Project acronym:	SAPIENT
Project title:	Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies
Project number:	261698
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2010.6.5-2: Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules
Contract type:	Collaborative project
Start date of project:	1 February 2011
Duration:	36 months

Deliverable 3.1:
Privacy Impact Assessment and Smart Surveillance: A State of the Art Report

Authors:	David Wright (Trilateral Research & Consulting); Raphaël Gellert, Rocco Bellanova, Serge Gutwirth (VUB-LSTS); Marc Langheinrich (University Lugano), Michael Friedewald, Dara Hallinan (Fraunhofer ISI); Silvia Venier, Emilio Mordini (CSSC)

Dissemination level:	Restricted to a group specified by the consortium (including the Commission Services)
Deliverable type:	Report
Version:	1.0
Due date:	28 February 2013
Submission date:	17 May 2013

About the SAPIENT project

The SAPIENT project that is expected to provide strategic knowledge on the state of the art of surveillance studies, emerging smart surveillance technologies, and the adequacy of the existing legal framework. In addition to addressing these core research goals, the project will entail the development and validation of scenarios around future smart surveillance systems, and will apply the best elements of existing PIA (privacy impact assessment) methodologies to construct a surveillance related PIA framework.

The work of the project will lead to a practical handbook which will help policy makers, technology developers and other stakeholders to better understand how and when smart surveillance should be used, and apply criteria to assure that such systems respect the privacy of citizens.

Terms of use

Suggested citation: David Wright et al., "Privacy Impact Assessment and Smart Surveillance: A State of the Art Report", Deliverable 3.1, SAPIENT Project, May 2013.

Document history

Version	Date	Changes
0.9	30 January 2013	Draft Version
1.0	17 May 2013	First Version

EXECUTIVE SUMMARY

OBJECTIVE OF THE DELIVERABLE

The main aims of D3.1 are

- To review existing privacy impact assessment (PIA) methodologies, and to determine their suitability for smart surveillance technologies;
- To extract the best elements that could be used in a PIA methodology for Europe, especially tailored for surveillance practices;
- To identify the limits and key challenges and check them against the particularities of smart surveillance.

A PIA can be defined as a

> a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. A PIA is more than a tool: it is a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after the project has been deployed.[1]

In this document, we first review existing privacy impact assessment methodologies, notably those used in Australia, Canada, France, Ireland, the Netherlands, New Zealand, the US, UK[2] and what is foreseen at the European Union (EU) level, to determine their suitability as a means (1) to verify that surveillance systems and the sharing of information is respecting the privacy of the citizens, (2) to limit the collection and storage of unnecessary data and (3) to find a balance between data collections needs and data protection and privacy. Some examples of PIAs targeted to surveillance technologies and applications are presented in the annex.

Second, the consortium identifies certain key features and limits of each of the existing PIA methodologies.[3] Indeed, each of the PIA methodologies has some interesting features which could be included in a PIA suitable for development and deployment of smart surveillance technologies and systems. On the other hand, it is also important to understand the present limits of already existing PIA methodologies, and to check them against the features and the challenges of present and prospective smart surveillance technologies and practices.

This documents builds on the outcomes and analyses of previous work carried out in SAPIENT, in particular, on Deliverable D1.1 the "State of the art report on smart surveillance", which identifies key elements of currently available technologies and emerging

[1] Wright, David, "The state of the art in privacy impact assessment", *Computer Law & Security Review*, Vol, 28, No. 1, Feb. 2012, pp. 54-61 [p. 55]. http://www.sciencedirect.com/science/journal/02673649.

[2] This selection is not limited to countries where the methodologies are formally labelled PIA: it also encompasses other PIA-like methodologies. This selection is linked to the need to understand the development and deployment of PIA-like measures within different institutional cultures.

[3] For example, the UK emphasises early consultation with stakeholders, including the public. Canada emphasises the need for government departments and agencies to submit a proper PIA with their funding submissions to the Treasury Board. In addition, PIAs must be forwarded to the Office of the Privacy Commissioner of Canada, who can and does audit PIAs. Canada publishes summaries of PIAs on departmental websites. US government agencies, such as the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB), are supposed to publish full PIAs on their websites (redacted as necessary).

trends[4]. It also benefits from the research and feedback received from representatives of the data protection authorities (DPAs) and other entities who are responsible for privacy impact assessment policy in their countries carried out in other projects.[5] Upon the conclusion of D3.1 and D3.2, we will seek further comments from DPAs and other stakeholders.

This deliverable will serve as the key background document for the development of a PIA methodology suitable for smart surveillance technologies and applications, which for ease of reference we call a surveillance impact assessment. Drawing on the results of this analysis, as well as of previous research carried out in SAPIENT, a set of criteria will be also identified that could be used to verify that surveillance systems and sharing of information respect the privacy of citizens, as well as other fundamental rights and ethical values.

MAIN FINDINGS OF THE DELIVERABLE

The document provides a state-of-the-art analysis of existing PIA methodologies and especially discusses their utility in dealing with the particularities of smart surveillance (see section 4.5 below). These particularities include, first, the fact that in many cases (e.g., in law enforcement applications) surveillance has security sensitivities not typically found in other issues involving data protection; second, existing PIA methodologies are especially focused on data protection, and less focused (or not at all) on the wider privacy issues related to privacy of communications (e.g., intercepts), privacy of the body (body searches), privacy of behaviour (video surveillance). In additional, surveillance may interfere with other fundamental human rights and ethical values which should be taken into considerations while analysing the impacts of these technologies or practices.

The deliverable includes an extraction of the best elements and main limits of existing PIAs and categorises a set of recommendations for a surveillance impact assessment (SIA) methodology for the EU. It should be noted that the landscape of privacy impact assessment in Europe is still in evolution, and many challenges in using such instruments in smart surveillance practices still have to be properly addressed. The interest in PIAs is growing, however, as Chapter 1 makes clear.

OVERVIEW OF THE DELIVERABLE

This deliverable is structured as follows:

Chapter 1 “Introduction” mentions the growing interest in PIA in Europe, and discusses recent developments of EU legislation on these themes. It also describes the aims and presents the structure of the deliverable. It concludes with some methodological remarks.

Chapter 2 “The origins of PIA and criteria to assess them” provides a short overview of PIA origins as an early warning device and a risk management tool, and describes the analytical framework used to assess PIAs which is built around 18 benchmarks.

Chapter 3 “Countries comparison” presents some examples of available PIAs in selected countries, and proposes a comparative analysis which aims at identifying the best elements.

