Australian Privacy Foundation

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

18 July 2008

Ms Karen Curtis
Privacy Commissioner

cc: Joan Sheedy, Assistant Secretary, Department of Prime Minister and Cabinet

Your reference C10786: AT

Disclosure of Financial Transaction Data by Australian Financial Institutions

We have received Mr Hummerston's letter dated 5 June 2008 ('your response' below) in response to our complaint (revised version dated 12 October 2006). Because of delays due to mail redirection, the letter was not received in time for us to respond by your deadline of 20 June. We requested, by email, an extension of time to the end of July. Given the time that your office has taken to deal with the matter, we feel that this is a reasonable request.

As your response acknowledges, there have been lengthy delays in your investigation of this matter and we would like to place on record our dissatisfaction with this. A delay of more than 21 months for investigation of a very significant systemic compliance issue is in our view quite unacceptable, and is another reason for representative complaints to the Privacy Commissioner now being widely perceived by civil society organisations as ineffective and a poor use of scarce time and resources. In turn, the consequent discouragement to use of this potentially valuable method for addressing systemic compliance issues tends to undermine the claim of the office to be fulfilling its mandate. We have in the past drawn attention to the inordinate delay in dealing with systemic complaints and had hoped that progress had been made.

In our complaint, we suggested that you consider dealing with it by means of an own-motion investigation, and Mr Hummerston confirmed in a letter dated 12 October 2007 that you had taken this option (although this is not mentioned in your response). Unfortunately, our confidence that this would be a more effective and efficient way of dealing with the complaint appears to have been misplaced.

In relation to your substantive findings, we are very disappointed that, after all this time, your response is so superficial and does not indicate a rigorous analysis of the compliance issues.

We note that you do not appear to have addressed at all our point that the issue of compliance was likely to vary depending on which of three time periods was considered – related to international publicity about the SWIFT issue and consequent levels of likely awareness by organisations in Australia.

Nor do you appear to support the notion that notification to data subjects has to be effective in communicating relevant and significant facts which may influence a persons informed consideration of consequences of their actions, endorsing instead a 'mere formality' model that has been criticised by citizens as unhelpful, and by business as wasted effort.

We make the following specific responses:

NPP 1.3

Concerning the requirement to disclose '(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind', you say 'Australian financial institutions are not required to specifically identify SWIFT or any other organisation to which financial institutions usually disclose personal information'. You state that 'financial institutions will normally disclose that customers' information may be sent overseas to overseas banks or beneficiaries, external service providers and to third parties as required or permitted by law', and seem to be satisfied with this general practice.

We read your findings as stating that the Commissioner's view is that there will never be any obligation on organisations to specify *particular named* organisations as 'usual disclosees', however significant the disclosure practice in question, or even any obligation to be *specific about the types* of organisations depending on the types of privacy risks involved in disclosure.

We submit that such an approach is wrong as a matter of law, as well as being poor privacy policy, on a number of grounds. First, to allow any statement of types of 'usual recipients', no matter how vague and uninformative (as in the example above), removes any role for (d) as effective privacy protection, which is not consistent with the purpose of the *Privacy Act* as remedial legislation. Second, if such an approach is taken, then to state that individual recipients need never be named may be to render the words 'the organisations' in (d) without any meaning, because disclosure of 'types of organisations' is all that will ever be required. We submit that (d) should be interpreted so as to require the disclosure of information relevant to the privacy protection of individuals.

Does the Commissioner have Counsel's advice supporting such a narrow interpretation of the Act on such an important issue?

We also read your finding as confirming that there is no requirement under NPP 1.3 to specify the country or countries of location of organisations to which information is 'usually disclosed', even in this case where the two locations in which SWIFT facilities are housed are known to institutions and could therefore readily be specified. In particular, the processing of all material in the US (thereby rendering it susceptible to unwarranted and arguably unlawful domestic agencies' searches, even where there is no connection with a US transaction or institution) is a critical and easily disclosed fact. There may be potential adverse consequences to many Australians from this unexpected technical diversion. The location of recipient organisations could be regarded as one way of specifying 'the types of organisations' where this is sufficiently important.

These are very significant interpretations of NPP 1.3, which severely limit its effectiveness in achieving the objective of putting individuals in a position where they can exercise an informed choice about whether to enter into a transaction. By omitting the key relevant detail, the data subject remains effectively ignorant of the relevant facts which would be essential to adequately inform them about the implications and risks of certain actions. Your office's interpretation does not result in a basis for informed decision-making, and effectively shields the banking industry from their obligation to keep their customers informed in an effective way.

We request your confirmation of these readings of your findings, a copy of any opinion you have to support this interpretation, and invite your comments on the effect of the interpretation on the effectiveness of the principle.

NPP 2

We note your response but point out that we did not allege any breach of this Principle in our revised complaint dated 12 October.

NPP 9

Your response suggests that Australian Financial Institutions would potentially be able to satisfy NPP 9 with respect to transfers of personal information outside Australia in several different ways:

(i) By relying on individuals' consent (NPP 9(b)); or
(ii) By relying on the exceptions for transfers necessary for the performance of contracts (either between the individual and the organisation or in the individual's interest) (NPP 9(c) and (d)).

We address each of these in turn below. They both involve what appears to be contentious interpretations of important matters under the Act. Do you have any Counsel's opinions supporting these interpretations?

