Australian
Privacy
Foundation

post: GPO Box 1196
Sydney NSW 2001
email: mail@privacy.org.au
web: www.privacy.org.au

Australian Privacy Foundation (APF) submissions on data breach notification guidelines

16 June 2008

The Australian Privacy Foundation

The Australian Privacy Foundation (APF) is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. We aim to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. We use the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed.

For further information about the Foundation, see www.privacy.org.au

Introduction

The APF supports the general proposal in the Federal Privacy Commissioner's Consultation Paper (OFPC, 2008) that the Commissioner should issue non-binding guidelines concerning data breach notifications under the *Privacy Act 1988*, applicable to both private sector organisations and government agencies.

> **Submission 1: APF supports the Commissioner issuing non-binding guidelines concerning data breach notifications.**

Uncertain status of the Commissioner's proposed 'Guide'

The Commissioner proposes to issue a 'Voluntary Information Security Breach Notification Guide'. The word 'guidelines' is never used in the document to describe what the Commissioner is doing, nor is any statutory source of authority for the Commissioner's actions mentioned. This is both puzzling and concerning, given that the only obvious source of authority to take such steps is the function of issuing Guidelines under s 27(1)(e) of the Act, which allows the Privacy Commissioner:

> (e) prepare, and to publish in such manner as the Commissioner considers appropriate, guidelines for the avoidance of acts or practices of an agency or an organisation that may or might be interferences with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals ...

The final 'or' gives the Commissioner two bases on which to issue s 27(1)(e) guidelines, but they are very different types of guidelines.

Guidelines under the first limb of s 27(1)(e), to avoid acts or practices 'that may or might be interferences with the privacy of individuals', refer in a very technical way to practices that may breach the Privacy Act 1988 (Cth) and lead to remedies by breaching the s14 Information Privacy Principles (IPPs) or, in the private sector context, the NPPs, or certain other legislative standards concerning tax file numbers (TFNs), credit information and so on. Only 'an interference with the privacy of the individual' may be the subject of a complaint to the Commissioner under s 36, or any of the remedies under the Act. Guidelines issued under this limb of s 27(1)(e) are therefore the Commissioner's non-binding interpretations of (or guidance on) what the IPPs or the NPPs require as a matter of law.

In contrast, Guidelines under the second limb of s 27(1)(e), to help avoid acts or practices 'which may otherwise have any adverse effects on the privacy of individuals', are merely the Commissioner's advice as to what he or she considers good practices. These Guidelines do not interpret the law, do not give a guide as to which acts or practices might breach the law, and can address privacy issues where there is no legislation at all on the subject.

Therefore, s27(1)(e) enables the Commissioner to formally issue any type of guidance to both the public and the private sectors, both guidance on how to avoid breaches of NPPs or IPPs, and guidance as to what is good practice in avoiding other types of adverse effects on individuals' privacy.

The APF considers that Commissioner should not ignore the clear provisions of the Privacy Act concerning how 'guidance' should be issued by the Commissioner. What is the purpose of s27(1)(e) if it is not used for guidance on data breach notification? Furthermore, the Commissioner should make it clear which part of s27(1)(e) various parts of the guidelines are made under. There is nothing to prevent the one document giving advice on how to avoid IPP/NPP breaches, and also to suggest good practices even if they are not needed to avoid breaches. Both business and government – not to mention individual citizens and consumers – would benefit from such clarity in what the Commissioner is doing.

> **Submission 2: The Privacy Commissioner should issue the proposed 'Guide' as 'guidelines' under s27(1)(e) of the *Privacy Act*, and should also make it clear in relation to particular parts of the 'Guide', which parts are guidelines under the first limb of (e) (guidelines on NPP or IPP compliance), and which are guidelines under the second limb (good practice advice). The Commissioner should not avoid using appropriate provisions of the Act.**

Data breach notifications and breaches of Privacy Principles

Although the Act does not impose explicit breach notification obligations, it does impose an otherwise undefined obligation to 'take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure'. It is a plausible argument that the obligation to protect against 'misuse' includes an obligation to

take reasonable steps following any data security breach in order to minimise its harmful effects.

The Consultation Paper recognises in general terms that 'notification may in some circumstances be considered as a reasonable step' (OFPC, 2008: 18), but does not take the next step to state whether failure to notify may also constitute a breach of the Security Principle. This failure to state a position on the most fundamental question of interpretation of a Principle is a disappointing failure to give guidance where it is needed.

