

Privacy Impact Assessment in Hong Kong from an International Perspective

Nigel Waters, Visiting Fellow and Research Associate, [Cyberspace Law and Policy Centre](#)¹ (CLPC), Faculty of Law, University of New South Wales, and Principal of [Pacific Privacy Consulting](#)²

1st HKU-UNSW Research Symposium, 2-3 December 2010, at UNSW, Sydney, Australia

Abstract: Privacy Impact Assessment (PIA) is defined and a brief history given of the promotion and use of PIA in Hong Kong. The only PIA on a Hong Kong Project published to date is discussed in some detail. Lessons are drawn from experience both in Hong Kong and in other jurisdictions for the effective use of PIA as tool for privacy or data protection.

Acknowledgements: This paper reflects on experience of Privacy Impact Assessment (PIA) in Hong Kong from the perspective of a practitioner who has conducted many PIAs, mostly in Australia but also in New Zealand and Hong Kong, and has also closely observed PIA experience around the world both as a civil society privacy advocate and an academic. The paper draws on work by Roger Clarke (Visiting Professor at CLPC) as part of a consortium responsible for a [report](#)³ on PIA for the UK Information Commissioner in 2007. It also draws on draft chapters by the author and by [Roger Clarke](#)⁴ for Wright, David, and Paul de Hert (eds.), *Privacy Impact Assessments: Engaging stakeholders in protecting privacy*, Springer, Dordrecht, 2011 (forthcoming), and a [paper](#)⁵ by Professor Graham Greenleaf on the history of the Hong Kong Smart ID card.

What is Privacy Impact Assessment?

Privacy Impact Assessment (PIA) is a technique first developed in the 1990s for assessing the privacy implications of major personal information handling projects. It has quickly become a part of the standard privacy protection toolkit in many jurisdictions. While it is mandatory in a few jurisdictions⁶, it mostly remains merely a recommended step in the consideration and approval processes for major projects⁷.

PIA comes in many different shapes, sizes and flavours. This reflects the wide range of motives and objectives for undertaking PIA; the identity, status and experience of both the client and the assessor; the stage of the subject project at which PIA is undertaken; the involvement of third parties and the development and approval process into which PIA is inserted.

There are as yet no recognised certification standards, in any jurisdiction, for PIA. Anyone is free to pitch for PIA work, and while there are some specialised firms and sole practitioners, more and more

¹ <http://www.cyberlawcentre.org/>

² <http://www.pacificprivacy.com.au/>

³ http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/privacy_impact_assessment_international_study.011007.pdf

⁴ <http://www.rogerclarke.com/DV/PIAG-Eval.html>

⁵ <http://www.austlii.edu.au/au/journals/ALRS/2008/10.html>

⁶ US *E-Government Act* 2002, Treasury Board of Canada PIA Policy 2002

⁷ See for instance Guidance on PIAs issued in Australia by the Federal and Victorian Privacy Commissioners, by the New Zealand Privacy Commissioner and by the UK Information Commissioner. For a comprehensive list, see Office of the Information Commissioner UK, 'Privacy Impact Assessments: International Study of their Application and Effects' Information Commissioner's Office, Wilmslow, I.K., December 2007, Appendix I, <http://www.rogerclarke.com/DV/ICOSTudy-2007-Apps.pdf>

PIA is being performed by mainstream legal, accounting and consulting practices. PIA practitioners have varying qualifications and levels of experience. The privacy community, and potential clients, currently have to rely on an informal peer review process whereby aspiring assessors are recommended, or not, by regulators, pressure groups or previous clients. Attempts have been made to establish a privacy profession, with associated standards and certification processes⁸, but most experienced PIA practitioners do not currently see any need to belong, relying instead on their track record and reputation.

A brief history of PIA in Hong Kong

The history of PIA in Hong Kong up until 2007 was summarised in [Appendix G](#)⁹ of the Report for the UK Information Commissioner. During 2000, the then Privacy Commissioner for Personal Data, Stephen Lau, called publicly for PIA to be undertaken both for the proposed new ID card and for electronic health initiatives. In 2001, the Commissioner issued [guidance](#)¹⁰ on e-Business which included recommendation of PIA as a tool for both private and public sector projects. In his 2003-04 Annual Report, the then Commissioner Raymond Tang indicated an intention to “educate the community, private and public sectors ... about Privacy Impact Assessment” and to “make PIA a focus of our efforts over the year and, in the longer term, move on to consider the related aspect of privacy compliance or the auditing of projects that have been evaluated by PIA.

