Privacy Commissioner
Te Mana Matapono Matatapu

Information Matching Bulletin

News from the Office of the Privacy Commissioner – June 2009

In this edition

Portable Storage Device Survey

The Office of the Privacy Commissioner recently completed a survey on the use of portable storage devices in the public sector. Portable Storage Devices (PSDs) include USB sticks, cell phones, iPods, PDAs (personal digital assistants), iPhones and netbooks.

The results of the survey were announced during Privacy Awareness Week (May 3 – 9) and are available on our website. The survey found that while many agencies already have some protections in place, there are some real gaps in procedure and practice that need to be addressed. We have provided feedback and recommendations to each agency surveyed and we will be issuing general guidelines shortly.

Early in 2008 the Privacy Commissioner announced that all information matching data being transferred on digital physical media were required to be protected by encryption.

Information Matching Interest Group

We would like to thank Inland Revenue for kindly hosting the meeting which took place on 19 March 2009. The meeting was very well attended with representatives coming from the Ministry of Social Development, Department of Labour, Ministry of Justice, Department of Corrections, Department of Internal Affairs, and Housing New Zealand.

Inland Revenue provided the main presentation at the meeting, explaining the development of the stakeholder management function within Inland Revenue and how they are addressing data sharing issues. We also heard from other agencies about their current development plans.

We are keen to receive suggestions about the topics/format of the next information matching interest group meeting (date to be advised). Think about a presentation you might present on behalf of your agency. Perhaps you have an information matching success story or cautionary tale to share? Please contact Neil or Colin with your ideas!

Shared Workspace discontinued

The Information Matching Shared Workspace which was launched in May 2007 has been discontinued. We have found that the workspace has not been sufficiently utilised to warrant the cost and work effort required to maintain its operation. The Office may look to develop some similar functionality on our own website in the future.

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. We are planning to do the next one in August.

To register interest in attending this workshop, contact Sharon Newton on (04) 4747590 or by email to sharon.newton@privacy.org.nz.

Achieving Privacy Through Security Measures

The Information Systems Control Journal, volume 2/2007 edition, featured an article by C. Warren Axelrod, Ph.D., CISM, CISSP, titled “Achieving Privacy Through Security Measures”.

C. Warren Axelrod suggests that applications are more often attacked than databases because the attacker does not generally need to have specialist knowledge of the infrastructure. Consequently Axelrod believes it is most important that application access controls are robust.

Identity and access management is unquestionably the most critical control for privacy and, in some ways, the most difficult and costly to implement, writes Axelrod. The ability to control access to information is becoming increasingly difficult as applications become more complex, with greater capabilities and interconnectivity among applications. Axelrod says that managing and controlling large amounts of activity is a heavy administrative overhead that can only be handled effectively, even in medium sized organisations, through sophisticated automation.

Legacy systems were never designed to provide the level of functionality needed to ensure compliance with today’s legal and regulatory requirements. Axelrod suggests that costly changes to legacy systems are needed to attain the necessary level of control and reporting, or they need to be replaced. In some cases a front-end system that manages many of the access functions can be developed, however Axelrod writes that this is still a considerable effort, and the applications must be amenable to such treatment. Given these warnings by Axelrod, it is essential that all proposals for new systems include strong access, control and reporting features.

Axelrod believes that encryption is largely oversold and overrated as a technique for protecting personal information. While data may be protected by encryption from direct attacks against the database, successful attacks are more likely through an application accessing the database.

Axelrod cites a higher risk of disclosure of personal information where attacks are directed at users, such as through key logging and phishing. Phishing and key logging are two examples where encryption of database information will not prevent an attack as access is gained through an access breach of the application. Axelrod states that blocking particular email attachments and other suspicious messages go a long way in reducing this risk.

Nevertheless, Axelrod says encryption can be of some value where the information is highly valuable or fits in the personal information category. It does make some types of attacks more difficult and it might deter the amateur completely, but might only slow down a more serious thief.

Axelrod concludes that [in the US] the cost of complying with new laws and regulations protecting information will be much greater than expected, but the imperative to stem the tide of data breaches will largely override these costs.

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

Rosie Byford
Team Leader, 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