# Comment on the Exposure Draft of Australian Privacy Principles

Submitted by the National Association for Information Destruction, Incorporated – Australasia Chapter

27 July 2010

**NAID-Australasia**
Level 31, RBS Tower @ Aurora Place
88 Phillip Street,
Sydney NSW 2000, Australia

## Introduction

The National Association for Information Destruction, Inc. - Australasia Chapter (NAID-Australasia) would like to thank the Australian Government for accepting and considering its comments on the Exposure Draft of the new Australian Privacy Principles issued on 24 June 2010.

Overall, the diligence, acumen and dedication of the authors has resulted in a set of guiding principles that will serve as a suitable and laudable litmus test to guide the creation of the remaining parts of a revised Privacy Act, which in turn will serve the citizens of Australia for the foreseeable future.

## About NAID and NAID-Australasia

The National Association for Information Destruction, Inc. (NAID) is the international trade association for commercial enterprises that offer information destruction services. While founded in United States in 1994, NAID has developed an international presence through the formation of strong chapters Canada, Europe and Australasia.

Presently, NAID has over 1,400 member locations around world and has developed a respected reputation for promoting high standards and ethics in an industry that serves a vital role in protecting personal information at its most vulnerable point – when it is discarded.

As a result, NAID has provided testimony by invitation at hearings of the US Senate Financial Services Committee hearings on data protection. NAID was also invited to provide testimony at hearings held by the Canadian House of Commons during that country's review of its preeminent privacy law; the Personal Information Protection and Electronic Document Act (PIPEDA). NAID also sits on the British Standards Institute's subcommittee responsible for developing practice standards for secure destruction services, which last year became a European Union Standard. Lastly, NAID worked closely, again by invitation, with the US Federal Trade Commission during the rulemaking phase of the Final Disposal Rule provision of the Fair and Accurate Credit Transaction Act (FACTA).

## Comments

As stated in the Introduction, the proposed Australian Privacy Principles are very well crafted. Drafters succeeded in achieving a balance between providing clear guidance while not being overly prescriptive. We commend the use of Reasonableness and Technological Neutrality to achieve this balance.

NAID will limit its comments to areas that fall within its specific area of expertise. In doing so, we also understand and appreciate that the issues we raise may be dealt with in the remaining parts of the new Privacy Act.

Specifically, we are recommending drafters consider adding language advising organisations to (a.) exercise due diligence in selecting data processing services and (b.) create written data security policies and procedures.

We further suggest that "Destruction" be defined within the "Definitions."

**Due Diligence in Selecting Data Processing Services**

Data Controllers have cause to outsource many data processing functions, as in the case of outsourcing secure destruction services. Under that same logic that would compel due diligence when sending Australian citizens' personal information outside of the country (Principle 8), the Privacy Principles would benefit from referencing the need for due diligence when selecting any third party processor.

Along that same line of thinking, the Privacy Principles might benefit by referencing a requirement to have a written contract with such third parties, linking said processor to same principles.

**Written Data Security Policies and Procedures**

While the Privacy Principles do call for written Privacy Policies (Principle 1), NAID-Australasia suggests that the guidelines should also advise organisations and agencies to have their data security policies and procedures documented in writing. This could be easily added to in Principle 11.

Most data protection laws have such a requirement because 1) having written policies and procedures is the only way to ensure employees and vendors are being given the proper direction, and 2) having such policies and procedures documented in writing is the only way any organisation can demonstrate that it comprehends and takes seriously their responsibilities to protect personal information. The alternative to having written data security polices and procedures

**Defining "Destruction"**

NAID-Australasia is gratified to see information destruction as the example used when describing reasonable security precautions (Principle 11). We appreciate that drafters understand that data disposal is one of the most often overlooked and misunderstood areas of information security.

Our last comment carries that point a bit further. Not only is destruction often overlooked, the entire concept of "destruction" is also often misunderstood. For instance, we have many examples of organizations and agencies relying on casual disposal or simple recycling as methods of destruction. Further, there are many who believe that hitting the "delete" button on a computer keyboard erases the information from the hard drive or that sending a computer to an electronic recycler provides destruction.

This is why we recommend providing a definition of "destruction within the Definitions section.

It is possible to define "destruction" while remaining technologically neutral, reasonable and non-prescriptive. One example defines "destruction" as "rendering the information on the media practicably unreadable, unretrievable or unreconstructable, and/or invokes procedures such as "shredding, incineration or erasure."

**Conclusion**

We will close as we opened, by thanking the Australian Government for the opportunity to provide our suggestions and by complimenting the drafters for their admirable efforts.

We come to this process understanding that we are influenced by the issues that affect our industry and expect reviewers to take that into consideration. Regardless of how our comments are evaluated or adopted, we feel the guidance provided within this the draft Australian Privacy Principles will serve the country's citizens and the regulatory process very well.

Respectfully submitted: 27 July 2010

Robert Johnson
Chief Executive Officer
NAID-Australasia