This item was submitted to [Loughborough's Research Repository](#) by the author.
Items in Figshare are protected by copyright, with all rights reserved, unless otherwise indicated.

Privacy impact assessment in the UK

PLEASE CITE THE PUBLISHED VERSION

<http://www.springer.com/law/international/book/978-94-007-2542-3>

PUBLISHER

© Springer

VERSION

AM (Accepted Manuscript)

LICENCE

CC BY-NC-ND 4.0

REPOSITORY RECORD

Warren, Adam P., and Andrew Charlesworth. 2019. "Privacy Impact Assessment in the UK". figshare.
<https://hdl.handle.net/2134/9253>.

This item was submitted to Loughborough's Institutional Repository (<https://dspace.lboro.ac.uk/>) by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to:
<http://creativecommons.org/licenses/by-nc-nd/2.5/>

Privacy Impact Assessment in the UK

Adam Warren¹, Andrew Charlesworth²

- 1. Introduction..... 2
- 2. Legislative and Policy Framework 3
- 3. The UK PIA Process 6
- 4. Case Study: Office for National Statistics (ONS), 2011 Census 8
- 5. Lessons learnt..... 10
- 6. Future developments 14
- 7. Conclusion 15

¹ Department of Geography, Loughborough University, UK.

² School of Law/Department of Computer Science, Bristol University, UK.

1. Introduction

The adoption of PIAs in the UK is a recent development. Both it, and related initiatives such as “privacy by design”, pioneered by the Ontario Information and Privacy Commissioner, Ann Cavoukian³ (discussed further below), can be seen as indicative of a disenchantment amongst some regulators, including the UK’s national data protection regulator, the Information Commissioner’s Office (ICO), with the largely reactive approach to regulation adopted by the EU Data Protection Directive and the national legislation which implements it. As has been argued elsewhere⁴, that regime, which depends heavily upon data subjects acting proactively via the subject access mechanism, both to ensure data controller compliance and to provide the regulator with information, has proven to be ineffectual in the face of contemporary technological developments. When one considers established technologies such as the World Wide Web, or developing technologies such as cloud computing, neither of these disaggregated data environments lend themselves to effective regulation via the Directive’s largely post hoc processes.

In addition, the ubiquity of information technology, the ease and speed of data transfers and the devolving of control over information within organisations have resulted in commercial and governmental data environments where significant personal data losses can result from the relatively minor actions of low-level employees or of data processors. The loss of 25 million child benefit records by HM Revenue and Customs, resulting from the actions of a junior civil servant, demonstrates clearly the problems that the incremental and unmonitored development of internal practices and procedures relating to personal data holdings can pose for effective organisational data protection compliance.

In such circumstances, a clear, regulator-approved, organisational process, the goal of which is proactive identification and removal or amelioration of potential data privacy risks, would seem an attractive sell to both commercial and governmental organisations. In principle, everyone in the data privacy process can benefit. The data controller will benefit from engaging in a risk management assessment which reduces the likelihood of negative public reaction, and increases its ability to reduce the need for costly retroactive amendments to systems and processes. The regulator may have access, either as part of the process, or retrospectively, to information detailing the actions and decisions of the data controller based on its assessment, which would then inform its own actions in regard to that data controller. The data subject may have greater access to information about the data controller’s processes and the steps that have been taken to ensure the integrity and security of their personal data.

With these issues in mind, in 2007 the UK’s ICO commissioned a report on the development and use of PIAs in other jurisdictions, notably Australia, Canada, Hong Kong, New Zealand and the United States.⁵ Commissioned in tandem with the report was a practitioner handbook for PIAs.⁶ Both report and handbook were officially launched in December 2007 at the ICO’s conference “Surveillance Society: Turning Debate into Action”. In July 2010, the ICO published its *Annual Report*. In a chapter entitled “Educating and Influencing”, a small paragraph noted that “over 300

³ OIPC, *Privacy by Design*, Ontario Information & Privacy Commissioner, Toronto, 2009.

<http://www.ipc.on.ca/images/Resources/privacybydesign.pdf>

⁴ Charlesworth, A., “The future of UK data protection regulation”, *Information Security Technical Report*, Vol. 11, No. 1, 2006, pp. 46-54.

⁵ ICO, *Privacy Impact Assessments: international study of their application and effects*, Information Commissioner’s Office, Wilmslow, 2007.

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

⁶ ICO, *Privacy Impact Assessment Handbook*, Information Commissioner’s Office, Wilmslow, 2007.

Privacy Impact Assessments have been started across central government and their agencies”⁷. Yet, despite this ostensible policy success for a tool that had been launched less than three years earlier⁸, very few UK privacy impact assessment (PIA) reports have reached the public domain. Moreover, evidence of private sector activity in this field is almost non-existent, being restricted to the occasional report⁹ or citation¹⁰. It is perhaps, therefore, not surprising that academic interest in PIAs has been limited. As of July 2010, the total number of citation counts on *Google Scholar* for articles titled “Privacy Impact Assessments” appears to be 86.¹¹

This chapter aims to stimulate interest in this topic, and address some of the gaps identified above, through an investigation of PIAs being processed in the UK. In order to investigate this topic, it is important to start with a clear definition. The meaning ascribed to the term “PIA” has varied over time and across most jurisdictions.¹² In this chapter, we use the following definition, synthesised from descriptions given in various international guidance material for PIAs:

A *Privacy Impact Assessment (PIA)* is a systematic process for identifying and addressing privacy issues in an information system that considers the future consequences for privacy of a current or proposed action.¹³

Our analysis commences with an overview of the UK legislative and policy framework, and the extent to which this influenced the development of a methodology for the conduct of PIAs within the UK. We then consider the UK PIA process, drawing from examples of PIAs undertaken since the publication of the ICO’s PIA handbook. The practicalities of conducting a PIA are illustrated through a case study of the UK 2011 census, informed by empirical research conducted by the authors during July and August 2010. This is followed by a discussion of lessons learnt from the national experience to date, identifying potential pitfalls, misconceptions and gaps in understanding. We then discuss possible future directions for PIAs in the UK, paying attention to the drive towards a proactive approach to regulation, the influence of cross-jurisdictional technologies and the involvement of the private sector in creating and using systems to facilitate accountability and compliance. Finally, conclusions are drawn.

