

Australian Privacy Foundation

Submission on OFPC Consultation Paper on Privacy - Collection of Publicly Available Personal Information

September 2002

Introduction

The Australian Privacy Foundation¹ welcomes the opportunity to make a submission on this important issue.

We note the limited scope of the proposed information paper – being confined to the collection of personal information from publicly available sources; and the reasons given for not broadening the scope. However, we find it difficult to confine our submission completely to the collection issue and request that you take into account some of the broader issues we canvass. We feel that an information paper that deals with some of the broader context would be more helpful, and note that you have already included some relevant discussion of the responsibilities of the providers of publicly available personal information under both Federal and State privacy laws. We argue that the information paper should be directed not just to *collectors* of publicly available personal information but also to the *providers* of such information.

For the purposes of this submission, the following labeling scheme is used to illustrate scenarios.

An organization that initially makes personal information publicly available is described as the source organization or party A

Other organizations which acquire the publicly available personal information from A for their own use are described as third parties or party or organization B (Third parties because the first two parties are the individual and party A). This use of ‘third party’ is consistent with the definition in the Victorian IPA)

Other organizations which acquire publicly available personal information indirectly from a type B organizations (often in a processed form with or without additional non-public information – such as a mailing list) are described as party or organization C. (These would also be third parties under the Victorian IPA, but are distinguished here for clarity).

¹ See www.privacy.org.au

Information and recording – Key Terms

The Privacy Act is unfortunately confused about the relationship between the broad concept of information and the more particular recorded forms of information. Its attempts to clarify and distinguish these concepts in our view often hinder rather than assist understanding.

The definition in the paper of ‘Publicly available personal information’ (PAPI) (it is not defined in the Act) is unhelpful in that it confuses rather than clarifies the relationship with ‘generally available publication’ (GAP), which *is* defined (as a particular information product).

It needs to be clearly understood that GAPs containing personal information (PI) are a sub-set of PAPI. In other words, all GAPs containing PI are necessarily PAPI, but not all PAPI is in the form of a GAP. For instance, information can be ‘generally available’ only on request, in which case it is PAPI but not a GAP. Also, personal information that was made available ‘incidentally’ but had to be assembled by the user would in our view be PAPI but not necessarily a GAP.

To create a GAP there would we think have to be some purposive assembly of information into a ‘product’. For example, an organisation which simply allowed public access (whether by manual inspection or by searching a web site) to information containing personal information, but without organizing it in any way that facilitated the retrieval of the personal information (eg: a newspaper archive, or a library copy of Council minutes), would in our view be providing PAPI but would not in itself be providing a GAP containing PI.

The definition of PAPI in the paper comes dangerously close to suggesting that most PAPI will be in GAPs – when in fact far more personal information will be PAPI in a variety of forms than is contained in the much more limited range of GAPs.

The definition of ‘public register’ is also unhelpful – it defines it in terms of “information that individuals are required by law to provide” rather than, as one would expect, a legal requirement to publish. By adopting this curious definition the scope of ‘public register’ is artificially restricted – excluding many public registers which contain information provided voluntarily and optionally. It is certainly true that a requirement to provide increases the significance of the privacy issues surrounding public registers, but this does not mean those issues are not also relevant to some extent to information provided voluntarily but required to be published once provided.

The definition of PAPI in the paper also suggests that some public registers will not be GAPs, and may not be publicly available at all. We suggest that this runs counter to the common usage of the term public register which emphasizes public availability (with or without a charge and/or conditions), with ‘collection for a public purpose’ being a characteristic of most public registers, but not their defining quality.

The definition in the NSW Act (PPIPA 1998) is more intuitive and includes not only information that is *required by law* to be made public but also any register of personal information that is *made publicly available or open to public inspection*.

