be that Australian judges, for example those in the Australian Capital Territory, are overloaded with work and that spreading the load through inclusion of AAT members is accordingly appropriate. We contend that from a justice perspective it is more effective to appoint and properly support additional judges. The Committee should be wary about the 'convenience' ethos that spreads responsibility to junior personnel whose appreciation of justice issues – highlighted in subsections 116(2) and 116(2A) – is less than those of their judicial peers.

Application

In relation to the new section 142A we note that although the restrictions may be effective within Australia they are open to abuse by overseas agencies. Governments seeking assistance from Australia will presumably articulate their requests broadly. Australian authorities under the legislation are bound not to misuse information gained through overseas requests but have no control of what foreign agencies see the information and what those agencies do with the information.

The nature of the law enforcement and national security challenges addressed by the *Convention* (and by the *Bill*) mean that the sharing of information with overseas entities is desirable and on occasion may indeed be imperative. It should not however be undertaken lightly. We suggest that the Committee in reporting on the *Bill* should explicitly emphasise that there are uncertainties and scope for abuse that cannot be redressed in Australia. Those concerns should be reflected in the reporting highlighted above and in careful scrutiny by the Attorney-General, Ombudsman and Inspector-General of Intelligence & Security regarding day by day implementation of the *Convention*.

The preceding comment does not mean that the authors of this submission are necessarily dismissive of the justice systems of *Convention* states; merely that the *Convention* regime relies on trust in the good faith and efficiency of Australia's partners in the *Convention* because Australian law will not extend to what happens once information goes offshore and will not provide redress if there is abuse.

Data Protection

The proposed amendment of data protection provisions in the *Criminal Code Act 1995* (Cth) is strongly supported as strengthening the protection of human rights, public administration and commerce within Australia.

Australian law regarding data protection is uneven and on occasion idiosyncratic, resulting in uncertainty, disagreement and potential escape from what would be an offence in other circumstances. As noted in the Explanatory Memorandum the inadequacy of Commonwealth, State and Territory law – specifically in relation to the *Convention* and more generally – is evident and non-trivial. That inadequacy has been reflected in reports by the Australian Law Reform Commission, the Australian Privacy Commissioner and other bodies.

The proposed amendment of sections 477.1, 477.2, 477.3, 478.1 and 478.2 is important, welcome and practical. In particular it recognises concerns within the legal and information technology communities regarding unauthorised access to, modification of or destruction of data that –

- is not held on an Australian government information network or device;
- does not involve a carriage service;
- is not 'restricted' information.

The adoption of a ‘network neutral’ approach that is not predicted on mishandling of official data is a major step forward in an environment where the national Government has yet to establish a statutory tort regarding breach of privacy and where private sector entities are experiencing difficulty with data loss, modification or destruction. Data offences do not respect institutional boundaries and the impact on individual lives (or the national economy) of offences in the private sector may be as significant as those involving government data.

More Information

The authors would be pleased to expand on comments in this document through a supplementary submission or through testimony in a committee hearing.

Bruce Arnold
24 July 2011

Skye Masters
24 July 2011