2. Legislative and policy framework

As noted above, the methodology for the conduct of PIAs in the UK was officially launched in December 2007 by the Information Commissioner’s Office. It took the form of a practitioner handbook (available electronically and, later, in hard copy), supported by a study investigating the use of PIAs overseas and the lessons learnt from their experiences.¹⁴ When developing the methodology for the UK, the team commissioned by the ICO were mindful of the fact that no previous official guidance had been published and that, at the time, there was no formal legislative

⁷ ICO, *Information Commissioner’s Annual Report 2009/10*, Information Commissioner’s Office, Wilmslow, 2010, p. 23.

http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2010.pdf

⁸ Warren, Adam, Robin Bayley, Colin Bennett, Andrew Charlesworth, Roger Clarke and Charles Oppenheim, “Privacy Impact Assessments: International experience as a basis for UK Guidance”, *Computer Law & Security Report*, Vol. 24, No. 3, 2008, pp. 233-242.

⁹ For example: 80/20 Thinking Ltd., *First Stage (Interim) Privacy Impact Assessment for Phorm Inc*, February 2008.

<http://blogs.guardian.co.uk/technology/Phorm%20PIA%20interim%20final%20.pdf>

¹⁰ ESRC Seminar Series, *Mapping the Public Policy Landscape: Assessing Privacy Impact*, 2009.

¹¹ Last reviewed on 23/08/10.

¹² See ICO, *Privacy Impact Assessments: international study...*, op. cit., fn. 5, and Tancock, D., S. Pearson and A. Charlesworth, *The Emergence of Privacy Impact Assessments*, HP Labs Technical Report (HPL-2010-63), 2010.

<http://www.hpl.hp.com/techreports/2010/HPL-2010-63.html>

¹³ Tancock et al., *The Emergence of Privacy Impact Assessments*, op. cit., fn. 12, p. 22.

¹⁴ The authors of this chapter were involved in this research project, which was commissioned by the UK Information Commissioner’s Office in 2007. Other members of the research team were Charles Oppenheim (Project Director), Colin Bennett, Robin Bayley and Roger Clarke.

basis, or governmental support, for the process. Consequently, the potential benefits to organisations had to be explicitly stated, and the tool itself had to be sufficiently flexible so as to be capable of being integrated within existing business processes. In addition, the project team, in their study, recommended that the ICO aim for a “structured and timetabled roll-out” of PIAs, encouraging organisations to develop internal expertise in PIA processes.¹⁵

A quarter century of increasingly rigorous UK data protection legislation has encouraged the development of strong networks of knowledgeable data protection officers (for example, NADPO¹⁶ and the Data Protection Forum¹⁷), creating regular opportunities for cross-organisational learning. There is also a long history of developing codes of practice within related sectors through umbrella groups (for example, ACPO¹⁸ and the CCTV User Group¹⁹). In theory, such groups could have influential roles in the introduction and promotion of PIAs.

Legislation

Since 1984, the UK has had overarching data protection legislation covering both public and private sectors. The most recent iteration, the Data Protection Act 1998 (DPA 1998), implemented the EU Data Protection Directive (95/46/EC). This extended the prior regime under the Data Protection Act 1984 to include, amongst other changes, extension of coverage to manual files; creation of a new category of sensitive personal data, subject to more rigorous processing preconditions; additional security requirements; increased, and stronger, rights for individual data subjects; and the prohibition of transfers of personal data to countries outside the European Economic Area, subject to certain conditions being satisfied.²⁰

At the European level, Art. 20 of the Data Protection Directive requires that processing operations likely to present specific risks to the rights and freedoms of data subjects should be examined prior to their start, an intervention described as “prior checking”:

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.
2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.
3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

S. 22 of the DPA 1998 provides for a version of prior checking by requiring that, as part of the notification process, certain processing might be assessed by the ICO for compliance with the provisions of the Act before the processing begins. The type of processing must be specified in an Order made by the Secretary of State, if it is considered that processing would be particularly likely to cause substantial damage or substantial distress to data subjects or otherwise significantly to prejudice the rights and freedoms of data subjects. While the UK government identified three possible categories of processing that might be covered by such “preliminary assessment” (data

¹⁵ ICO, *Privacy Impact Assessments: international study...*, op. cit., fn. 5, p. 31.

¹⁶ National Association of Data Protection Officers. <http://www.nadpo.org.uk/>

¹⁷ Data Protection Forum. <http://www.dpforum.org.uk/>

¹⁸ Various iterations, most recently: ACPO, *Guidance on the Management of Police Information*, Second Edition, 2010. <http://www.acpo.police.uk/asp/policies/data/MoPI%202nd%20Ed%20Published%20Version.pdf>

¹⁹ CCTV User Group *Model Code of Practice and Procedures Manual*, 2002. <http://www.cctvusergroup.com/index.php>

²⁰ Charlesworth, Andrew, “Implementing the European Union Data Protection Directive 1995 in UK law: The Data Protection Act 1998” *Government Information Quarterly*, Vol. 16, No. 3, 1999, pp. 203-240.

matching, processing involving genetic data and processing by private investigators), to date, no such order has been made in the UK. Indeed, Elizabeth France, while Information Commissioner:

...was of the opinion that “no ‘assessable processing’ should be designated”, i.e. that no processing operations should be made subject to a prior assessment at all.²¹

This rejection of prior assessment likely stemmed from the lack of necessary in-house technology expertise at the ICO which would have been required in order for such ‘prior assessments’ to have constituted a meaningful oversight mechanism. Other EU Member States have adopted prior checks for particular types of processing relating, for example, to sensitive data, offences and criminal convictions, and genetic data.²²

Previous research undertaken for the ICO²³ suggested that the UK should reconsider its position on prior checking. It is possible that wider use of PIAs could form part of such a process as they would:

- facilitate the process of prior checking by allowing the supervisory authority to draw upon the results of PIAs incorporated into organisational processes, such as risk assessments for new or redesigned projects;
- broaden the pool of organisational privacy understanding and expertise such that organisations will be more readily aware of the need for prior checking when it is appropriate, and better able to supply the supervisory authority with appropriate information about the project or process for an appropriate prior-checking assessment or decision to be made efficiently.