The NSW definition does however restrict itself to ‘registers’ of personal information . Register is undefined, but one could expect *register of personal information* to mean a list purposefully designed to convey information about individuals. Not all entries on the list need be individuals (so that for example the registers of various types of licensee that can be inspected would be *registers of personal information* under the NSW Act even though some, or most of the entries are for legal entities). But it would have to be more than a list which *incidentally* contained some personal information (so that publications of case law, for example, would not be a *register of personal information* under the NSW Act simply because the names of parties used to cite judgments are in some cases those of individuals, nor because some judgments contain personal information about named individuals).

The Victorian Act (IPA 2000) uses yet another definition of public register - it must be a *document* (but this includes electronic databases etc); be *required by a law* (other than the FOIA or PRA) to be *open to inspection* by the public (but not necessarily made available in any other form). Register is defined independently of personal information ie: a register may or may not include personal information

Policy discussion - Your questions 1.1 & 1.2

The introductory policy discussion is useful and should be included in any information paper (ut see comment on structure and content at the end).

Unfair collection and use (NPPs 1.2 and 2)

– Your questions 2.1 - 2.7

In our view it is impossible to limit the discussion of how the *collection* principle NPP 1 applies to publicly available personal information without reference also to the *use* principle NPP 2.

If the organization responsible for making information publicly available does not seek to place any restrictions or limitations on the use of the information (whether or not they are enforceable in practice), it is difficult to see how any use of the information by a third party could be seen as ‘unfair’.

On the other hand, if the organization responsible for making information publicly available *does* seek to place any restrictions or limitations on the use of the information, then an intentional use in contravention of those restrictions or limits should be regarded

prima facie as unfair. (It may also be unlawful if the restrictions or limitations have a basis in law).

Unfortunately fairness, in Australian privacy laws, is a concept that is restricted to collection, and does not apply to use (or disclosure) (compare European laws which include the concept of fair *processing*). There is no requirement under Australian privacy principles for *use* to be fair.

A third party that collects information that is made publicly available will have a purpose or purposes in mind. These may be consistent with any restrictions or limitations, or inconsistent. As long as there is one consistent purpose, it is difficult to see how collection could be considered unfair, even if the third party has another inconsistent purpose in mind – this can only be controlled, if at all, by the *use* principle (NPP2 or equivalent). Given that a third party could always claim that *one* of its purposes was simply to retail/disseminate the information (the same purpose that it was originally made publicly available), how could collection ever be unfair?

However, the ability of the use principle (NPP2) to control unwelcome uses of publicly available information (such as *CrimeNet* and *Wanted World Wide*) is limited by its acceptance of use for the primary purpose of collection without consent. The principle works reasonably well when collection is directly from the individuals concerned and they have a genuine choice as to whether to give the information in the first place. But it does not work well when collection is from a third party source, or where individuals have no choice as to whether to give the information. Much publicly available personal information combines both of these characteristics, and NPP 2 fails to offer individuals any effective control over uses which may be unwelcome, unless the source organization has imposed some restrictions or conditions.

This should therefore be the focus of attention – if the sources of publicly available personal information can be encouraged to specify the permissible uses, and make respect for that specification a condition of access, then third party users can be held accountable for any departure. In this respect, we like the approach taken by the Victorian Privacy Commissioner - in his recent report on Building Permit Data - of distinguishing between purpose and subsequent uses – which may or may not be allowed with or without conditions.

Statutory restrictions on uses, with penalties for non-compliance, is the strongest and therefore preferable way of specifying permitted uses. Contractual limits or conditions are the next best option – not so much for their direct enforceability as for the foundation they provide for effective application of the privacy principles – particularly NPP 1.2. This is because whatever a third party organization might like to do with personal information, it cannot claim to be fairly collecting for purpose Y if use Y is expressly prohibited by the source organization. It can collect fairly for purpose X (a use allowed by the source organization) but then in order to use it for use Y the third party must satisfy one of the exceptions to NPP2 – it cannot rely on Y being the *primary* purpose.

The media exemption

The utility of the Privacy Act in regulating the collection and use of publicly available personal information is significantly weakened by the media exemption provided by s.7B(4). This exemption undermines the control of publicly available personal information in the following way.