(i) Consent

Are you suggesting that Australian institutions have relied on 'implied' consent? The information from the ABA that members have amended or are amending their telegraphic transfer forms to incorporate express consent suggests that this has been the case. But it invites a number of further questions:

- Do you consider that implied consent is a sufficient basis for reliance on NPP 9(b) in the context of transfers involving the use of SWIFT? If not, then why have you not considered whether banks and other financial institutions relying only on implied consent have previously been in breach of the Act, and perhaps are still in breach of the Act? It does not seem that you have established that all 88 SWIFT members have changed their forms, as you seem to have only dealt with a few banks at best.
- If you do consider implied consent is sufficient, how can individuals be expected to form a view sufficiently informed as to provide a foundation for implied consent in the absence of any information about the role of SWIFT in the foreign transfer system?
- Whilst it is reasonable to assume that individuals would expect disclosures to the country to or from which they are transferring funds, what basis is there for an assumption that they would expect transfers to third countries being those involved in the international payments system, and specifically those in which SWIFT has its facilities? Further, what basis is there to expect them to appreciate that their transaction data would be transferred to a country

such as the US which has extremely limited privacy protections, in those cases where there is no obvious connection with or reason for US involvement?

- Do or will the amendments to forms expressly mention SWIFT, or do you take the view that a general reference to 'transfers outside Australia' will suffice? It would have been helpful to have included examples of amended forms, so that we could make our own assessment of their adequacy. Are you able to provide any examples of the new disclosures?

We assume you are saying that whatever position individual institutions are taking on notification to customers, this can be considered a purely voluntary 'extra', given that in your view they can rely on other exceptions to NPP 9 (see below).

Please confirm that this is a proper reading of your position and that you do not see NPP 9 as requiring any additional notification beyond that required for compliance with NPP 1.3 (see above).

(ii) Necessary for performance of a contract

Your response does not provide any analysis or explanation of the way in which these exceptions (NPP 9 (c) and (d)) apply to the circumstances of transfers involving the use of SWIFT. The letter merely asserts that these exceptions 'could be relied upon by Australian financial institutions as the transfer of personal information is necessary for the performance of the international money transfer.'

This assertion makes no attempt to distinguish between the different transfers involved, and in particular the non-obvious and un-necessary transfer of all material to unrelated countries. As noted above, it is obvious that international money transfer necessarily involves *some* transfers of personal information to *some* entities. It does not however follow that it necessarily involves transfer to SWIFT, and even if it did, that those transfers necessarily required transfer to *all* of SWIFT's processing locations, including those in the United States which are at the heart of the privacy concerns flagged in so many other countries, as you must be well aware.

Your response seems to be equivalent to accepting that the *status quo* in how any international transfer is carried out is necessarily the only way in which a contract could be performed, irrespective of its consequences for privacy and irrespective of whether any alternative ways of carrying it out are possible. If this is not the case, we seek your clarification. If it is the case, we submit that it is not a correct interpretation of the *Privacy Act*.

In short, your response does not adequately address the application of exceptions (c) and (d). We seek a further response on this point.

NPP 4

Your response does not address our allegation that the actions of Australian financial institutions in their use of SWIFT constitute a breach of NPP 4.

We look forward to your further response addressing this ground of our complaint.

Respondents other than Banks

Your response appears to relate only to 13 members of the Australian Bankers' Association. Our complaint related to an unspecified number of 'Australian financial institutions who are users of the SWIFT network'. We referred to the SWIFT Annual Report's reference to 88 non-bank Australian institutions.

Your response is silent as to whether you have sought to establish which other institutions use the SWIFT network, and whether you have taken any steps to communicate with them about their compliance with the NPPs with respect to transfers via SWIFT.

We seek your response to our complaint as it relates to Australian financial institutions other than the 13 members of the ABA to which you refer, and note that there are apparently 75 other such institutions.

Relevant information concerning SWIFT

We are very surprised that your response does not include any information about SWIFT and its interbank transfer facility, particularly in light of what we understand to be changes to its operations resulting from similar complaints to data protection regulators in Europe and elsewhere.

We are also very surprised that you have made no reference to action taken by your counterparts in other countries, and the outcomes. We expressly mentioned this other action in our complaint, in the hope that your investigation would involve liaison with those authorities and consideration of their findings.

We request that you address these aspects of the complaint.

Conclusion

We look forward to your reply to our responses above.

Your very narrow approach to handling this complaint (even as an own motion investigation) demonstrates, in our view, a failure to see the representative complaint mechanism as a useful way of addressing generic and systemic privacy compliance issues. By failing to explore either the effect of your findings on the objectives of the NPPs, or the inter-relationships between the principles in the context of overseas transfers, we feel you have missed a significant opportunity.

At the very least, we would have expected some acknowledgement of the policy issues raised by these practices, and reference to the Australian Law Reform Commission's Review of Privacy, in the course of which some of these issues were addressed, including by the Commissioner's own submissions.

We are inclined to interpret your handling of this complaint as illustrative of a number of systemic weaknesses in both the Act itself and in your office's approach to the statutory responsibilities of the Privacy Commissioner. For this reason, we are copying this correspondence to the Information and Security Branch of the Department of Prime Minister and Cabinet. The Foundation also considers that these weaknesses should become a matter of public record and debate, and will seek to bring them to public attention.

Yours sincerely,

Graham Greenleaf,
Board Member on behalf of the Board
Australian Privacy Foundation