The next Commissioner, Roderick Woo, continued to encourage PIA, saying in one of his first [press conferences](#)¹¹ that “An ideal way is to encourage data users to undertake privacy impact assessment before implementing any project that may involve the use of personal data in order to plug the loopholes likely to contravene the requirements of the Personal Data (Privacy) Ordinance.” In 2008, a [report](#)¹² of a major inspection of the HK Hospital Authority included a recommendation to make it a policy to conduct privacy impact assessment, and similar recommendation was made to the Food and Health Bureau.

Most recently, in 2009, the Commissioner [assisted](#)¹³ the Transport Department of the HKSAR government in reviewing tenders for a PIA of a traffic management project. And in his final work programme [report](#)¹⁴, outgoing Commissioner Woo flagged an intention “to conduct first a Privacy Impact Assessment and then a Privacy Compliance Audit in respect of the Electronic Health Record Sharing Programme. This is likely to take more than five years from early 2010.”

Despite this record of support and encouragement of PIA, none of the successive HK Privacy Commissioners have to date issued any formal guidance on when and how to conduct PIA – unlike many privacy regulators in other jurisdictions, including Australia, Canada, New Zealand and the UK¹⁵. The guidance from these Commissioners are however relevant and available for use by data users in Hong Kong.

It is also surprising, and disappointing, that the Privacy Commissioner did not expressly address the role of PIA in the [review](#)¹⁶ of the Hong Long law he initiated in 2006, with the result that it has not

⁸ See [International Association of Privacy Professionals \(iaPP\)](#), founded in the US but now with chapters in other parts of the world, including Australia (<http://iappanz.org/>)

⁹ http://www.rogerclarke.com/DV/ICOSTudy-2007-AppG_HK.pdf

¹⁰ http://www.pcpd.org.hk/english/publications/eprivacy_9.html

¹¹ http://www.pcpd.org.hk/english/infocentre/press_20050901.html

¹² http://www.pcpd.org.hk/english/files/publications/anreport09_07.pdf

¹³ http://www.pcpd.org.hk/english/files/publications/anreport10_06.pdf

¹⁴ http://www.pcpd.org.hk/english/publications/files/work_report_e.pdf

¹⁵ See footnote 7.

¹⁶ http://www.pcpd.org.hk/english/review_ordinance/reviewordinance.html

been taken up by the government. The HKSAR government's October 2010 [Report](#)¹⁷ on Public Consultation on the Review of the Personal Data (Privacy) Ordinance, on which it has sought public comment by 31 December 2010, makes no express reference to PIA. This contrasts with recent reports in other jurisdictions which have recommended a formal role for PIA in the legal privacy protection regime.¹⁸

There are no records or statistics of the number of PIAs to have been undertaken in Hong Kong. In a slide accompanying a 2005 conference [presentation](#)¹⁹ the then Acting Privacy Commissioner, Tony Lam cited three examples of PIAs conducted in Hong Kong were mentioned, being the 'Caller Number Display' feature of telecommunication services; an 'Electronic Road Pricing' proposal and 'Online banking services, but none of these have been publicly reported. To date only one PIA for a Hong Kong project – the smart ID card – has been made public. While it is now nearly a decade old, the experience of this PIA, undertaken by the author and colleagues, illustrates many of the issues that still arise in relation to the use of PIA as a tool of privacy or data protection.

A case study of PIA in Hong Kong – the Hong Kong Smart ID card (SMARTIC)

The Immigration Department of the Hong Kong Special Administrative Region commenced a project in the late 1990s to replace the previous Territory identity card, introduced in 1987, with a new HKSAR 'smart' identity card (SMARTIC), to contain a microchip and biometric information.²⁰

In 2000, the author, with a team which included Professor Roger Clarke, was commissioned to undertake a PIA of the SMARTIC project. A generous budget (at least by Australian and New Zealand standards) allowed for a comprehensive and detailed assessment, but the client did not welcome many of the recommendations, and there was considerable tension during the finalisation of the report, leading to a final product which did not highlight key recommendations, leaving them to be 'discovered' by readers in the body of a lengthy document. Unsurprisingly, this meant that the PIA work was not used as effectively by potential critics, or in the course of the political process, as it could have been, had the assessors been able to present their findings differently.