[4] See Gutwirth, Serge, Rocco Bellanova, Michael Friedewald, Dara Hallinan, David Wright, Paul McCarthy, Julien Jeandesboz, Emilio Mordini, Silvia Venier, Marc Langheinrich, and Vlad Coroama, "Smart Surveillance - State of the Art Report", Deliverable 1.1, SAPIENT Project, 2012.
[5] See the PIAF project, Privacy Impact Assessment Frameworks. http://www.piafproject.eu/

Chapter 4 “Best elements and key challenges” identifies benefits as well as some limitations in relation to developing a PIA framework suitable for smart surveillance.

Chapter 5 addresses human rights issues and surveillance, including a reference to the suitability of Article 33 Data protection impact assessment in the proposed Data Protection Regulation as a modus operandi for surveillance systems and projects.

Chapter 6 contains our conclusions, including an analysis of the various PIA reports found in the Annex. Having reviewed several PIA reports from Australia, Canada, the UK and US that deal with surveillance systems, we find shortcomings in existing PIA approaches in dealing with surveillance projects, which is why a special surveillance impact assessment methodology seems justified.

CONTENTS

1 INTRODUCTION

1.1 THE GROWING RELEVANCE OF PRIVACY IMPACT ASSESSMENT IN THE EU

The European Commission has proposed a major revision to the European Union's data protection framework. The proposed Regulation, released on 25 January 2012, represents the biggest overhaul in data protection since the Data Protection Directive (95/46/EC) was adopted in 1995. The new Regulation would introduce many novelties and innovations, and it would be directly applicable in the Member States, whereas they were able to transpose the old Directive as they saw fit, which led to differences in the data protection framework from one Member State to another. There are still other important reforms, including one that relates to the SAPIENT project, i.e. the introduction of Data Protection Impact Assessment. Under Article 33 of the proposed Regulation, organisations would be obliged to conduct a "data protection impact assessment" where processing operations present specific risks to the rights and freedoms of data subjects.[1]

The Commission had already signalled its interest in privacy impact assessment (PIA) as an important instrument in the data protection toolkit well before publication of the proposed Regulation. For example, in a Communication in November 2010, the Commission said that with new technologies "ways of collecting personal data have become increasingly elaborated and less easily detectable".[2] Recognising this, the Commission launched a review of the current legal framework that came to the conclusion "that the core principles of the Directive are still valid and that its technologically neutral character should be preserved. However, several issues were identified as being problematic and posing specific challenges. These included – among others – the impact of new (surveillance) technologies.[3]

Among other things, the Commission said it would "enhance" data controllers' responsibility by "including in the legal framework an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance".[4]

As another example of PIAs becoming recognised as an official governance tool, the Commission issued a Recommendation in May 2009 in which it said that, with regard to RFID applications, "Member States should ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments".[5] Although the Article 29 Data Protection Working Party rejected industry's first attempt, it did endorse a revised framework in February 2011. In its endorsement, the Art. 29 WP said that risk management "is an essential component of any

[1] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", COM(2012) 11 final, Brussels, 2012. For a more detailed analysis of this provision, see *Infra*, Conclusion.
[2] European Commission, "A comprehensive approach on personal data protection in the European Union", COM(2010) 609 final, Brussels, 2010.
[3] Ibid.
[4] Ibid.
[5] European Commission, "Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification", C (2009) 3200 final, Brussels, 2009.

Privacy and Data Protection Impact Assessment Framework".[6] It also welcomed "the explicit inclusion of a stakeholder consultation process as part of the internal procedures needed to support the execution of a PIA".[7] The scope of that stakeholder consultation process in actual practice remains to be seen. The Art. 29 WP concludes its Opinion with the observation that "A PIA is a tool designed to promote 'privacy by design', better information to individuals as well as transparency and dialogue with competent authorities."[8]

The third example of the Commission's interest in PIA (or DPIA) is the PIAF (Privacy Impact Assessment Framework) project[9], which was commissioned by the EC's Directorate-General Justice with the task of reviewing existing PIA methodologies in those countries with the most experience in PIA, i.e., Australia, Canada, Ireland, New Zealand, the UK and the US. The purpose of the review was to identify best practice elements which should feature in a European PIA methodology. PIAF also surveyed data protection authorities in the Member States to have their views on the implementation of a PIA policy.[10]

Together with its proposal for a general data protection regulation, the European Commission also published its proposal for Police and Criminal Justice Data Protection Directive.[11] In contrast to the general Regulation, the proposed Directive does not contain a requirement to conduct data protection impact assessments. Art 26 of the draft Directive only calls on the Member States to ensure that controllers in the police and justice sector consult the supervisory authority prior to the processing of certain types of personal data (similar to the "prior consultation" provision, already foreseen in Article 23 of the Council Framework Decision covering the former third pillar). Many of the smart surveillance technologies that are in the scope of the SAPIENT project will be used for security-related applications and will thus fall within the legislative scope of the proposed Directive. Nevertheless, we deem a PIA framework to be an important element for responsible research and innovation also in this field.[12] In this sense, as discussed below, several countries already carry out PIAs on law-enforcement-related measures.

1.2 AIM AND STRUCTURE OF THE DELIVERABLE

This deliverable provides a state-of-the-art analysis on PIAs and checks this model against the features of emerging smart surveillance practices and relevant legislation at the EU level. The deliverable will serve as a background document for the development of a methodology for PIA targeted to smart surveillance, which will be presented in SAPIENT D3.2.

[6] Article 29 Data Protection Working Party, "Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications", Working Paper 00327/11/EN, WP 180, Brussels, 2011.
[7] Ibid.
[8] Ibid.
[9] http://www.piafproject.eu
[10] Wright, David, and Kush Wadhwa, "Introducing a privacy impact assessment policy in the EU Member States", *International Data Privacy Law*, Vol. 3, No. 1, 2013.
[11] European Commission, "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offencesor the execution of criminal penalties, and the free movement of such data", COM(2012) 10 final, Brussels, 25 January 2012.
[12] Wright, David, Raphaël Gellert, Serge Gutwirth, et al., "Precaution and privacy impact assessment as modes towards risk governance", in René von Schomberg (ed.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, Publications Office of the European Union, Luxembourg, 2011.

This deliverable draws on the research undertaken in the PIAF project as well as other PIA-related sources to provide a comparative analysis against 18 benchmarks of privacy impact assessment policies and methodologies used in the above-mentioned countries. Among the benchmarks or points of comparison are whether PIAs are mandatory, whether they are to be published, whether they deal with just data protection (information privacy) or include other types of privacy within their scope, whether they support consultation with stakeholders, whether they provide for third-party review or audit, and so on. The analytical framework used to assess PIA methodologies is detailed in Chapter 2 of the present document.