It is clear, however, that while supervisory authority prior checking in specific circumstances may be provided for in the UK data privacy regime, it is not in itself synonymous with the PIA process, as currently understood.

Thus, while they are capable of supporting a legislated (if largely unused) prior **assessment** process, PIAs themselves have no statutory footing in the UK, and thus cannot be made a legally mandated process for either the public or private sector, without further legislative enactment. However, as in other jurisdictions, recent developments in the UK have resulted in a requirement being placed on some parts of the public sector (and anecdotally it appears, indirectly on quasi-public and private organisations exercising public sector functions) to adopt PIAs, as a required element of internal project development processes.

Policy

Although the introduction of PIAs into the UK was primarily promoted by the production of the ICO-commissioned handbook, further impetus was added by a number of data handling scandals involving public and private sector organisations.²⁴ Arguably the highest profile incident, the loss of 25 million child benefit records by HM Revenue and Customs, resulted in a Cabinet Office review. The resulting report, *Data Handling Procedures in Government* (the “Data Handling Review”), mandated the use of PIAs in central government departments from July 2008. The Data Handling

²¹ Foundation for Information Policy Research (FIPR), *Children’s Databases – Safety and Privacy: A Report for the Information Commissioner*, March/August 2006, p.187.

<http://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf>

²² ICO, *Privacy Impact Assessments: international study...*, op. cit., fn. 5, Appendix H, pp. 5-9. See also Chapter 4 of this book: Le Grand, Gwendal, Emilie Barrau and Florence Raynal, “Prior checking, a forerunner to privacy impact assessments”.

²³ FIPR, op. cit., fn. 21.

²⁴ Private sector data losses included bank and insurance details by a number of financial institutions. See, for example, the Financial Services Authority report, *Data Security in Financial Services*, April 2008.

http://www.fsa.gov.uk/pubs/other/data_security.pdf

Review drew attention to the benefits of this process, stating the ICO had made “a powerful case” for government to adopt PIAs, which, if carried out at an early stage

enable organisations to anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions. Risks can be managed through the gathering and sharing of information with stakeholders. Systems can be designed to avoid unnecessary privacy intrusion, and features can be built in from the outset that reduce any impact on privacy. The Privacy Impact Assessment adopts a risk management process approach, periodic reports from which [Privacy Impact Assessment Reports] may be published or distributed to stakeholders.²⁵

In addition, the review called for the process to be built into existing government reviews of information and technology projects.²⁶ The ICO has incorporated this advice into its own policy approach, eschewing the production of templates and instead encouraging organisations to “embed” PIAs within existing processes, for example, when seeking information assurance accreditation or engaging on public consultations.²⁷

In this context, PIAs support accountability, efficient management and effective incorporation of risk assessments into key decision-making processes. In the private sector, further motivations may be at play, for example, conferring competitive advantage, demonstrating legal compliance, saving money and preventing adverse publicity. In short, PIAs can be regarded as more beneficial to organisations than to individuals. The need to convince agencies and businesses that they are the right thing to do for “business” reasons trumps the ostensible goal of protecting and advancing privacy rights.²⁸

3. The UK PIA process

The UK PIA process is outlined in the ICO handbook, updated in June 2009.²⁹ As the size of projects and the degree of privacy risk involved vary enormously, the ICO guidance seeks to direct organisations to conducting the most appropriate level of assessment. The processes consist of the following:

Process	Action
Initial assessment	Examines the project at an early stage, identifies stakeholders, assesses privacy risks and decides whether a PIA is necessary and, if so, what level of PIA is required.
Full-scale PIA	An in-depth internal assessment of privacy risks and liabilities, consisting of five phases usually conducted in sequence. They include the following: <ul style="list-style-type: none">i. Preliminary: establishes and ensures a firm basis for the PIA, so that it can be conducted effectively and efficiently.ii. Preparation: makes the arrangements needed to enable the following phase (i.e., consultation and analysis) to run smoothly.iii. Consultation and analysis: identifies problems early on, discovers effective

²⁵ Cabinet Office, *Data Handling Procedures in Government: Final Report*, Cabinet Office, London, 2008, p.19. <http://www.cabinetoffice.gov.uk/media/65948/dhr080625.pdf>

²⁶ Known as the “Gateway”, the review process is managed by the Office of Government Commerce. It delivers a “peer review” in which independent practitioners from outside the programme and project examine its progress and the likelihood of successful delivery. http://www.ogc.gov.uk/what_is_ogc_gateway_review.asp

²⁷ Telephone conversation with ICO representative, July 2010.

²⁸ For a more in-depth discussion of privacy policy and governance, see Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge, MA, 2006.

²⁹ ICO, *Privacy Impact Assessment Handbook: Version 2.0*, Information Commissioner’s Office, Wilmslow, 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

	<p>solutions and ensures that the design is adapted to include those solutions.</p> <p>iv. Documentation: documents the PIA process and the outcomes and delivers a PIA report.</p> <p>v. Review and audit: ensures that the undertakings arising from the consultation and analysis phase are actually within the running system or implemented project.</p>
Small-scale PIA	Similar to a full-scale PIA, but less formalised and requires less exhaustive information-gathering and analysis and usually focuses on specific aspects of a project.
Privacy law compliance check	Examines compliance with statutory powers, duties and prohibitions in relation to the use and disclosure of personal information.
Data protection compliance check	Checks for compliance with the Data Protection Act of 1998. An organisation usually conducts this check when the project is more fully formed.

