Privacy Commissioner
Te Mana Matapono Matatapu

Information Matching Bulletin

News from the Office of the Privacy Commissioner – March 2010

In this edition

Law Commission: Review of the Law of Privacy

In late 2006, the Law Commission started a project involving a four stage review of privacy law. Stage 1 involved a high level policy overview to assess privacy values in the face of changing technology, international trends, and their implications for New Zealand law.

Stage 2 looked at whether the law relating to public registers requires change as a result of privacy considerations and emerging technology. Stage 3 of the project looked at the adequacy of New Zealand's civil and criminal law remedies relating to invasions of privacy.

Stage 4 is a detailed review of the Privacy Act 1993. The issues paper for stage 4 is expected to be released soon (near the beginning of March) and the Law Commission would like to hear from organisations that have comments on the paper and proposals for reforms of privacy law. The issues paper will include a chapter on information matching which will put forward a number of proposals for amendments to the existing information matching provisions in the Privacy Act.

Information Matching Interest Group

The next Information Matching Interest Group meeting will be held on 23 March 2010. John Burrows and Ewan Morris from the Law Commission will be talking about their review of information matching, which forms part of their detailed review of the Privacy Act. For more information please contact colin.trotter@privacy.org.nz.

Information matching workshops

The half day workshops are designed to give some practical background knowledge about the Privacy Act along with more detailed information about preparing an Information Matching Privacy Impact Assessment.

The timing of the next workshop is dependent on having enough participants registered. To register interest in attending this workshop, contact Sharon Newton on (04) 4747590 or by email to sharon.newton@privacy.org.nz.

Data Transfer Security

The Privacy Commissioner's requirement that agencies use encryption for online data transfers in authorised information matching programmes has been in place for several years. In 2008, that requirement was extended to include transfers of physical digital media (for information matching programmes) following overseas reports of data loss and a review of agency practices in New Zealand.

My study of online transfer standards and practices found that overseas data protection authorities[1] do not generally have a prohibition on the use of online transfers, nor do they have equivalent powers in their legislation to mandate the use of encryption. However, most of the authorities which responded to me issue guidelines relating to information transfers, and suggest the use of encryption for high risk transmissions.

My search for legislation in other jurisdictions that regulate online communications found many examples where encryption was not mandated but was encouraged to be considered or recommended. A search for information about the New Zealand banking industry found that encryption on the transfer of financial transactions is the norm.

In the government sector, the NZ ICT Security Manual (NZSIT 402:2008) issued by the Government Communications Security Bureau (GCSB) is the most relevant, comprehensive and authoritative source of advice for NZ government agencies to follow for ICT matters. The NZSIT manual provides direction on security requirements using the information classifications of in-confidence, sensitive, and restricted.

The wall-chart guidelines for protection of official information can be downloaded from www.security.govt.nz. The wall chart offers criteria to assist in the classification of information based on the damage that would result from unauthorised disclosure, and specifies what protective measures ought to be applied to that information. Personal information most closely aligns with the in-confidence classification.

While electronic transfers across public networks like the internet must be encrypted for information classified as either restricted or sensitive, information classified as in-confidence does not have to be encrypted but must be assessed before transmitting.

The Privacy Commissioner's requirement that transfers of personal data used in information matching programmes be encrypted is in response to the significant risks of unauthorised disclosure of information about thousands of individuals.

There are likely to be other data transfers which involve the personal details of many thousands of individuals that fall outside of the information matching framework, and some of these may currently be unencrypted. This is a risk area that may need to be reassessed because of the increasing security risks of using the internet channel.

Colin Trotter

Publications

There are a number of other publications and reports available from the Privacy Commissioner that may be of interest to those involved in information matching. These are listed on the Privacy Commissioner's website, www.privacy.org.nz.

Contacts

Wellington
109-111 Featherston Street
gen-i Tower, 4th Floor
PO Box 10-094
Wellington, New Zealand
Telephone: 64-4-474 7590

Neil Sanson
Data Matching Compliance Adviser
Direct Line: 64-4-474 7592

[1] Responses received from the Netherlands, Sweden, United Kingdom, and Australia.

Rosie Byford
Team Leader, Policy and Technology
Direct Line: 64-4-494 7082

Colin Trotter
Senior Adviser, Data Matching Compliance
Direct Line: 64-4-494 7087

You can contact us by email. Our standard email format is first name.surname@privacy.org.nz