The PIA policies and methodologies have some strong points, but also shortcomings, as audits in Canada and the US have pointed out. Our deliverable breaks new ground by providing a comparative analysis of the key features of the PIA policies and methodologies in selected countries in order to make recommendations for construction of an optimised PIA and/or surveillance impact assessment (SIA) *process* for use within EU Member States (and elsewhere) based on the best elements of existing policies and recommendations. The comparative analysis of existing PIA methodologies is provided in Chapter 3, while best elements as well as some key challenges for the development and use of such instruments in smart surveillance practices are presented in Chapter 4.

The elements regarded as the "best" are considered as such not only by the authors, but also by other PIA experts, as will be noted (see Chapter 2). While there are differences between the *content* of a PIA addressing information privacy and a PIA specifically targeted to smart surveillance, we think the *process* of conducting each can be more or less the same. The PIAF project identified 16 steps in the PIA process[13], starting from preliminary steps such as performing a threshold analysis to determine whether a PIA is necessary, and identifying the persons involved in the development of the PIA and related budget. The PIA process includes a detailed description of the project or technology under assessment, the involvement of relevant stakeholders in the identification of risks, as well as the formulation of solutions and recommendations. In the last phase of the process, a PIA report is published and updated as necessary, and the recommendations are addressed. A third party review can be also performed as a last stage to ensure the PIA recommendations have been properly carried out.

1.3 METHODOLOGY

The concept of PIA emerged and grew *outside* Europe from about the mid-1990s, in Australia, Canada, New Zealand and US. In this deliverable, we took the decision not to limit the analysis to the most advanced experiences of PIAs around the world, including the above-mentioned countries where PIAs developed as an early warning instrument and a risk management tool particularly targeted to informational privacy. We also aimed at describing some recent PIA-like developments in European countries or at the EU Institutions level. The analysis is therefore not limited to countries where the methodologies are formally labelled PIA, but that it also encompasses other PIA-like methodologies. The final goal is to understand how the PIA model is being received in Europe, how it is evolving also in light of on-going legislative developments, and, considering SAPIENT focus, whether it is suitable for surveillance practices and technologies.

[13] Wright, David, and Kush Wadhwa, "A step by step guide to privacy impact assessment", Presentation paper for the second PIAF workshop, Sopot, Poland, 24 April 2012. http://www.piafproject.eu/Events.html

The comparative analysis of existing PIAs methodologies and identification of best elements is built on the basis of 18 criteria. A comparative assessment of the various PIA policies and practices using a set of 18 criteria derived from the PIA literature, notably papers prepared by PIA pioneers such as Roger Clarke, Blair Stewart, David Flaherty, Nigel Waters and Elizabeth Longworth, has already been made elsewhere by one of the authors of this deliverable.[14] The analytical framework used to compare PIAs base on these 18 assessment criteria is described in Chapter 2.

The assessment of the suitability of the "PIA model" for smart surveillance practices in Europe, based on the analysis of best elements as well as limitations, is made by checking this model against the features of smart surveillance (as identified in previous work carried out in SAPIENT WP1), and on current legislation and on-going legislative developments at the EU level. (See section 4.5.)

[14] Wright, David, Rachel Finn and Rowena Rodrigues, "A comparative analysis of privacy impact assessment in six countries", *Journal of Contemporary European Research*, Vol. 9, No. 1, 2013.

2 THE ORIGINS, CURRENT TRENDS AND CRITERIA TO ASSESS PIAS

The aim of this chapter is to provide a brief historical overview of the origins of PIAs, developed as a risk management tool particularly targeted at information privacy. These common roots explain PIAs as a unique conceptual object, and support the comparative analysis done in this deliverable with other PIA-like developments. Emerging surveillance technologies, however, are impacting on various types of privacy (and not just information privacy), as well as other fundamental human rights and ethical values. The view of SAPIENT is that, based on these initial characteristics, a PIA focused on surveillance should be broadened to include considerations of other types of privacy as well as of fundamental human rights and other ethical values.

The first part is devoted to tracing a short historical overview of PIAs, while the second part discusses current trends. The third section deals with the description of the analytical framework used to assess PIAs. Best elements of PIAs are pointed out to support a set of recommendations for an optimised PIA methodology for the EU.

2.1 THE ORIGINS OF PIAS

Privacy impact assessments have been used since the early 1990s. Among the early pioneers are Blair Stewart, the assistant privacy commissioner of New Zealand, Roger Clarke, a PIA consultant in Australia, Nigel Waters, formerly the deputy privacy commissioner of Australia, Elizabeth Longworth, then a consultant in Australia and now a high-ranking official at the UN, and David Flaherty, the former privacy commissioner of British Colombia. All of these PIA luminaries participated in a Privacy Issues Forum in Christchurch, NZ, in June 1996.[15] The experts conceptualised PIAs especially on the basis of environmental impact assessment, and picked up from EIAs such notions as engaging stakeholders, identifying risks, identifying alternatives, publishing the reports.

The idea of a risk assessment tool addressing privacy risks was first promulgated in the experts' countries (i.e., New Zealand, Australia and Canada), and then in other countries, such as the US and, more recently, the UK, Ireland, Slovenia and by the European Commission. These experts are one of the most legitimate sources of analysis and assessment of current status of PIA methodologies. Especially Stewart and Longworth defined many of the parameters of the concept of PIA as it is understood today.

In one of the earliest papers on PIA, Elizabeth Longworth (1996) describes PIA as an early warning device and a risk management tool. She says assessing the privacy implications of a new technology should take place "before it is launched, rather than a retroactive assessment against a statutory structure", a point with which and virtually all PIA advocates would agree. She cites Tim McBride who put forward a list of items that a PIA should contain. However, she does not mention stakeholder consultation or independent third-party review or audit of PIAs, elements that we consider essential to the credibility of a PIA. She says she had adopted **a more generic approach covering a wider range of projects than just**

[15] Papers that originated from this event are Longworth, Elizabeth, "Notes on Privacy Impact Assessmentas", Longworth Associates, Christchurch, NZ, 1996; Stewart, Blair, "PIAs – an early warning system", *Privacy Law and Policy Reporter*, Vol. 3, No. 7, 1996.. For more details about the origins of PIA, see Clarke, Roger, "Privacy impact assessment: Its origins and development", *Computer Law & Security Review*, Vol. 25, No. 2, 2009, pp. 123-135.

information technology since 1992. We also agree that PIAs should have a wider purview than just information technology.