Table 1: UK PIA process: an overview

To be effective, a PIA needs to be conducted at a stage where it can “genuinely affect the development of a project”³⁰. It therefore needs to be seen as a separate process from compliance checks or data protection audits, both of which comprise analyses of systems already in place “against a prevailing legal, management or technology standard”³¹. Conversely, a PIA aims to prevent problems arising, and hence to avoid subsequent expense and disruption.³² The ICO advises that responsibility for PIAs be placed at a senior executive level – ideally, the lead for risk management, audit or compliance – in order to reflect the strategic importance of the exercise. The guidance recommends a team or committee approach, with the PIA usually conducted by a senior member of the project team. This can include, with varying degrees of participation, the following personnel:

- Programme and project managers
- Privacy policy advisors
- Legal advisors
- Records management staff
- Information technology or data security experts
- Communications staff
- Other functional specialists, as appropriate.³³

Examples of PIAs conducted in the UK are outlined in Table 2, below.

Organisation	Project / procedure assessed	Type of PIA
UK Anti-Doping (2010 ³⁴)	The disclosure of personal data to UK Anti-Doping by the Serious Organised Crime Agency	Small-scale
Northern Ireland Statistics and Research Agency (NISRA) (2010)	2011 census for Northern Ireland	Full-scale
Office for National Statistics (ONS) (2009)	2011 census for England and Wales	Full-scale
UK Border Agency (2009)	Exchange of fingerprint information with immigration authorities in Australia, Canada, United States and New Zealand	Small-scale

³⁰ Ibid., p. 3.

³¹ ICO, *Privacy Impact Assessments: international study...*, op. cit., fn. 5, p. 1.

³² ICO, *Privacy Impact Assessment Handbook*, op. cit., fn. 29.

³³ Tancock et al., *The Emergence of Privacy Impact Assessments*, op. cit., fn. 12.

³⁴ The year in this column relates to the year of publication of the PIA report.

National Policing Improvement Agency (2009)	Electronic exchange of police intelligence across England and Wales via the Police National Database	Full-scale
---	--	------------

Table 2: PIAs conducted in the UK

Some organisations employ external consultants to carry out a PIA, either because they believe that they do not possess the necessary skills in-house, or they wish the PIA to be perceived as being as independent as possible from potential influences within the organisation. Some examples are outlined in Table 3, below.

Organisation	Type of privacy impact assessed	Consultancy employed
Aegate (Pharmaceutical authentication services)	Use of RFID technologies to authenticate prescription pharmaceuticals at the point of sale	Enterprise Privacy Group
Department for Transport	National time-distance-place road pricing policy ³⁵	Enterprise Privacy Group
Phorm Inc.	Behavioural targeted advertising	80/20 Thinking Ltd

Table 3: Examples of PIAs outsourced to consultants

External consultants often bring considerable experience to the PIA process, lending impartiality to the process. They can offer frank advice when initiatives are deemed to be unwise or ill-conceived, and tend to have greater expertise and familiarity with relevant legislation.³⁶ Yet, there are disadvantages. Smaller organisations may find them prohibitively expensive. Moreover, there is scepticism about consultants using “cookie cutter” PIAs whereby the same templates are used for vastly different clients.³⁷ There is also a risk that organisations will seek to use external consultants to attempt to “legitimise” controversial projects or applications. For example, a “PIA” conducted in 2008 by the consultancy group 80/20 Thinking Ltd for Phorm, a company specialising in targeted online advertising, generated considerable debate among privacy experts, and in sections of the mainstream media, about the motivations behind the exercise.³⁸ In practice, the exercise undertaken by 80/20 Thinking Ltd cannot be accurately described as a PIA, given that the technology and its applications were already fully developed and in use in business operations, and Phorm was clearly seeking to retrospectively validate those applications rather than to establish any potential impact on privacy with an eye to proactive mitigation. A more accurate description of the exercise undertaken would thus be a privacy audit or compliance check.³⁹

We will now consider the processes involved in the conduct of a PIA at the Office for National Statistics (ONS), which is responsible for producing official statistics and conducting surveys on behalf of the UK government.

4. Case study: Office for National Statistics (ONS), 2011 census

The ONS, as the executive arm of the UK Statistics Authority, is responsible for conducting the census in England and Wales. Scotland and Northern Ireland are subject to separate censuses carried out by their devolved agencies. The census is compulsory throughout the UK, and is

³⁵ In this system of road pricing, vehicle owners are charged based on when, where and how much they drive.

³⁶ ICO, *Privacy Impact Assessments: international study...*, op. cit., fn. 5.

³⁷ Ibid.

³⁸ See, for example, Arthur, Charles, “Simon Davies (of Privacy International, and 80/20 Thinking) on Phorm“, Technology Blog, *The Guardian*, 20 March 2008.

<http://www.guardian.co.uk/technology/blog/2008/mar/20/simondaviesofprivacyintern>. See also BBC News, “Phorm needs ‘better protection’”, 18 March 2008. <http://news.bbc.co.uk/1/hi/technology/7303426.stm>

³⁹ 80/20 Thinking Ltd., op. cit., fn. 9.

conducted every 10 years. The next survey is due to be carried out in 2011 and, according to the ONS, the data collected will be used “solely for the production of statistics and statistical research”⁴⁰. The legal basis for conducting a national census was established by the Census Act 1920. This is supported by the Census Order (directing that a particular census of the population shall be taken) and Census Regulations (covering procedural and practical arrangements for the census). Both the Order and the Regulations are laid before both Houses of Parliament.⁴¹ The census provides three broad categories of information:

- Counts of population units – people, households and dwellings;
- Population structures – e.g., family and household relationships, ethnic groups;
- Population and housing characteristics – e.g., health, employment and qualifications.⁴²