Any organization that obtains publicly available personal information that can fit within the media exemption is free to collect and use that information in whatever way it likes, subject only to the very weak conditions in s.7B(4). Almost any organization that wants to publish personal information (such as *CrimeNet*) can be a 'media organisation'; 'journalism' is undefined, and there is no quality control over the standards to which it must be publicly committed (a publisher could in effect write its own). Given these weaknesses, such an organization can lawfully ignore any restrictions or constraints that the source organization (A) might seek to impose, unless this is done by contract – and even then enforcement would be uncertain.

You mention this exception in paragraph 51, but only in the context of sensitive information. We suggest it is a much wider problem that seriously undermines any attempt to control the collection and use of publicly available personal information. While we accept that it is beyond the scope of the current exercise, we would like to see an acknowledgement of the problem, with at least a referral to the forthcoming review of the Act.

Countering business alarmism

Claims by business groups that restricting the uses of publicly available personal information would have a major adverse impact on direct marketing activity and jobs (alluded to in paragraph 27 of the paper) should be subjected to critical scrutiny.

In the first place, even if personalized direct marketing was entirely prohibited (and no-one suggests it should be), businesses could still send unsolicited communications to households, and could even target particular socio-economic groups by using aggregate census data or other neighbourhood profiles based on non-personal information about such things as housing types, patterns of sales etc.

Business lobbyists should be asked to provide empirical evidence of the difference that a loss of personalization would make. The likely effect would simply be an as yet unquantified loss of *efficiency* in direct marketing. This would not necessarily lead to a loss of sales or jobs - it would more likely lead simply to a re-adjustment in the balance between direct marketing and other forms of advertising and marketing.

In any case, restricting the uses of publicly available personal information would not necessarily have a dramatic impact on the availability of personalized marketing lists. Many of these are now compiled from previous transactions – lists based on actual

purchasing history are likely to be much more valuable and effective than those based on the sort of information to be found in publicly available sources such as public registers. The latter source data can at best be used to make informed guesses about likely interest in goods and services, which is inevitably a second best to actual behaviour.

Privacy laws will also of course have an effect on the collection and use of transaction information, but are only likely to make marketing lists progressively more accurate and efficient, as consent is obtained and those who do not wish to be approached in this way are progressively excluded.

In the long term, it is quite possible that the direct marketing industry will benefit from the application of privacy principles rather than be damaged by them.

NPP 1.4 – Your questions 3.1 – 3.4

Taken literally, this principle could prove a major impediment to indirect collection. We assume that this is one principle which the Commissioner will interpret with particular regard to the other public interests set out in s.29, and a generous interpretation of what is not reasonable and not practicable, so as not to interfere with significant existing commercial and administrative practices.

Whilst it might seem desirable to encourage direct collection as an alternative to collection from publicly available personal information, we question whether this is really practicable or sensible in most cases, for the reasons which your paper explains. We too would be interested to hear of practical examples of where it might be possible to insist on direct collection even where the information is publicly available, but none come to mind. Unless some examples can be given as an illustration, we doubt if the information paper should push this issue, lest it be seen as unrealistic advice that brings the Privacy Act into disrepute.

NPP 1.5 - Your questions 4.1 – 4.6

We support the broad interpretation of ‘from someone else’ to include collection of publicly available personal information from publications. As the paper suggests, individuals would expect the requirement to apply equally to collection from a person or organization or from a ‘thing’, and in any case we agree that collection from a thing is in effect collection from the person or organization which compiled the thing. The intention of this principle would be seriously subverted if the alternative narrow view was taken.

We do not think the paper places enough emphasis on the responsibility of the organizations which compile and make available publicly available personal information to convey the information referred to in NPP 1.3.