In a paper presented at the International Conference of Data Protection and Privacy Commissioners in September 2000, David Flaherty describes PIA as a tool for assessing "new products, practices, databases and delivery systems involving personal information".[16] We would add to Flaherty's notion that a PIA should be used wherever there is a risk of compromising all types of privacy, not simply those involving personal information.[17] Flaherty goes on to say that "Ultimately, a privacy impact assessment is a risk assessment tool for decision-makers that can address **not only the legal, but also the moral and ethical, issues** posed by whatever is being proposed." This is an important point, one with which we support – i.e., that a good PIA should take into account not only legal issues, but also ethical and social issues. Flaherty continues that PIAs "can ultimately be reviewed by central government and the privacy commissioner's office at an appropriate later step in the process. A similar model can work in the corporate world. A data protection office has to delegate as much work as possible in order to avoid being swamped." While Flaherty is certainly right that data protection authorities would not be able to review all PIAs they should at least review a serious sample of reports. **Review by a DPA or a third-party authority authorised by the DPA is essential to ensure the quality of the PIAs.** Flaherty advocates user-friendly PIA methodologies: "My major criticism of the existing guides to conducting privacy impact assessments is that they violate the KISS principle; that is, 'keep it simple, stupid'. They give the appearance of being too complicated and burdensome for the users at organisations that will be asked to do the actual work." It was in this **spirit of keeping things simple** that the PIAF project prepared its "Step-by-step guide to PIA"[18], which is only six pages long. Flaherty is in favour of publication of PIAs: "I urge public bodies and other organisations in the private sector to post any privacy impact assessment on their website so that it is available to anyone and everyone, including privacy advocates who may wish to second-guess the choices that have been made." **Publication is indeed necessary for PIAs to merit credibility, to improve transparency and accountability**.

On the issue of **public involvement in PIA**, Nigel Waters wrote: "Ideally, a PIA for a government scheme should be part of a public process and the public should be involved in the design of the PIA itself — helping to identify what questions to ask and who should be involved … But it is unrealistic to expect that agencies who are commissioning privacy invasive schemes to open them to public scrutiny voluntarily, before they have had a chance to consider the findings of an assessment internally and prepare their defences."[19] This consideration is extremely relevant for the applicability of a PIA targeted to smart surveillance practices, considering their crucial and sensitive role in government and law enforcement applications.

Consultation and engagement with stakeholders need to be a matter of policy. Otherwise organisations will avoid it. On the other hand, participatory processes are always costly and

[16] Flaherty, David, "Privacy Impact Assessments: An Essential Tool for Data Protection", *Privacy Law and Policy Reporter*, Vol. 7, No. 5, 2000.
[17] Several PIA methodologies (see below) refer to the four different categories (or types) of privacy identified by Roger Clarke.
[18] Wright, David, and Kush Wadhwa, "A step-by-step guide to privacy impact assessment", Paper presented at: Second PIAF workshop, 24 April 2012, Sopot, Poland, 2012.
[19] Waters, Nigel, "Privacy Impact Assessment – Traps for the Unwary", *Privacy Law & Policy Reporter*, Vol. 7, No. 9, 2001.

time consuming – not only for the producers and operators of technological systems but also for those groups representing citizen interests, i.e., associations and non-governmental (NGOs). It will thus be necessary to find an appropriate level of involvement depending on the seriousness of the privacy impacts.

Waters further explores who should prepare or commission a PIA. He feels, probably rightly, that the proponent of a scheme "will rarely if ever be enthusiastic about [the PIA], which is after all designed to identify and explore potential drawbacks and disadvantages". While Waters argues that a PIA should be commissioned "by someone other than the scheme proponent" we think that **conducting a PIA should be the responsibility of the project manager.** He can put together a team with an external assessor, but ultimately the project manager should be responsible and accountable for the PIA, the adequacy of which can be assessed by criteria such as were stakeholders engaged, was the report published, was the PIA submitted to an audit.

Waters is of the view that "the relationship between PIA consultants and the proponent of the scheme under review is not a normal consultant-client one. It is probably closer to auditor and client… some external authority is required for a PIA… This is why many privacy advocates have called for a PIA requirement to be written in to privacy legislation, at least for *significant* schemes (but who decides what is significant in the absence of a PIA?)". The European Commission has attempted to define what is *significant* in Article 33 of its proposed Data Protection Regulation, as noted below.

Finally, it should be noted that we agree with Waters' **four "key design principles"** which should be addressed in the practice of privacy impact assessment "to minimise privacy intrusion and surveillance where it is not a fundamental requirement. New business or government initiatives with privacy implications should firstly ensure that it is technically possible to turn surveillance off. Secondly the default setting should be 'surveillance off'. Thirdly, there should be no undue pressure for individuals to consent to changing the default setting. And fourthly, any public interest override must be subject to express legal authority and appropriate accountability safeguards."[20]

Blair Stewart refers to PIA as a process and as "a valuable technique for identifying future privacy and data protection impacts and for reducing or mitigating any adverse effects".[21] Stewart says "a PIA will often look beyond just a 'system' per se into, for instance, 'downstream' effects on persons who are affected in some way by the proposal."[22] This is in our view an important characteristic of a well-designed PIA process. Stewart also says PIA "focuses on understanding future systems with a view to identifying and mitigating forecast adverse impacts and informing decision making as to whether the project should proceed and in what form."[23] He notes that PIA is mandatory in several jurisdictions, but not all. Interestingly, he says to be credible and effective, a PIA should include "an independent component". He comments that "It would be difficult for Privacy Commissioners or the

[20] Waters, Nigel, "'Surveillance-Off': Beyond Privacy Impact Assessment – Design Principles to Minimize Privacy Intrusion", Paper presented at: 16th Annual Privacy Laws and Business International Conference: Transforming Risk Assessment into Everyday Compliance with Data Protection Law, St John's College, Cambridge, England, 7–9 July, 2003.
[21] Stewart, Blair, "Privacy Impact Assessment: Some Approaches, Issues and Examples", *Information technology management research*, Vol. 4, No. 3, 2002, pp. 23-38.
[22] Ibid., p. 24
[23] Ibid., p. 25

public to have complete confidence in a PIA which had been written solely by agency staff who are closely involved in driving a particular proposal notwithstanding the personal expertise and integrity of such people." Stewart's condition for confidence in the PIA could be met if the PIA is subject to third-party review or audit, just as a company's financial accounts are checked by an independent auditor. Stewart continues that "it may be valuable to submit a draft version to appropriate privacy experts for peer review".[24] We also share his emphasis on **PIA as a *process*** rather than focusing solely on the production of a PIA report. And a PIA should not be equated with a privacy compliance audit, i.e., checking that the project to be assessed complies with existing legislation. We also agree with Stewart saying **PIA "should go beyond the legal tests**… into identifying best practice and identifying the ways, through mitigation, or identification of alternatives, a privacy-respectful outcome can be obtained."[25] We think this is a hallmark of an optimised PIA. Finally, we support Stewart's argument for making completed PIA reports publicly available – or at least those parts that do not include sensitive material. [26]