As these statistics are published for small population groups (down to approximately 125 households or 250 people) and are cross-tabulated with other variables, effective privacy safeguards governing the collection and use of personal data are paramount. Accordingly, publication of the results of the census is subject to additional statutes including the DPA 1998 and the Statistics and Service Registration Act 2007. This legislative framework is supported by a detailed procedural review, undertaken by the ONS over the last four decades, of the methods and processes underpinning each census.⁴³ Thus, the review process prior to the 2011 census commenced in 2002 by posing the question: “Is there a need for another census?”. Once that question was answered in the affirmative, preparations began in earnest, with a series of consultations over the census design (to ensure accurate population counts, maximise overall response, provide high quality statistics) and questionnaire content (so that it produced useful outputs, catered for small population groups, served the UK as a whole). As a result, the ONS were fully cognisant of the process-orientated approach advocated in the ICO's PIA handbook. As the internal processes assessing the 2011 census were well advanced by the time the handbook was published in 2007, the ONS conducted its “PIA” on work that had largely been done. Although this approach runs counter to the prospective nature of the PIA, it is nevertheless instructive to follow the processes enacted by the ONS as it sought to identify privacy risks inherent in conducting the census, and develop solutions to “accept, mitigate or avoid them”⁴⁴.

Perhaps the greatest difficulty encountered by the ONS was in locating appropriate expertise on PIAs. Following the ICO's publication of the PIA handbook, and its subsequent promotion of the tool, the ONS met with representatives from the data protection regulator during 2008 and 2009. These meetings could be deemed successful in that they reinforced the need for the ONS to build on its existing internal review process to consider, in greater detail, new arrangements for the 2011 census compared with the 2001 census; highlight any changes that raised new privacy concerns; and describe the safeguards put in place to protect the privacy of all census respondents.⁴⁵ Moreover, the ONS was clearly persuaded during these discussions that it “had little choice” but to conduct the PIA. It immediately elected for the full-scale PIA (without considering the screening process outlined in the handbook) as (i) the census programme was “so important” and (ii) it “would be expected” of them. Yet, although the ONS found the PIA handbook to be helpful, especially in

⁴⁰ ONS, *Report of a Privacy Impact Assessment conducted by the Office for National Statistics in relation to the 2011 Census England and Wales*, Office for National Statistics, London, 2009, p. 4.

<http://www.ons.gov.uk/census/2011-census/2011-census-project/commitment-to-confidentiality/privacy-impact-assessment--pia--on-2011-census.pdf>

⁴¹ The National Assembly for Wales is consulted in the making of any Census Order. Moreover, Welsh Ministers are now responsible for the Regulation in Wales.

⁴² ONS, *op. cit.*, fn. 40, p. 4.

⁴³ Much of the information in this section is based on a telephone conversation with an ONS representative (August 2010).

⁴⁴ ONS, *op. cit.*, fn. 40, p. 6.

⁴⁵ *Ibid.*, p. 5.

outlining the processes to be enacted and requiring it to check legal compliance, it was unable to make contact with anyone with direct experience of conducting PIAs in the UK. The handbook “contained a lot of processes but did not tell [the ONS] what to do”⁴⁶. This proved to be the greatest stumbling block. In the absence of a referral from the ICO, exemplar PIA reports conducted by other UK government departments or a list of approved consultants with suitable expertise, the ONS resorted to consulting PIA reports conducted by public bodies in New Zealand and the United States.⁴⁷ At the time, there appeared to be a clear PIA “skills gap” within UK organisations and a need for PIA processes to be incorporated within the professional training of those responsible for leading the assessment, for example, through the Managing Successful Programmes, a project management course taught at the UK’s National School of Government.

In addition, the ONS expressed disappointment with the response to its stakeholder consultation. In spite of receiving a list of civil society organisations from the ICO, and issuing direct invitations to these and related bodies, representatives from only two groups attended the consultation event (with another individual contributing via e-mail) and neither provided particularly meaningful feedback. This experience suggests the need for a clearer, more consistent process for ensuring wider societal engagement with PIAs, particularly in the early stages of projects. This could be achieved through more innovative means of publicising ongoing PIAs, possibly via a dedicated portal or one-stop shop. This would raise the profile of PIAs, particularly if organisations are also encouraged to publish Plain Language PIA reports, and increase the obligation for civil society groups to participate in policy processes affecting citizens’ personal privacy.

On the whole, the ONS reported that conducting the PIA process did not cause it to uncover anything “unexpected” in its approach to the 2011 census. In part, this may be due to its existing adherence to a series of rigorous, well-established rolling consultation processes in preparation for each upcoming census. Nevertheless, the PIA did prove helpful in “pulling together” various strands of the ONS’s work and providing further evidence (through publication of a PIA report) that, as an organisation, it was taking privacy seriously. This was reflected in the section in the ONS PIA report relating to the legal basis for the 2011 census, which was stated to owe the most to the ICO PIA handbook.⁴⁸ Finally, the ONS was conscious of the largely retrospective nature of the PIA conducted. In some respects, this was unavoidable due to the PIA handbook being published so far into the ONS’s own internal review process for the 2011 census. Nevertheless, the ONS stated that, with hindsight, it would have consulted with the ICO and engaged with stakeholders at a much earlier stage in process, recognising that there is little point in involving these groups unless they have a realistic opportunity to alter the design and implementation of the project.

5. Lessons learnt

In the report commissioned by the ICO⁴⁹, it was noted that PIAs were generally perceived to be more effective when

- they offer a prospective identification of privacy risks *before* systems and programmes are put in place;
- they assess the proposed initiatives within a framework which takes into account the broader set of community values and expectations about privacy;

⁴⁶ Telephone conversation, ONS representative, August 2010.

⁴⁷ The ONS representative was aware of a PIA report conducted by the Department of Finance and Personnel in Northern Ireland. However, it related to a vastly different topic – a review of domestic rating systems, with a view to encouraging various groups to take up domestic rate reliefs. See – Department of Finance and Personnel (Northern Ireland), *Review of Domestic Rating Data Sharing Privacy Impact Assessment (PIA)*, Bangor, 2008.

⁴⁸ Telephone conversation, op. cit., fn. 46.

