Australian Privacy Foundation

p o s t: GPO Box 1196
Sydney NSW 2001

e m a i l: enquiries@privacy.org.au

w e b : www.privacy.org.au

30 November 2009

Submission to the Department of Prime Minister & Cabinet regarding Cross Border Data Transfers

Submission by the Australian Privacy Foundation

Supported by a range of privacy and consumer organisations and individual experts (See Appendix 1)

About the Australian Privacy Foundation

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. Since 1987, the Foundation has led the defence of the right of individuals to control their personal information and to be free of excessive intrusions. For information about the Foundation see www.privacy.org.au

Problems with the proposed UPP 11

As the Government is aware, the Australian Privacy Foundation is concerned that the Government's response to the proposed *UPP 11 Cross Border Data Transfers* provides inadequate protection for all Australians' personal information. This submission does not repeat all of the detailed arguments that have been presented to the Department of Prime Minister & Cabinet - instead it highlights some key concerns and seeks a specific Government response. We have also included a list of supporting privacy and consumer organisations and individual experts (See Appendix 1).

The proposed UPP 11 does not restrict the transfer of data offshore under any circumstances. Nor does it include any requirements for organisations to take steps to ensure that data is protected when it is transferred overseas. Indeed, the current wording of the proposed UPP 11 is such that it is impossible to breach UPP 11 itself.

The key specific concerns with the current wording are:

1. UPP 11 is not written as a *positive* principle. It does not contain any requirement for action, risk assessment or care by an organisation sending data offshore. It states that organisations "remain accountable" for information transferred offshore, but it then defines "accountable" so that it is limited to accountability only for breaches of privacy that occur. UPP 11 therefore only operates after the event - when it is too late for a consumer who has suffered a breach of their personal information

2. UPP 11 contains no restrictions at all on who the data can be sent to or where the data can be sent. Data could be sent to a known criminal in the most high risk jurisdiction without breaching UPP 11.

3. The exceptions in UPP 11 are not exceptions to a restriction on export. They are merely exceptions to accountability (which is itself limited to after the fact accountability for breaches).

4. One of the exceptions in UPP 11 is the subject of additional concern. Exception A exempts the organisation from accountability where they "reasonably believe" that the recipient of the information is subject to a law or binding scheme which effectively upholds privacy protections that are substantially similar to the UPPs. The term "reasonably believe" should be removed as it will act as a loophole that can be exploited by organisations to export data to risky jurisdictions that do not provide adequate protection (for example, destinations where data processing is less expensive). The reasonable belief test is a very low bar for an organisation, but a very high bar for an affected consumer to disprove.

The APF has outlined its concerns to the Department in some detail in recent email correspondence and at a telephone conference on 28 October 2009. APF members have also published a range of critiques of the proposed UPP 11 (both before and after the Government's response to the ALRC report), including:

Greenleaf (2009)
http://www.apo.org.au/commentary/rudd-government-abandons-border-security-privacy

Connolly (2008)
http://www.galexia.com/public/research/articles/research_articles-art54.html

Cyberspace Law and Policy Centre (2008)
http://www.cyberlawcentre.org/ipp/publications/CLPC%20Submission%20on%20UPPs%20final.pdf

There has been some recent discussion that UPP 11 can be improved by simply providing additional guidance and / or a more detailed definition of the term "accountable". However, the APF believes that the structure of UPP 11 is fundamentally flawed and we submit that the section must be remodelled, rather than relying on additional guidance.

We note that the effect of all of the other UPPs can be understood without reference to additional guidance and definitions.

Preferred approach for Cross Border Data Transfers

Privacy stakeholders want to see UPP 11 re-written as a positive requirement that requires organisations to take reasonable measures to ensure the privacy of information transferred offshore. This will mean that some transfers must not proceed because of the risk to data and the absence of protection. Further, it must be possible for a consumer to complain of a breach of UPP 11 itself.

Privacy stakeholders support an accountability approach only where it is combined with the above requirements. We can see some benefits for consumers in being able to make a local complaint about a breach that occurs offshore, but accountability for breaches is not a sufficient protection if applied as a stand-alone provision.