Roger Clarke, who has written more about PIA since the early 1990s than anyone else, says that PIA is properly distinguished from other kinds of activities by the following characteristics:

- *a PIA is performed on a project or initiative* (i.e. a PIA is distinct from an organisational privacy strategy);
- *a PIA is anticipatory in nature*, conducted in advance of or in parallel with the development of an initiative, rather than retrospectively (i.e. a PIA is distinct from a privacy audit);
- *a PIA has a broad scope in relation to the dimensions of privacy*, enabling consideration of privacy of the person, privacy of personal behaviour and privacy of personal communications, as well as privacy of personal data (i.e. a PIA is distinct from a mere 'data protection impact assessment' that the draft GDPR mentions);
- *a PIA has a broad scope in relation to the perspectives reflected in the process*, taking into account the interests not only of the sponsoring organisation, and of the sponsor's strategic partners, but also of the population segments affected by it;
- *a PIA has a broad scope in relation to the expectations against which privacy impacts are compared*, including people's aspirations and needs, and public policy considerations, as well as legal requirements (i.e. a PIA is distinct from a compliance assessment, whether against privacy laws generally, or data privacy laws in particular, or a specific data protection statute);
- *a PIA is oriented towards the surfacing both of problems and of solutions to them* (i.e. a PIA is more than just a privacy issues analysis);
- *a PIA emphasises the assessment process* including information exchange, organisational learning, and design adaptation (i.e. a PIA is not merely focused on the expression of a carefully-worded privacy impact statement);
- *a PIA requires intellectual engagement from executives and senior managers* (i.e. a PIA is not a mere checklist ticked through by junior staff or lawyers).[27]

While we endorse all of Clarke's points, we would add the following ones:

- a PIA report should be published;

[24] Ibid., p. 29.
[25] Ibid., p. 30.
[26] Ibid., p. 31
[27] Clarke, 2009.

- a PIA process should include elements of stakeholder participation;
- a PIA report should undergo an independent audit.

On the issue of mandatory PIAs, Clarke is of view that "Requiring that one be conducted for every project is likely to be counter-productive because it tends to encourage merely formal checklist-filling rather than intellectual engagement with the issues. It is more common for organisations to be required to consider whether a PIA is needed."[28] However, he cites Bennett and Raab in saying that personal information systems should be "regarded as (relatively) dangerous until shown to be (relatively) safe, rather than the other way around" – which we view as sensible advice.[29] This consideration is relevant for smart surveillance as well, since these technologies and applications have the potential to raise critical privacy, data protection and ethical issues.

2.2 LEARNING FROM PIA EXPERIENCE

The fact that the above-referenced PIA pioneers all knew each other and exchanged views on PIAs very early on helps explain why PIA (at least using this term) first appeared in Australia, Canada and New Zealand (it developed in the US more or less in the same time frame). The influence of these pioneers has continued to be felt. When the UK's Information Commissioner's Office published its PIA Handbook in 2007, it was based on a review of PIA in these other countries. Roger Clarke was a member of the consortium that undertook the work for the ICO and was a principal author of the Handbook. The Irish Health Information and Quality Authority trod a similar path. It too carried out a review of PIA approaches in these other countries before it published its Guidance document in 2010.

Although there are differences between the PIA policies and methodologies of these countries, one can also see an increasing convergence in approaches, in good part because later countries, the UK and Ireland, have sought to learn from the experience of others. The increasing convergence is manifested by, for example, the emphasis on stakeholder consultation which features strongly in the UK and Irish PIA guidance documents, but less so or not at all in some of their antecedents. Convergence is also seen in definitions too, for example, of the term "project". Even certain phrases (PIA is described as "an early warning system") turn up again and again. It has to be mentioned here that other countries, such as Germany or France, were not less concerned about possible privacy impacts of new technologies but did not follow the same path as the English-speaking countries.

That PIA as a policy and methodology has some features in common with environmental impact assessment (EIA) is no accident. Blair Stewart, among other experts, has pointed to EIA as a direct forbear of PIA.[30] In both cases, the impact assessment aims to identify risks and solutions and to engage stakeholders in the process. In this deliverable, as mentioned

[28] Ibid., p. 129

[29] Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge, Mass. and London, 2006, p. 62.

[30] In an e-mail dated 21 October 2011 to David Wright, Stewart said, "In putting together my first conference session on PIA (1996) and a resource paper for that session, I did make an analogy with EIA which I had a passing familiarity with through studying environmental law (with Tim McBride as it happens, Tim was also the foremost NZ expert in privacy law at the time I was at university, indeed virtually the only NZ expert in privacy until the 1990s). I mainly used some definitions of 'environmental impact assessment' to craft a definition of PIA. I also liked the analogy of the cumulative effects of a degraded environment to compare with the insidious erosion of privacy."

above, our definition of PIA includes reference to the key function of consulting stakeholders, i.e., PIA is

> a methodology for assessing the impacts on privacy of a project, technology, product, service, policy, programme or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. A PIA is more than a tool: it is a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after deployment of the project.[31]

While we discuss "privacy impact assessment" throughout this paper, the reader may wish to note that the European Commission refers to "privacy and data protection impact assessment" in its RFID recommendation[32] and uses the term "data protection impact assessment" in its Data Protection Reform proposal. We prefer the original term of privacy impact assessment, because we view data protection (information privacy) as only one type of privacy, and government agencies and companies should consider as well the risks to other types of privacy in any initiative they develop. In relation to this, we distinguish seven types of privacy – privacy of the person, of personal behaviour, of personal communications, of personal data, of location, of thought and feeling, and of the group or association.[33] All these types of privacy should be taken into account in a privacy impact assessment. A data protection impact assessment is too limited in scope.