⁴⁹ ICO, *Privacy Impact Assessments: international study...*, op. cit., fn. 5, pp. 29-30.

- they refer to an entire process of assessment of privacy risks rather than a statement or end-product;
- they have, and are perceived to have, the potential to alter proposed initiatives in order to mitigate privacy risks;
- their scope and depth are sensitive to a number of crucial variables: the size of the organisation, the sensitivity of the personal data, the forms of risk, the intrusiveness of the technology;
- they are part of a system of incentives, sanctions and review, and/or where they are embedded in project workflows or quality assurance processes, as is common with other forms of risk assessment;
- the individuals charged with completing PIAs not only have good programme knowledge, but also have access to multidisciplinary expertise from a variety of perspectives – privacy law and practice, information security, records management and other functional specialists as appropriate;
- the PIA tool is accessible, readily available and easy to access, and the process involved is flexible;
- there is a process of formal or informal external review either by central agencies or privacy oversight bodies;
- there is a strong advocacy role played by the relevant oversight body;
- there is external consultation with outsiders affected by the initiative. Public consultation is often advised;
- there is transparency, and the resulting statements or reports are published. Openness of process and output enhances trust in the initiative being proposed.

Some initial observations on these points from the UK context can be made. The available evidence suggests that ICO has clearly worked very hard, both in public and behind the scenes, to promote the use of PIAs; to seek and utilise feedback to make the handbook more user friendly; and to encourage government agencies which have undertaken PIAs to make their reports public. The focus of the ICO's work has been government, and it appears that there has been relatively little interaction with the private sector. Criticism could perhaps be levelled at the ICO with regard to the review of Phorm's business undertaken by 80/20 Thinking Ltd. (see above), where a clear public statement why an *ex post facto* review of an existing business practice should not be viewed as a PIA would have been useful, but was not forthcoming. The Phorm example also suggests that there was, initially at least, a paucity of expertise on PIAs available to organisations wishing to undertake them, and that this, depending on one's perspective on that particular instance, could mean that an organisation might misunderstand the purpose of the process, or might cynically seek to mischaracterise it. The last three years have seen a considerable upturn in consultants claiming PIA expertise, and organisations such as the Enterprise Privacy Group have been instrumental in helping government departments tackle PIAs for complex and potentially controversial projects.

In terms of guidance, the Ministry of Justice is responsible for advising government departments, and has recently published a short guidance document on handling PIAs.⁵⁰ However, the Ministry of Justice does not itself review departmental PIA processes or reports, and may not be informed when PIAs are undertaken. As such, detailed data protection responsibilities, including establishing PIA processes, are routinely devolved to individual departments. There does not currently appear to be any central co-ordination of officials or civil servants with PIA experience across government departments; any central guidance as to the type of projects that would fall within the "mandatory" PIA requirement; or any central guidance on appropriate or approved consultants. Based on the experience of organisations in other jurisdictions, particularly the Canadian federal jurisdiction, it seems likely that there will continue to be a PIA skills gap both within UK organisations and in the

⁵⁰ Ministry of Justice, *Undertaking Privacy Impact Assessments: The Data Protection Act 1998*, London, 2010.
<http://www.justice.gov.uk/guidance/docs/pia-guidance-08-10.pdf>

consultancy market going forward. Encouraging departments to share PIA tools, templates and frameworks across government will help to overcome that gap and hasten the spread of PIA good practice and innovation.

The UK has no formal process of external review by central agencies or by the ICO. As noted above, the ICO has played a key advisory role, but would unlikely be able to take on a formal scrutiny role, at least in the form the regulator currently takes. As a result, its role has been primarily in advising on methodology and helping organisations to embed PIA processes in existing practices. Following the Data Handling Review, the Cabinet Office has responsibility for monitoring the use of PIAs in government, although it is not clear exactly how it intends to carry out this monitoring and/or enforcement role. As such, there is insufficient evidence at present to determine whether or not the ad hoc processes of review currently in place are, or will be, effective at ensuring that government agencies fully engage, or engage effectively, with the PIA process. While any move to a mandatory review of PIAs is highly unlikely, a requirement that government departments provide notification and/or submission of outputs including PIA reports to either the Cabinet office, or the ICO, would facilitate oversight by allowing them to request and review selected PIAs of particular interest, and to engage in more targeted departmental, sectoral or government-wide compliance audits.

The focus on departmental responsibility, the apparent lack of PIA cross-fertilization across departmental boundaries, and what appears to be relatively “hands-off” oversight raise questions about the current ability of governmental PIA processes to deal with privacy issues at a strategic level. In other words, how would a department approach a decision to create or adapt a system or policy, which arises from the actions of a higher level of government, e.g., the Executive or Parliament, or a decision where the carrying out of policy requires inter or multi-departmental input? For example, the policy behind plans to share data across government departments in the UK may come from the Executive, and require implementing measures across a number of departments. If each department is responsible for its own PIA process, then there is a risk that privacy failures that arise directly from the Executive decision, or from issues that are not the specific responsibility of any one department, are not appropriately addressed. Another problem may arise where the cumulative effect of programmes initiated by different departments upon the individual are not addressed. For example, Department A seeks to initiate a project involving an individual’s personal data. Before doing so, they carry out a departmental PIA. Their PIA alerts them to the privacy risks for individuals of their particular project but, in the absence of knowledge about projects in other Departments, may not take account of the cumulative risk posed by that collection in combination with the collections of personal information by Departments B, C and D.

