Australian Privacy Foundation

post: GPO Box 1196
Sydney NSW 2001
phone: +61 2 9231 4949
facsimile: +61 2 9262 3553
email: mail@privacy.org.au
web: www.privacy.org.au

The Secretary
Parliamentary Joint Committee on the Australian Crime Commission
Suite S1 107
Parliament House
Canberra ACT 2600

29 August 2003

Dear Ms Weeks

Cybercrime Inquiry

I refer to our letter of 29 April, in which we requested the opportunity to make a submission once we saw what proposals were being made by government agencies and others. We note that a number of submissions have now been made and hearings held. Due to overseas absences we have only just been able to compile this submission and hope that the Committee may still be able to take it into account

While we have not had the resources to look at all this material, we do have some key concerns that we would now like to bring to the Committee attention. Overall we endorse the submissions of Electronic Frontiers Australia and the NSW Council for Civil Liberties. We note that there is not yet a submission from the federal Privacy Commissioner on your Web site, and would hope that the Committee has actively sought the Commissioner input

We would be particularly concerned at any proposals to increase the level of routine monitoring of individuals transactions, whether it be on the Internet or in other systems such

as banking, and any related proposals to mandate the retention of transaction records for any longer than commercial considerations require.

We suggest that all the evidence points to the inability of law enforcement agencies to process the vast amount of information they already receive. Rather than seeking to increase the volume of information — with its major implications for individuals' privacy and freedoms, we suggest that the emphasis should instead be on agencies working 'smarter' and in a more integrated way to investigate well founded suspicions of wrongdoing. The need is not to generate more suspicions — often based on matching and profiling programs of dubious integrity, but rather to investigate existing intelligence — with an emphasis on human intelligence and analysis rather than inherently unsound automate programs.

We are alarmed that the Attorney-General's Department, in its submission, pays only lip service to privacy in a brief factual statement of privacy law. We would suggest that as the policy department responsible for privacy protection, AGs should be providing a more sophisticated treatment of the balance to be struck between the various public interests. We further suggest that their failure to do so highlights, not for the first time, the anomalous co-location of privacy and other human rights policy responsibilities within a Department that is predominantly, and increasingly, concerned with law enforcement and security interests. We hope that the Privacy Commissioner will to some extent remedy this imbalance, but would also request the Committee to consider recommending the re-location of privacy and human rights responsibilities to a more 'sympathetic' environment within the federal bureaucracy.

We note that several submissions make reference to the Internet Industry Association's draft Cybercrime Code of Practice. Despite promises since last year, this draft has only recently been exposed to consultation with 'civil society' interests and we are not surprised to find that the closed process of consultation with law enforcement interests only has led to a flawed and unbalanced Code. I will send our submission on the Code to the Committee when it is completed.

The same problem of inadequate consultation applies to many of the other initiatives detailed in the AGs Department submission, such as the *AUSTRAC Proof of Identity Steering Committee*; the *Action Group into the Law Enforcement Implications of Electronic Commerce (AGEC)*; the *Electronic Security Coordination Group (ESCG);* and the *Information Infrastructure Protection Group (IIPG)*. While there are clearly some operational discussions which would need to remain confidential for security reasons there is no good reason why the overall policy deliberations of such inter-departmental groups should not be more open.

Other initiatives which do involve business interests but have no consumer or civil society input are of even greater concern — in particular the *Business—Government Task Force on Critical Infrastructure* and its offshoot *Trusted Information Sharing Network for Critical Infrastructure Protection (TISN).* We understand that the Australian Bankers Association has expressed some concern about the possible use of the TISN to transfer personal information about bank customers and is seeking indemnity from any action for breach of confidence or of privacy laws. We can fully understand the need for better co-ordination and co-operation

on infrastructure protection, but any proposals for increased sharing of personal information raise completely separate issues and demand a wider public debate.

In this respect we strongly endorse the proposals by the Privacy Commissioner made to another current Inquiry (*Joint Parliamentary Committee of Public Accounts and Audit — Inquiry into the Management and Integrity of Electronic Information in the Commonwealth*) for Privacy Impact Assessments. We cal on your committee to endorse the Privacy CommissionerÕs call for more systematic use of Privacy Impact Assessments (PIAs). Many new government initiatives progress too far down the track of policy approval before serious privacy implications are recognized. Attempts to limit their impact or propose less threatening alternatives then have to battle entrenched bureaucratic and/or political interests. Requiring compliance with privacy principles, while essential, is not sufficient. The current law essentially only provides assurances of ÔgoodÕ housekeepingÕ once a decision has been made to collect and use personal information in a particular way. The Privacy Act does not currently require any detailed analysis of privacy impacts, or detailed justification of new intrusions or of new programs of matching or profiling using existing information.

All significant new government initiatives involving the use of personal information should be required to prepare and publish a privacy impact assessment at an early stage. Established models for such a requirement exist in Canada[1] and the United States[2], while the New Zealand Privacy Commissioner has issued useful PIA Guidelines[3].

Thank you

Nigel Waters
Board member
Australian Privacy Foundation

[1] See http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr1_e.asp
[2] E-Government Act of 2002 *Public Law 107-347*
[3] See see www.privacy.org.nz