De Hert has criticised data protection impact assessment as merely a compliance check, "simply checking the legal requirements spelled out in the European data protection framework".[34] He points out that the Charter of Fundamental Rights of the European Union differentiates between privacy (Art. 7) and data protection (Art. 8).[35] "Depending on the nature of the data used, personal data and/or location data and/or traffic data, and depending on the nature of the processing involved (private, public, law enforcement), one can establish a checklist based on these regulations that when carried out properly will make up the data protection impact assessments. No more and no less".[36] He goes on to argue that "Beyond compliance checks with legal regulations, one must consider more qualitative requirements that have to do with legality, legitimacy, participation and, especially, proportionality… These qualitative principles – accounting for the difference between a compliance check and a true impact assessment – are key considerations in determining whether privacy is respected in the context of the ECHR [European Convention on Human Rights] and the relevant case law of the ECtHR [European Court of Human Rights]."[37] Like Clarke, De Hert finds that privacy goes beyond data protection: "the privacy right has served as a catch-all tool, covering a sophisticated collection of interests, ranging from intimacy, sexual choice, personal identity, moral and physical well-being, reputation, formation of human relationships, health and environmental protection, collection of and access to personal information".[38] For these and other reasons, we prefer the term privacy impact assessment

[31] Wright, David, "The state of the art in privacy impact assessment", *Computer Law & Security Review*, Vol, 28, No. 1, Feb. 2012, pp. 54-61 [p. 55]. http://www.sciencedirect.com/science/journal/02673649.
[32] European Commission, "Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification", 2009.
[33] Finn, Rachel L., David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp. 7-10.
[34] De Hert, Paul, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, p. 34.
[35] Ibid., p. 33.
[36] Ibid., p. 35.
[37] Ibid., p. 38.
[38] Ibid., p. 39

over data protection impact assessment. The former is wider-ranging and can catch intrusions and compromises that may not be caught by a data protection impact assessment.

2.3 AN ANALYTICAL FRAMEWORK TO ASSESS PIAS

While the PIA literature is not voluminous (but is growing), researchers have identified criteria that make a "good" PIA. These include what a PIA is, how it should be conducted, what it should contain, how organisations undertaking PIAs should be supported, and how PIA recommendations should be implemented and monitored.

The comparative analysis of selected PIAs methodologies as presented in the following chapter is built around 18 criteria, which have been derived from the PIA literature[39], or introduced as new considerations. The 18 assessment criteria include the following:

1. Is PIA regarded as a process?
2. Does the PIA guide contain a set of questions to uncover privacy risks?
3. Does the PIA guide target companies as well as government?
4. Does the PIA address all types of privacy (informational, bodily, territorial, locational, communications)?
5. Is PIA regarded as a form of risk management?
6. Does the PIA guide identify privacy risks?
7. Does the PIA guide identify possible strategies for mitigating those risks?
8. Does the PIA guide identify benefits of undertaking a PIA?
9. Does the PIA guide support consultation with external stakeholders?
10. Does the PIA guide encourage publication of the PIA report?
11. Does the PIA guide provide a privacy threshold assessment to determine whether a PIA is necessary?
12. Does the PIA guide provide a suggested structure for the PIA report?
13. Does it advocate undertaking a PIA for proposed legislation and/or policy?
14. Does the guide say that PIAs should be reviewed and updated throughout the life of a project?
15. Does the guide explicitly say that PIA is more than a compliance check?
16. Does the PIA policy provide for third-party, independent review or audit of the completed PIA report?
17. Is PIA mandated by law, government policy or must a PIA accompany budget submissions?
18. Do PIA reports have to be signed off by senior management (to foster accountability)?

As one can see from the above list, these criteria are general and not targeted to developing a PIA suitable for surveillance practices. If the aim is to assess the validity of a PIA particularly targeted to smart surveillance, we suggest that particular attention should be put to question 4 above, which should be expanded to include other fundamental rights that may be impacted by surveillance. The other questions more generally refer to how to implement the PIA *process*, which is not strictly linked to the type of risk under assessment – as stated in section 1.2.

[39] A comparative analysis using these criteria has been already made in Wright, David, Rachel Finn and Rowena Rodrigues, "A comparative analysis of privacy impact assessment in six countries", *Journal of Contemporary European Research*, Vol. 9, No. 1, 2013.

3 COUNTRY COMPARISON

The aim of this chapter is to present a comparison of existing PIA methodologies in a selected group of countries. We took the decision not to limit the analysis to the most advanced experiences of PIAs, i.e., in countries where PIAs developed as an early warning instrument and a risk management tool particularly targeted to informational privacy (Australia, Canada, Ireland, New Zealand, UK and the United States).

We also describe some more recent PIA-like developments in two other European countries (France, Netherlands) and at the EU level (the RFID PIA Framework). The aim is to understand how the landscape is evolving in Europe and is being received by non-Anglo-Saxon countries.

The second goal of this chapter is to investigate whether current models for PIAs are suitable for assessing surveillance systems, technologies and practices. To this end, we have analysed the adequacy of PIA reports that focus on surveillance systems.

3.1 AUSTRALIA

We begin our review of PIA methodologies with Australia and, in particular, two guidance documents, one produced by the Office of the Privacy Commissioner of Australia (now the Office of the Information and Privacy Commissioner) and the other produced by the Office of the Privacy Commissioner of Victoria.

3.1.1 Office of the Privacy Commissioner of Australia

The Office of the Privacy Commissioner (OPC) published its *Privacy Impact Assessment Guide* in August 2006, and a revised version in May 2010.[40] The *Guide* is addressed to those who undertake a PIA, irrespective of whether they are from government agencies, the private sector or not-for-profit sector (i.e., civil society organisations). This is an important point to note. Any organisation, from whatever sector, should undertake a PIA if it is planning a project that might pose risks to privacy. However, there is no legislative requirement in Australia to conduct a PIA. It does not impose a particular PIA style ("There is no one-size-fits-all PIA model.") but suggests a flexible approach depending on the nature of the project and the information collected.

Another important distinction between the Australian PIA Guide and some of its counterparts is that it makes the point (at p. iii) that **information privacy is only one aspect of privacy**. Other types of privacy include privacy of the body, privacy of behaviour, privacy of location and privacy of communications, as mentioned above.

It defines "project" as "any proposal, review, system, database, program, application, service or initiative that includes handling of personal information".[41] Note that the definition excludes proposed policies or legislation (which, by contrast, the ICO PIA Handbook includes). The *PIA Guide* says (p. viii) a PIA should be an integral part of the project from the beginning. A PIA should evolve with and help shape the project, which will help ensure

[40] Office of the Privacy Commissioner (OPC), *Privacy Impact Assessment Guide*, Sydney, 2010.
[41] The UK *PIA Handbook* uses a similar definition. See *I*nformation Commissioner's Office (ICO), *Privacy Impact Assessment Handbook*, Version 2, UK Information Commissioner's Office, London, 2009.

that privacy is "built in" rather than "bolted on" (which echoes the same wording used in the ICO *PIA Handbook*).