Next steps

The Australian Privacy Foundation seeks urgent clarification of the Government's position on UPP 11. Obviously, we wish to see the concerns raised in this letter (and raised in other critiques of UPP 11) addressed in the exposure draft of the proposed legislation. However, we also call on the Government to clarify its policy position regarding UPP 11 as a matter of urgency, by responding to this letter or making other appropriate public statements.

The APF is concerned that all of the privacy protections offered by the other UPPs will be meaningless if there is no protection for data once it is transferred offshore.

For further information contact:

Roger Clarke
Chair
E-mail: chair@privacy.org.au
APF Web site: http://www.privacy.org.au

APPENDIX - Supporting organisations and individual experts

Organisations

- Australian Communications Consumer Action Network (ACCAN)
- Australian Financial Counseling and Credit Reform Association (AFCCRA)
- Australian Privacy Foundation (APF)
- CHOICE
- Civil Liberties Australia
- Consumer Action Law Centre (CALC)
- Consumer Credit Law Centre NSW
- Consumers' Federation of Australia (CFA)
- Council of Social Services NSW
- Cyberspace Law and Policy Centre (UNSW)
- Electronic Frontiers Australia (EFA)
- Internet Society Australia (ISOC-AU)
- Liberty Victoria
- NSW Council for Civil Liberties
- Public Interest Advocacy Centre (PIAC)
- Welfare Rights Centre

Individual privacy, consumer and human rights experts

- Robin Banks, Chief Executive Officer, Public Interest Advocacy Centre
- Carolyn Bond, Chief Executive Officer, Consumer Action Law Centre
- Dr Julie Cameron , Board Member, Australian Privacy Foundation
- Chris Connolly, Director, Galexia and Board Member, Australian Privacy Foundation
- Dr Roger Clarke, Director Xamax, Visiting Professor UNSW, Visiting Professor in Computer Science, Australian National University and Board Member, Australian Privacy Foundation
- Dr Juanita Fernando, Lecturer, Faculty of Medicine, Nursing and Health Sciences, Monash University and Board Member, Australian Privacy Foundation

- Professor Graham Greenleaf, Law Faculty UNSW, Co-Director, Cyberspace Law and Policy Centre and Board Member, Australian Privacy Foundation
- Fiona Guthrie, Executive Director, Australian Financial Counselling and Credit Reform Association
- Nicola Howell , Lecturer, Law School, Queensland University of Technology
- Dr Usman Iqbal, School of Surveying and Spatial Information Systems, UNSW and Board Member, Australian Privacy Foundation
- Anna Johnson, Director, Salinger Privacy
- Katherine Lane, Principal Solicitor, CCLC NSW
- Catriona Lowe, Chair, Consumers' Federation of Australia
- Dr Katina Michael, Associate Professor, School of Information Systems and Technology at the University of Wollongong and Board Member, Australian Privacy Foundation
- Maree O'Halloran, Director, Welfare Rights Centre
- Holly Raiche, Executive Director, ISOC-AU
- Gordon Renouf, Director Policy and Campaigns, CHOICE
- Professor Supriya Singh, School of Accounting & Law, RMIT University
- Lindy Smith, Board Member, Australian Privacy Foundation
- Dr Dan Svantesson, Associate Professor at the Faculty of Law, Bond University and Board Member, Australian Privacy Foundation
- Gerard Thomas, Policy and Media Officer, Welfare Rights Centre
- Dr Holly Tootell, Senior Lecturer in the Faculty of Informatics, University of Wollongong and Board Member, Australian Privacy Foundation
- David Vaile, Executive Director, Cyberspace Law and Policy Centre (UNSW) and Board Member, Australian Privacy Foundation
- Nigel Waters, Board Member, Australian Privacy Foundation and Principal Researcher, Interpreting Privacy Principles Project, Cyberspace Law & Policy Centre, UNSW
- Matthew Watts, Board Member, Australian Privacy Foundation
- Jan Whitaker, Principal, JL Whitaker Associates and Board Member, Australian Privacy Foundation
- Stephen Wilson, Managing Director, Lockstep Group