In some cases, the source organization will be a public agency and therefore subject to one of the equivalent principles to NPP1.3 (eg: IPP 2 for Commonwealth and ACT agencies, IPP 3 for NSW agencies and IPP 1.2 for Victorian agencies). If these agencies are complying adequately with the relevant principle, individuals should have been made aware that the information might be provided to organizations of all the likely third party types (covering item (d) in NPP 1.3).

Some of the other matters listed in NPP 1.3 are unlikely to be relevant to third party collection (such as items (e) and (f)). Item (b) is likely to be satisfied by the cumulative effect of compliance with privacy principles across all sectors – as individuals become generally aware of their right of access and correction.

The items in NPP 1.3 that are unlikely to be satisfied in advance are (a) – the identity of the organization and how to contact it, and (c) the third party's purpose. These are very specific and in the circumstances of collection from publicly available personal information can only really be satisfied by the third party organization itself. The only 'relief' from this obligation is if the steps that would need to be taken were 'unreasonable'.

It would not generally be reasonable to expect third party organizations to contact individuals in advance of collecting information about them from publicly available personal information. But it would rarely be *unreasonable* to expect them to notify the individual that they had collected their information, tell them the purpose (and remind them of their access and correction rights) *at the time of first contact* after the collection (as you suggest in paragraph 49).

In this respect we are disturbed by the recent media release from the Attorney-General concerning charities use of telephone directories. We think that his statement that "*Charities and other organisations that make use of information provided in generally available publications are not under similar obligations*" pre-empts the outcome of your consultation and is likely to be wrong in law. Whether or not there is a reasonable expectation that telephone directories will be used as prospect lists by marketers (including charities) does not in our view detract from their obligation under NPP1.5 to inform the people they contact of their identity and purpose in having collected the information from a directory.

We also support the suggestion that a third party organization (B) that uses publicly available personal information in its 'products', but does not itself contact individuals – instead passing it on to others (C) who will be contacting individuals; should require its clients (C) to notify the individuals about at least the identity of B and B's purpose. But we would go further than your suggestion (in paragraph 50) that this should only be 'on request' – there is no reason why B should not make pro-active notification by C a condition of providing the personal information.

NPP 10 - Sensitive Information - Your question 5.1

On other occasions we have pointed to the weakness of the NPPs in imposing special controls only on the *collection* of sensitive information and not on its *use*. This weakness is highlighted in the context of publicly available personal information. The consultation paper suggests that NPP10 requires a third party organization (B) collecting sensitive personal information from a publicly available source to seek the individuals' consent, in advance (this is the clear implication of 10.1(a) – the individual *has consented*). This is clearly impracticable in many cases and if strictly applied would mean that organizations could freely inspect, but not record, sensitive personal information that is publicly available. It is difficult to see the policy sense in such a requirement. The threshold issue of whether to 'protect' sensitive personal information that is publicly available has usually been made on other criteria – often a legal requirement to publish. What is needed in these circumstances is effective control over the *uses* that can be made of the information – preventing it from being collected is at best a crude and blunt way of achieving this.

Where sensitive personal information is included 'incidentally' in publicly available information, we do not think that NPP 10 should be applied so as to prevent third parties (B) from making it available in other forms, provided those forms do not materially increase the accessibility of the personal information. To apply the principle strictly in these circumstances would we suggest be widely seen as interfering significantly with a wide range of socially useful practices including the activities of libraries and information services. What is needed is a way of distinguishing potentially harmful 're-processing' (such as the *CrimeNet* and *Wanted World Wide* initiatives), from 'neutral' re-processing which does not focus on incidental personal information. We cannot offer a ready made solution to this difficult issue, but suggest that an attempt be made to offer some distinguishing criteria in the information paper.

Structure and content

We suggest that there is a need both for a fairly detailed paper explaining and discussing the issues, and for a concise check list for practical guidance.

End.

*Australian Privacy Foundation
C/- Law Faculty
Room 1212 Mathews Building
University of NSW 2052
t. 02 9385 1208
f. 02 9385 1778
For e-mail contact see covering e-mail*