The *PIA Guide* says that "Consultation with key stakeholders is basic to the PIA process." The Privacy Commissioner encourages organisations, "where appropriate", to make the PIA findings available to the public.[42] The PIA Guide says publication "adds value; demonstrates to stakeholders and the community that the project has undergone critical privacy analysis; contributes to the transparency of the project's development and intent".[43]

Although the *PIA Guide* acknowledges different PIA models, it says there are generally five key stages in the PIA process:[44]
1. Project description
2. Mapping the information flows and privacy framework
3. Privacy impact analysis
4. Privacy management
5. Recommendations.

The *PIA Guide* says the Office of the Privacy Commissioner has no formal role in the development, endorsement or approval of PIAs. However, subject to available resources, the Office may be able to help organisations with advice during the PIA process.[45]

3.1.2 Victoria Privacy Commissioner (OVPC) PIA Guide

Roger Clarke has described the PIA guide produced by the Office of the Victorian Privacy Commissioner (OVPC) as "one of the three most useful guidance documents available in any jurisdiction, anywhere in the world".[46] The current OVPC *PIA Guide* dates from April 2009.[47] It is the second edition of the guide originally published in August 2004.

The OVPC *PIA Guide* is primarily aimed at the Victorian public sector, but it says it may assist anyone undertaking a PIA. Like the Australian OPC *Guide*, it says that privacy considerations must be broader than just information privacy; bodily, territorial, locational and communications privacy must also be considered.

It sets out various risks thematically linked to Victoria's privacy principles as well as possible strategies for mitigating those risks. A template provides the structure of a PIA report, which the user can adapt to his or her circumstances.

[42] The Privacy Commissioner acknowledges (p. xviii) that there may be circumstances where the full or part release of a PIA may not be appropriate. For example, the project may still be in its very early stages. There may also be security, commercial-in-confidence or, for private sector organisations, other competitive reasons for not making a PIA public in full or in part. However, transparency and accountability are key issues for good privacy practice and outcomes, so where there are difficulties making the full PIA available, the Commissioner encourages organisations to consider the release of a summary version.
[43] OPC (Office of the Privacy Commissioner), 2010, pp. x, xviii.
[44] Ibid., p. xii ff.
[45] Ibid., p. xix
[46] Clarke, Roger, "PIAs in Australia: A Work-in-Progress Report", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.
[47] Office of the Victorian Privacy Commissioner (OVPC), *Privacy Impact Assessments: A guide for the Victorian Public Sector* (Edition 2), Melbourne, 2009.

The *Guide* uses the word "project" to encompass any type of proposed undertaking, including "legislation" and "policy", which are not mentioned in the Australian OPC *Guide*.[48] It says the size or budget for a project is not a useful indicator of its likely impact on privacy.

The *Guide* recommends that a simple threshold privacy assessment be routinely conducted for every project to determine whether a PIA is necessary. The *Guide* has 17 simple yes/no questions (e.g., will the project involve the collection of personal information, compulsorily or otherwise?). If the answer to any of the questions is yes, the organisation should seriously consider initiating a PIA.

The *Guide* says up-front commitment from an organisation's executive to the conduct of PIAs is needed to ensure buy-in to the PIA's eventual recommendations.[49] The *Guide* advocates publication of the PIA report: Releasing a PIA report gives the public an opportunity to express concerns and have them addressed before a project has been implemented. The *Guide* says the PIA should be dynamic, updated as changes are contemplated to projects.

Organisations should consult early with the privacy commissioner if
- there is a large amount of personal information at issue;
- the project involves sensitive information;
- there will be sharing of personal information between organisations;
- any personal information will be handled by a contracted service provider;
- any personal information will be transferred outside Victoria; or
- there is likely to be public concern about actual or perceived impact on privacy.

Like most other guidance documents, the *Guide* says that a PIA should assess not only a project's strict compliance with privacy and related laws, but also public concerns about the wider implications of the project. It cites the New Zealand *PIA Handb*ook which notes that "Proposals may be subject to public criticism even where the requirements of the Act have been met. If people perceive their privacy is seriously at risk, they are unlikely to be satisfied by [an organisation] which justifies its actions merely by pointing out that technically it has not breached the law".[50]

The *Guide* says that public consultation as part of the PIA process not only allows for independent scrutiny, but also generates confidence amongst the public that their privacy has been considered. Public consultation may generate new options or ideas for dealing with a policy problem. If wide public consultation is not an option, the *Guide* says the organisation could consult key stakeholders who represent the project's client base or the wider public interest or who have expertise in privacy, human rights and civil liberties.

The report generally recommends publication of the report, but recognises that some considerations, such as security, may influence the decision to publish.[51] In such cases, it says that a properly edited PIA report would usually suffice to balance the security and transparency interests. One option is to publish both the PIA report and the organisation's response to its recommendations, and then seek feedback through consultation on whether the

[48] Ibid., p. 5
[49] Ibid., p. 6
[50] Privacy Commissioner's Office, *Privacy Impact Assessment Handbook*, Wellington, New Zealand, 2007.
[51] OVPC (Office of the Victorian Privacy Commissioner), 2009, p. 20.

proposed response is acceptable to stakeholders, whether the project should proceed and/or which option/s to follow.

3.2 CANADA

In this section on Canada, we highlight some of the key provisions in the Canadian government's Directive on privacy impact assessment, its PIA guidelines and the PIA guidance documents used in Ontario and Alberta. In the annex, we also analyse a Canadian PIA report concerning a smart surveillance technology: the Automatic Licence Plate Recognition system (see Annex B).

Directive on Privacy Impact Assessment

In Canada, policy responsibility for privacy impact assessment in the federal government lies with the Treasury Board of Canada Secretariat (TBS), which defines PIA as "a policy process for identifying, assessing and mitigating privacy risks".[52] TBS promulgated a new Directive on Privacy Impact Assessment in April 2010.[53]

The directive ties PIAs with submissions to the Treasury Board for program approval and funding. This is one of the strongest features of Canadian PIA policy. PIAs have to be signed off by senior officials, which is good for ensuring accountability, before a submission is made to the Treasury Board. The PIA is to be "simultaneously" provided to the Office of the Privacy Commissioner. Institutions are instructed to make parts of the PIA publicly available, i.e., an overview and PIA "initiation", and specify "risk area identification and categorisation". Exceptions to public release are permitted for security as well as "any other confidentiality or legal consideration". Heads of government institutions are responsible for monitoring and reporting their compliance with the PIA directive and the TBS "will monitor compliance with all aspects of this policy".