The PIA recommendations, together with the government's response following discussions with the Privacy Commissioner, were presented to the Legislative Council (LegCo) Security Panel, thereby becoming public, in February 2001²¹, although the full PIA Report was not made public until some time in 2002²². A meeting of the Panel in December 2001 was given a list of the privacy related measures and actions taken by the Project to that date with a re-assurance on the government's decision to limit non-immigration functions for the new card, and to make any such functions available on a voluntary basis – consistent with the PIA recommendations.²³ However, in early 2002, amendments to the Registration of Persons Ordinance were introduced to allow for multiple non-

¹⁷ http://www.cmab.gov.hk/doc/issues/PCPO_report_en.pdf

¹⁸ Including the Australian Law Reform Commission's 2008 [Report 108 For Your Information](#) (Recommendation 47-4) <http://www.alrc.gov.au/publications/report-108>; and the EU Commission's November 2010 [Communication 2010/609 A comprehensive approach on personal data protection in the European Union](#), http://ec.europa.eu/justice/news/intro/news_intro_en.htm#20101104.

¹⁹ http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Paper_Technological_ubiquity_and_privacy.pdf

²⁰ The history of the SMARTIC project can be traced from an index to Legislative Council policy papers on the project at http://www.legco.gov.hk/database/english/data_se/se-hksar-identity-card-project.htm and a critical overview of the entire programme is provided by Graham Greenleaf in a 2008 paper *Hong Kong's 'smart' ID card: Designed to be out of control*, <http://www.austlii.edu.au/au/journals/ALRS/2008/10.html> (also Chapter 5 of Bennett, C and Lyon, D *Playing the Identity Card*, Routledge, 2008)

²¹ Paper at <http://www.legco.gov.hk/yr00-01/english/panels/se/papers/b752e04.pdf>

²² Report (abridged version) at <http://www.legco.gov.hk/yr00-01/english/fc/esc/papers/esc27e1.pdf>

²³ Paper at <http://www.legco.gov.hk/yr01-02/english/panels/se/papers/itbse1220cb1-666-1e.pdf>

immigration uses of the SMARTIC, contrary to the PIA report which had recommended legislative barriers to function creep.

The Department subsequently commissioned a second PIA as “an assessment on how the technical design has addressed the key data privacy recommendations in the first PIA report.” The recommendations of the second PIA, again together with the government’s response and taking account of the Privacy Commissioner’s views, were also made available to the LegCo Panel, in 2002.²⁴ A third PIA remains unpublished, while a fourth and final PIA, sometime in 2004-05, provided:

“an overall post-implementation review of data privacy protection relating to system controls, functionalities and manual procedures to ascertain that all privacy protection measures have been suitably implemented and are operating effectively in practice.”

The presentation of the fourth PIA to the LegCo panel states that:

“The Consultant finds that Immd is privacy conscious and has a strong commitment to addressing privacy issues and concerns arising from the SMARTICS project. Immd has also been responsive in implementing the recommendations arising from the various PIAs.”²⁵

The second, third and fourth PIAs were carried out by different consultants from the first (it is not known if the same consultant was responsible for the last three). Whilst it is not uncommon for agencies to use different consultants for different stages of PIA (see also the Australian e-health identifier project²⁶), it does mean a loss of continuity and experience, and it may be questioned whether the initial assessors would necessarily have the same confidence that their recommendations had been implemented as the ‘new’ assessors appear to have in the HK case. There are however potential benefits in ‘peer review’ and it is arguably just as likely that a second assessor would pick up weaknesses in the initial report or identify additional issues, as that they will provide a less rigorous assessment.

The potential for different conclusions to be drawn from the same facts strengthens the case for maximum transparency – if all PIA reports are made public, then interested parties can compare them and form their own judgement about their relative strengths.

Comparison of the three published sets of PIA recommendations for the HKSAR Smart ID card also illustrates another predictable trend – that in the later stages of a project, attention focuses on detailed systems design and procedural safeguards, compared to the consideration of ‘big picture’ issues, such as justification for privacy intrusion, alternatives, and risks of function creep, that is possible and justifiable at earlier stages. Once key decisions on project scope and design have been made, it is unreasonable to expect PIA assessors to revisit issue that have been effectively closed through the political process. That does not of course prevent interest groups continuing to pursue wider issues and it is worth noting that questions from HK legislators about wider uses of the ID card have continued, with the government giving assurances about future consultation.

Lessons from PIA experience

The experience of the SMARTIC PIA illustrates both the utility and constraints of PIA as a privacy or data protection tool. These lessons are confirmed by subsequent PIA experience in other jurisdictions.