Although the value of “inward-facing” use of PIAs to inform management risk assessments appears to be increasingly established, at least in government agencies, the use of PIAs for “public-facing” activities seems much less developed. This may be due to the fact that the ICO has emphasised the self-assessment nature of PIAs, with the focus on process and not on generating documentation for public review. Currently, obtaining information about the conduct of PIAs, or information relating to specific PIA outcomes, is far from easy. There may well be “over 300 Privacy Impact Assessments ... started across central government and their agencies”⁵¹, but there is little evidence of that activity available to the public. Equally, it appears that the paucity of PIA-related information and reports is depriving other government agencies of a potentially valuable source of information, which may result in departments having to “reinvent the wheel” when setting up PIA processes. There are some publicly available PIA reports, for example:

- The UK Border Agency’s PIA report on the exchange of fingerprint information with immigration authorities in Australia, Canada, New Zealand and the United States (38 pages) is

⁵¹ ICO, *Information Commissioner’s Annual Report 2009/10*, op. cit., fn. 7, p. 23.

readily available from their website, and it is clearly envisaged that continuing public feedback will be part of the “evergreening” process for the document, i.e. it is intended that the document will be used as a focus for ongoing privacy evaluation⁵²;

- The National Policing Improvement Agency’s PIA report on the Police National Database (42 pages) is available from their website, and was published with the intent that it might stimulate further input, as the initial PIA process received “a low number of responses” from a “narrow range of organisations”⁵³;
- The Office for National Statistics’ PIA report on the 2011 Census in England and Wales (62 pages) is available from their website. This report is less obviously geared towards continuing public engagement, possibly due to the ONS’s existing policy of engaging in ongoing consultation on the census⁵⁴.

But these examples seem to be the exception rather than the rule across government. While it is possible that information on ongoing and completed PIAs could be obtained by the public via freedom of information requests⁵⁵, the apparent reluctance on the part of government agencies to promote and disseminate their PIA outcomes would seem to run counter to the public engagement ethos that underpins the ICO’s initiatives.

In the public sector, more thought needs to be given to developing a coherent approach to PIA consultation and dissemination. A key weakness in other jurisdictions has been the generally unstructured approach to these issues. At present in the UK, as elsewhere, there is:

- no consistent process for ensuring effective consultation with stakeholders, notably the general public, e.g., a register of ongoing PIAs, consultation periods and relevant contact details;
- no consistency in reporting formats for PIAs, whether in draft or completed, e.g., a PIA might be reported in a detailed 62-page document, or simply mentioned in a paragraph in a general impact statement⁵⁶; and,
- no strategy for ensuring that where PIA decisions and reports are made publicly available, that they are easily accessible, perhaps from a centralised point, e.g., the UK Office of Public Sector Information (OPSI) or the ICO.

If the public are unaware of consultations, are unable to effectively parse reports or compare the relative quality of reports from different agencies, or are unable to easily access reports, then poor public engagement and ineffective tripartite regulation of agency practices (i.e. through the interaction of regulator, regulated, and public or public representative bodies) of agency practices are almost inevitable.

The issues raised above are not exclusive to the UK experience of PIAs. In fact, they are virtually all issues that have arisen in other jurisdictions, enhanced in some cases by the peculiarities or particularities of the UK governmental and regulatory systems. Nor are these issues insurmountable,

⁵² UKBA, *Report of a Privacy Impact Assessment conducted by the UK Border Agency in relation to the High Value Data Sharing Protocol amongst the immigration authorities of the Five Country Conference*, UK Border Agency, London, 2009.

⁵³ NPIA, *Police National Database – Privacy Impact Assessment Report*, National Policing Improvement Agency, London, 2009.

http://www.npia.police.uk/en/docs/Privacy_Impact_Assessment.pdf

⁵⁴ ONS, op. cit., fn. 40.

⁵⁵ Subject, of course, to the wide exemptions granted to government departments in the FOI Act 2000.

⁵⁶ See, for example:

- Department of Communities and Local Government, *Making better use of energy performance data: Impact Assessment*, Consultation, March 2010.
<http://www.communities.gov.uk/documents/planningandbuilding/pdf/1491281.pdf>
- Department for Transport, *Impact Assessment on the use of security scanners at UK airports*, Consultation, March 2010. <http://www.dft.gov.uk/consultations/closed/2010-23/ia.pdf>

although overcoming them will likely involve a considerable degree of political will, careful administrative co-ordination and thoughtful public engagement.

6. Future developments

We would be on rather firmer ground when assessing the future of PIAs in the UK if there was greater certainty about the situation in the present. However, there are several potential drivers that could significantly influence the future role and scope of PIAs:

- The international drive for data privacy mechanisms that encourage proactive regulation via targeted and appropriate systems of accountability;
- The influence of globalisation, combined with jurisdiction-dissolving technologies, such as the World Wide Web, social networking tools and cloud computing;
- The interest of the private sector in creating and using systems to facilitate accountability and compliance.

It is no secret, as noted in the Introduction above, that there is dissatisfaction with the current EU data privacy framework. Both the UK ICO⁵⁷ and the European Commission⁵⁸ have recently produced reports examining possible future developments in the EU approach to data privacy. One heavily promoted approach is the concept of “privacy by design”, defined as “the philosophy and approach of embedding privacy into the design specifications of various technologies”⁵⁹. Privacy by design (PbD) is premised on several key principles, notably:

1. Recognition of the core privacy principles as the default position in a system or process;
2. Recognition of the organisational benefits of addressing privacy interests and concerns proactively and pre-emptively;
3. Early mitigation of privacy concerns when developing IT systems and business practices, throughout the entire information life cycle;
4. Embedding of privacy as a core component in the design and architecture of IT systems and business practices, so as to enhance both privacy and system functionality;
5. Keeping the interests of the individual uppermost by offering strong privacy defaults, appropriate notice and empowering user-friendly options such as privacy-enhancing technologies (PETs);
6. Business practices and technologies should be operated according to stated promises and objectives, and subject to independent verification;
7. Knowledge of the organisation and of the related privacy sub-domains (legal compliance, technology, business operations, customer relations) is critical and requires qualified leadership and professional input.

As such, PbD as a philosophy appears very much in tune with the light-touch approach that the UK ICO has tended to adopt as a regulator (although the lack, until recently, of a “big stick” may have played a role in this), and the ICO has already indicated support for the PbD approach. Creating a regulatory system premised on PbD would be simpler if PIAs were to have already become a familiar part of the UK data privacy regime, not least because there would be a greater pool of expertise and organisational and technical support to draw upon. Such a regime would also be

⁵⁷ Robinson, N., H. Graux, M. Botterman and L. Valeri, *Review of the European Data Protection Directive*, Information Commissioner's Office, Wilmslow, 2009.