Similarly, Step 3 in the draft Guidelines lists factors that should be considered in determining whether to inform the Privacy Commissioner, but they are stated very generally and without implying that the Commissioner should be informed in any particular circumstances. There seems to be a great deal of reticence about giving any clear suggestions about what *should* happen (on a basis of good practice) simply because the Act does not require that it *must* happen. The Privacy Commissioner does not risk venturing an opinion on anything substantive, and therefore does not actually give 'guidelines' in the usual sense of the word.

> **Submission 3: APF submits that the Commissioner should issue guidelines concerning the circumstances under which failure to provide notification is likely to be considered as a failure to take reasonable steps for the purposes of the Security Principle.**

There is no doubt that a good deal of common sense and practical experience can be found in the Commissioner's draft guidelines, but it is surprising how little firm advice is available from them.

Presumptions as a useful device in guidelines

The OFPC draft follow guidelines issued by various Canadian Privacy Commissioners, by New Zealand's Commissioner (NZ PC, 2008) and most recently by Victoria's Privacy Commissioner (OVPC, 2008). These guidelines share some of the limitations that APF sees in the OFPC draft.

On 1 April 2008, the UK Information Commissioner's Office (ICO) published new guidance on how to manage data security breaches and when to notify the ICO of such breaches (UK ICO, 2008). The guidance sets out what the ICO considers to be the four important stages of any breach management plan. The UK office 'recommends that serious breaches be brought to its attention', and when 'the presumption should be that a report to the ICO is appropriate', although its Act is equally silent on the subject:

> Stage 3: **Notification of breach** Although there is no legal obligation imposed on data controllers, the Information Commissioner recommends that serious breaches be brought to its attention. 'Serious breaches' are not defined, but the guidance does detail the principal considerations for a data controller when determining whether it is appropriate to notify the ICO. The primary factor is the potential harm that may be suffered by individuals. This is to be measured by reference to the volume and sensitivity of the data involved. The guidance suggests that where there is a large volume of data (ie. over 1000 individuals involved) and there is a real risk of individuals suffering some harm, the presumption should be that a report to the ICO is appropriate. Similarly, where the volume of data is relatively small, but there is significant risk of individuals suffering harm, there should also be such a presumption. The guidance also offers a description of what information a notification should include and the steps that the ICO may take when a breach is reported.

The ICO's guidance illustrates a Commissioner giving very clear advice, but qualifying it by describing it as a presumption, so that while it is usually applicable, the facts of a particular situation may occasionally make inapplicable.

The APF accepts that the Commissioner (or the Commissioner's Office) cannot give detailed unequivocal statements about what will and will not constitute a breach of an IPP or NPP, since the Commissioner may be required to make decisions concerning complaints on very similar factual circumstances. There must always be scope for the Commissioner to decide that the particular circumstances of a situation complained about are such that a breach has or has not occurred contrary to the impression that may be given by guidelines, since they cannot anticipate every variation in context. Similarly, advice on what is generally a good practice may sometimes be inapplicable in unusual circumstances. However, this problem does not mean that the Commissioner should retreat from giving substantive and useful guidance. The UK ICO approach of stating presumptions on such matters as when notifications should be given (at risk of breach of the Security Principle or some other Principle) is worth further investigation and possible emulation.

> **Submission 4: The APF submits that the Commissioner should take an approach similar to the UK Information Commissioner, and issue guidelines which state presumptions as to when notification to the Commissioner, and/or to the individuals affected, are appropriate. Such presumptions may be useful both in relation to breach avoidance guidelines, and good practice guidelines.**

References

NZ PC (2008) – Privacy Commissioner (New Zealand) 'Privacy Breach Guidelines' at http://www.privacy.org.nz/privacy-breach-guidelines-2 (February 2008)

OFPC (2008) – Office of the Federal Privacy Commissioner (Australia) *Consultation Paper – Draft Voluntary Information Security Breach Notification Guide* (April 2008)

OVPC (2008) – Office of the Victorian Privacy Commissioner 'Responding to Privacy Breaches', May 2008

UK ICO (2008) Information Commissioner's Office (UK) *Guidance on data security breach management,* April 2008
<http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf>