Privacy and information security – is mandatory data breach notification the answer?

iappANZ breakfast seminar, 27 July 2011, Corrs Chambers Westgarth, Sydney

Theme: the policy and regulatory issues surrounding the information security aspects of privacy and whether introducing a mandatory breach notification model would enhance data protection.

Nigel Waters, Pacific Privacy Consulting (www.pacificprivacy.com.au), and Australian Privacy Foundation (www.privacy.org.au)

Mandatory data security breach notification (DSBN) is not *the* answer (there is no silver bullet!) but it could make an important contribution to increased privacy protection.

Justification for additional measures such as DSBN

- Greater awareness of breach incidence/severity (recent spate of reported breaches[1] Sony, Citigroup, RSA, and locally, Vodafone January 2011, Lush February 2011, Medvet SA drug laboratory July 2011)
- Greater risk of damage – ID crime more prevalent?
- Greater exposure due to aggregation (globalisation) – larger databases, dispersed storage (cloud) both more and less vulnerable
- Many other 'non-privacy' reasons for considering DSBN as a security measure

Why mandatory?

- Not generally in data controller's interests to notify or publicise breaches
- Usually only considered when breach already or about to be made public
- If voluntary likely to be only more responsible controllers that notify – worst offenders won't

Multiple objectives of DSBN:

- Putting affected individuals in a position where they can take appropriate action, including protective measures and seeking redress
- Raising awareness of privacy issues more generally amongst affected individuals (e.g. awareness of breaches should also generate interest in notice, choices, access rights etc)
- Ensuring data controllers suffering a breach do not escape attention and effects, including necessity for remedial action, liability for compensation, (and reputational damage, if publicised)
- General awareness raising (if publicised) amongst data controllers, and incentive for them to take precautions, including improved security

The extent to which a mandatory DSBN scheme will achieve these objectives will depend on:

- Coverage (exceptions?)
- Criteria for notification
- Recipients of notification – Regulator and/or affected individuals
- Sanctions – regulator powers
- Level of publicity

[1] Privacy Rights Clearinghouse (US NGO) reports 2,582 data breaches made public since 2005 (http://www.privacyrights.org/data-breach)

Overseas experience

- Limited reporting of actual experience
- DSBN is mandatory in most US States (since 2002 - 46 as at November 2010) National laws proposed
- Norway 2005 (mandatory for sensitive data), Japan 2005 (mandatory for financial services) UAE 2006 (financial services mandatory notification to regulator only; Spain 2007 mandatory internal register but voluntary notification; Germany mandatory 2009, Austria mandatory 2010
- In EU mandatory DSBN for telcos/ISPs under 2009 EU e-privacy Directive, effective May 2011 – other members without existing DSBN requirement slow to implement – current consultation on additional rules
- Voluntary elsewhere – Regulator and/or Law reform recommendation and/or guidance in many jurisdictions – Australia, NZ, Canada
- Notification required by regulators in response to major incidents – e.g. Sony, Vodafone
- Firm proposal for revised general EU Directive/Regulation
- Canvassed in current reviews of OECD GLs and Council of Europe Convention 108

How should DSBN be made mandatory?

- Addition to security principle in privacy law?
- Separate principle in privacy law?
- Separate law? (Easier, given priority – c.f. Spam and Do-not-call Register)

Scheme design

- Requirement should be proportionate to scale and severity of breach
- Needs thresholds and criteria (exceptions)
    - objective criteria e.g. no of affected subjects?
    - subjective criteria e.g. 'real risk of serious harm' (but who judges?)
- Exceptions?
    - publicly available data (but what if breach of normal access rules?)
    - encrypted data (but what standard?)
    - prejudice to law enforcement investigation (who decides?)
- Tiered requirement – perhaps notify regulator initially, take advice on notification of affected individuals
- Should all customers/data subjects be notified? – not just those affected (may be difficult to tell who is affected)

Sources:

http://en.wikipedia.org/wiki/Security_breach_notification_laws
http://www.ncsl.org/default.aspx?tabid=13489

Burdon, M, Lane, B and von Nessen, P, *'The Mandatory Notification of Data Breaches: Issues Arising for Australian and EU Legal Developments'* (2010) 26(2) *Computer Law & Security Review* 115 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1697929

Karin Retzer and Joanna Lopatowska, Morrison & Foerster LLP, April 2011, *Dealing with data breaches in Europe and beyond* - this article is part of the Practical Law Company (PLC) multi-jurisdictional guide to data protection www.practicallaw.com/dataprotectionhandbook.