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf

⁵⁸ Korff, D., and I. Brown, *Different Approaches to new Privacy Challenges in particular in the Light of Technological Developments*, European Commission, DG Justice, Freedom and Security, Brussels, 2010.

http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

⁵⁹ OPIC, op. cit., fn. 1.

attractive to organisations seeking to utilise developing information technologies such as cloud computing.

Cloud computing is essentially Internet-based computing, whereby a large pool of easily usable and accessible virtualised resources (such as hardware, development platforms and/or services) can be dynamically reconfigured to adjust to a variable load (scale), allowing for an optimum resource utilisation.⁶⁰

While cloud computing technology is potentially extremely cost effective, the nature of the technology means that a data controller processing personal data “in the cloud” will often:

- not have control over the machine and software that is being used (outsourcing);
- not be able to control and may not know where in the world the data is being processed (offshoring);
- not be the sole user of the hardware, platform or service (multi-tenancy/virtualisation);
- be in a position where they may be switched automatically between systems owned by different suppliers automatically according to demand (autonomic technology).

These features of cloud computing clearly present a significant challenge to data controllers seeking to adhere to the requirements found under current legislation, notably the restrictions on cross-border data transfer. A PbD regulatory framework underpinned by effective PIAs could be the basis for a regime based on the use of a combination of privacy policies and contractual terms to create accountability in the form of transparent, enforceable commitments to responsible data handling.⁶¹ The tools that might support such a framework are already under development, ranging from automated decision-support tools to aid organisations in undertaking effective PIAs⁶², to trusted computing tools for security and audit⁶³ and trusted virtual platforms⁶⁴. There is thus an incentive for the private sector to build upon the early work on PIAs conducted by the public sector in the UK to the potential benefit of both.

7. Conclusion

The UK Information Commissioner’s Office’s championing of the incorporation of PIAs into public and private sector management processes, via its commissioning of the initial research and the incremental development of its PIA handbook, has come at a particularly fortuitous time. A “perfect storm” of technological and business innovation, high profile and large-scale personal data leaks, and decreasing public confidence in existing data protection and privacy laws has led to increasing international interest in seeking more effective and efficient means to protect personal data and privacy. The ICO’s work has thus been at the forefront of the next generation of PIA process development, and is being drawn upon by early PIA adopters, such as the Ontario Information and Privacy Commissioner (OIPC), when they come to review their existing models and guidance. The ICO has also been keen not to rest on its laurels, with the second iteration of the

⁶⁰ Tancock, D., S. Pearson and A. Charlesworth, “A Privacy Impact Assessment Tool for Cloud Computing”, in *Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2010)*, Indiana University, USA, Nov 30-Dec 3, 2010 [forthcoming].

⁶¹ Pearson, S., and A. Charlesworth, “Accountability as a Way Forward for Privacy Protection in the Cloud”, in M.G. Jaatun, G. Zhao and C. Rong (eds.), *CloudCom 2009: Proceedings*, Lecture Notes in Computer Science, 5931/2009, Springer, 2009, pp. 131-144.

⁶² Tancock et al., op. cit., fn. 60.

⁶³ Pearson, S., “Trusted Computing: Strengths, Weaknesses and Further Opportunities for Enhancing Privacy, Trust Management” in Peter Herrmann, Valérie Issarny and Simon Shiu (eds.), *iTrust 2005, Proceedings*, Lecture Notes in Computer Science, 3477/2005, Springer, 2005, pp. 305-320.

⁶⁴ Dalton, C., D. Plaquin, W. Weidner, D. Kuhlmann, B. Balacheff and R. Brown, “Trusted virtual platforms: a key enabler for converged client devices”, *Operating Systems Review*, Vol. 43, No. 1, 2009, pp. 36-43.

PIA handbook appearing after only two years as the ICO seeks to draw upon and incorporate feedback from its users.

In terms of adoption of PIAs, it appears that this has primarily, if not exclusively, occurred in the public sector, as a result of the post-Data Handling Review policy. Whilst some private sector companies do engage in PIA-like processes, in general, the private sector has up till now shown little enthusiasm for the ICO's handbook. Examples from other jurisdictions (e.g., the Royal Bank of Canada) suggest that the process envisaged in the handbook is considerably more detailed than current private sector requirements.

To the outside onlooker, the PIA picture within the public sector appears still to be fragmented and confused. In contrast to the activities of the ICO, the Cabinet Office and Ministry of Justice have been slow to establish a framework to enable departments to plan, conduct and review PIAs in a manner which is consistent across government. This is problematic on two levels. First, the current situation appears to be an inefficient use of government resources, with departments apparently unable to draw effectively upon each other's prior experience and outputs. Second, if there is a lack of cross-governmental communication regarding PIAs, then their use as an effective mechanism for strategic review of privacy risks is signally decreased.

Given the relative paucity of evidence currently available, it is difficult to provide a clear assessment of the state of play with regard to PIAs in the UK. The apparently inward-facing nature of the majority of PIAs suggests that, as with PIAs in some other jurisdictions, e.g., those carried out within the Ontario provincial government, PIAs are going to be used primarily as risk assessment tools. If this becomes the primary function of UK PIAs, then it is likely that the UK will fail to capture the wider public benefits of more open PIA processes.

It is particularly important that organisations carrying out PIAs are not discouraged by low response rates to, or lack of wide public engagement with, early stage PIAs. Previously, the public have had no great expectation of consultation in many areas covered by PIAs, so it is unsurprising that current participation is limited. Wider availability of user-friendly PIA reports, combined with innovation in public engagement strategies should, over time, create a greater expectation amongst the public of involvement in policy decisions which affect their privacy. Seeking more extensive public engagement in both consultation and dissemination may also help to prevent PIAs from devolving into yet another administrative "box-ticking" exercise.