²⁴ Paper at <http://www.legco.gov.hk/yr01-02/english/panels/se/papers/se0710cb2-2433-7e.pdf>

²⁵ Paper at <http://www.legco.gov.hk/yr04-05/english/panels/se/papers/secb2-858-1e.pdf>

²⁶ The Australian National E-Health Transition Authority (NeHTA) commissioned three separate PIAs from different assessors over a period of three years – they are published at <http://www.nehta.gov.au/connecting-australia/privacy/pias>

Most PIA reports will have only a limited ability to effect change, on their own, in the design or implementation of a major project. For a variety of reasons, most PIA reports will only go some way towards specifying changes to project design and implementation that will reduce privacy intrusion and enhance privacy protection and safeguards.

Where, as is normal, the assessor is engaged and paid by the project proponent, the pressures on the assessor mean that PIA reports will often only hint at potential problems. Assessors trying to fully document adverse privacy effects, or suggest alternatives or safeguards, but constrained in their ability to do so too bluntly, can often nevertheless include clues which can be detected and interpreted by experienced readers. Those who have faced this dilemma will recognise the frustration of having left what they think are obvious clues, or potential ammunition, only to watch regulators, non-government organisations and legislators fail to detect the clues and follow up accordingly.

All concerned should become more realistic in their expectations as to what a PIA report can achieve on its own without other interested parties becoming involved, reading the clues, and making use of the report to influence the outcome.

Privacy regulators in particular need to become more active in following up on PIA reports, asking project proponents to explain which if any of a PIA recommendations it accepts, and if not why not? Where recommendations are accepted, there also needs to be subsequent follow-up to ascertain if they have actually been implemented, and again, if not why not? It is all too easy for project proponents to say initially that they accept and will implement suggested changes, only to find reasons later to backslide, and either partially or wholly abandon their initial commitment.

There is a perception that privacy regulators have too often seen the issuance of PIA guidance, and the subsequent take-up of PIA by agencies and organisations as 'mission accomplished'. They may see PIA activity in response to guidance as a way of relieving them of responsibility for proactive work in relation to the projects concerned. In an environment where financial and staff resources available are always constrained, regulators understandably can be tempted to focus those resources on projects where there has been no PIA, or on other areas of work altogether, such as complaint handling. But this can be a false economy, if PIA activity does not result in actual changes to project design and implementation.

As with all areas of their work, privacy regulators may get a better 'return' for the deployment of scarce resources by following through at least some 'exemplar' PIAs, and publicising the outcomes as a way of demonstrating the value of PIA (or alternatively of demonstrating the risks of not addressing privacy implications).

Even if the conduct of PIA becomes mandatory, as has been suggested in some jurisdictions²⁷, it would be impracticable to mandate the adoption of all PIA recommendations. There are after all always other interests to be balanced against privacy protection, and circumstances will change, such that it will not always be appropriate to implement all recommendations. But regulators can at least follow through and require project proponents to justify why they have not accepted or implemented PIA recommendations.

²⁷ E.g. Australian Law Reform Commission, *For Your Information*, Report 108, May 2008, Recommendation 47-4 http://www.austlii.edu.au/au/other/alrc/publications/reports/108/_3.html#Heading403; UK House of Lords, Constitution Committee - Second Report, *Surveillance: Citizens and the State*, January 2009, paragraph 30. <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1808.htm#a56>

Many public sector projects require legislative authorisation, and PIA can and should be an important input to legislative processes. Unfortunately, legislative authority is often granted before a PIA is undertaken, which limits the scope for PIA findings to influence project design, even if they can still contribute to implementation safeguards.

Ideally, PIA should be undertaken in time for the report to be made available to legislators before they are called on to debate authorising legislation.

Conclusion

In conclusion, all interested parties need to develop a more sophisticated understanding of the practical and political realities, and take these into account when commissioning, reading and using Privacy Impact Assessment (PIA) reports.

PIA has great potential as a privacy protection tool, but that potential will only be realised if it is accepted that a PIA report is not an end in itself and will not generally lead unaided to better privacy outcomes. Assessors carrying out PIAs operate under significant constraints and are subject to many pressures that may prevent them from achieving as much with the processes and reports as others might expect.

But PIA can at least provide useful information for others to use in the bureaucratic and political environments where project designs are formed and where decisions on whether, when and how to implement are made.

The lessons drawn out in this paper are applicable in Hong Kong, Australia and all other jurisdictions, whether or not they currently have a privacy or data protection law.