The TBS does not approve PIAs; it only reviews them to ensure that "the assessment is complete". The TBS requirements convey to the reader that the emphasis is on completion of a PIA report, rather than PIA as a process. The directive makes no provision for stakeholder engagement. Nor does it address the benefits of undertaking a PIA and finding solutions to privacy risks.[54] While the Directive does not refer to the TBS's PIA Guidelines, these are still recommended even if they have not been revised since August 2002.[55]

The first step in the PIA process is to determine whether it is required, and the first question to ask is, "Is personal information being collected, used or disclosed in this initiative?" If the answer is "no", then a PIA is not required. If the answer is "yes" or "maybe", officials should then go through the checklist of 11 questions on the first page of the guidelines. These

[52] Treasury Board of Canada Secretariat (TBS), "Policy on Privacy Protection", 1 April 2008.
[53] Treasury Board of Canada Secretariat (TBS), "Directive on Privacy Impact Assessment", 1 April 2010.
[54] Although the PIA Directive does not mention benefits or solutions, the PIA Guidelines do mention potential outcomes, which can be regarded as benefits or solutions.
[55] In an e-mail dated 8 July 2011 to David Wright, a TBS spokesperson said that although the Guidelines "predate the current Directive on Privacy Impact Assessment, much of the analytical guidance contained therein is still sound…. The new Directive has greatly lightened the administrative burden surrounding the reporting of PIAs and eliminated the need for Preliminary PIAs…. We are in the process of developing guidance around the new Directive which will be made available on the IPPD website at http://www.tbs-sct.gc.ca/ip-pi/index-eng.asp in the coming months."

questions are somewhat like those in the privacy threshold assessment used in the Australian OPC and Victoria PIA Guides, among others. Also like those guides, the TBS PIA Guidelines are based upon privacy principles – in this case, those in the Canadian Standards Association's *Model Code for the Protection of Personal Information*[56] as well as federal privacy legislation and policies.

Other PIA guidance documents state that the purpose of a PIA is to identify and mitigate privacy risks. Interestingly, the TBS Guidelines state that "a key goal of the PIA is to effectively *communicate* the privacy risks… [and] to contribute to senior management's ability to make fully informed policy, system design and procurement decisions".[57] The Guidelines identify several common privacy risks, such as data profiling/data matching, transaction monitoring, identification of individuals, physical observation of individuals, publishing or re-distribution of public databases containing personal information and lack or doubtful legal authority.

The Guidelines include two questionnaires to help identify privacy risks or vulnerabilities in the proposal and to facilitate the privacy analysis. The questionnaires include a "yes" or "no" field as well as a "Provide details" field for explaining how a particular requirement is met or why it is not met. The Guidelines say that departments and agencies can undertake generic or overarching PIAs where proposals are similar or interrelated to avoid duplication of effort.

3.2.1 Ontario

In Ontario, since the late 1990s, the principal driver behind government policy in relation to PIAs was not the privacy oversight body, but a central agency called the Management Board Secretariat (MBS). As early as June 1998, a completed PIA became a pre-requisite for approval of Information and Information Technology (I&IT) project plans submitted for Cabinet approval.[58] In December 2010, Ontario's Office of the Information and Privacy Commissioner released a revised *PIA Guide*, replacing the 2001 version. The *Guide* provides an overview of the PIA methodology and outlines the privacy activities required throughout a project's lifecycle. It also explains how to integrate a PIA into project management and use the results to meet corporate governance requirements. Three PIA tools were also released at that time and provide detailed instructions, checklists, templates and other resources to help projects complete the PIA process. It is too early to draw conclusions on their use.[59]

Section 6 of the Regulation to the Personal Health Information Protection Act (PHIPA) mandates PIAs for Health Information Network Providers (HINP), when two or more Heath Information Custodians (HIC) use electronic means to disclose Personal Health Information (PHI) to one another.[60]

The *Privacy Impact Assessment Guide* for the Ontario Public Service says ultimate accountability for privacy protection rests with the Minister, as head of each government

[56] http://www.csa.ca/cm/ca/en/privacy-code
[57] Treasury Board of Canada Secretariat (TBS), "Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks", Ottawa, 2002, p. 2.
[58] Clarke, "Privacy impact assessment: Its origins and development", 2009, p. 127.
[59] Bayley, Robin M., and Colin J. Bennett, "Privacy Impact Assessments in Canada", in Wright, David and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.
[60] Tancock, David, Siani Pearson, and Andrew Charlesworth, "Analysis of Privacy Impact Assessments within Major Jurisdictions", in *Proceedings of the Eighth Annual International Conference on Privacy, Security and Trust*, Ottawa, 17-19 August 2010, IEEE Press, 2010, pp. 118-125.

institution.[61] The head is responsible for complying with the Freedom of Information and Protection of Privacy Act (FIPPA) and for ensuring that personal information held by the ministry is accurate, up to date and collected, used and disclosed only as authorised. The *Guide* defines privacy impact assessment as "a consistent and systematic approach for identifying and analysing privacy risks when changing or developing programs or systems". It is also described as "both a due diligence exercise and a risk management tool".[62]

The *Guide* says it is important to look at other types of privacy when assessing a project, i.e., freedom in the physical domain, freedom of movement or expression or of the person or personal space; freedom to communicate privately with others; freedom to determine when, what, how and with whom they share their personal information. It adds that "An activity may comply with the law but still be seen as unnecessarily privacy invasive." It states that "The potential damage to the individual must take precedence in your assessment over organizational risks." It also adds that "Risk management can mitigate a risk, but it can never be completely avoided or eliminated. If your project involves personal information, there always will be some privacy risk."[63]

3.2.2 Alberta

In 2001, the Office of the Information and Privacy Commissioner (OIPC) of Alberta introduced its first Privacy Impact Assessment (PIA) questionnaire. In the following eight years, according to the OIPC, the practice of privacy impact assessments matured and the number of PIAs increased dramatically. In January 2009, the OIPC revised its PIA template and guidelines.[64]

Those submitting PIAs are advised to consider the feedback from the OIPC before they implement their projects covered by Alberta's Health Information Act (HIA). Otherwise, if the OIPC identifies privacy concerns, "it may be necessary to make expensive and time-consuming changes to your project late in the development cycle".[65] The OIPC appears to exercise much more power than most of its counterparts. Not only are PIAs dealing with health information mandatory, they must be submitted to the OIPC before implementation of a new system or practice. If the OIPC finds shortcomings, projects can be turned down or forced to make costly retrofits. It appears to play a much more activist role in reviewing PIAs than many of its counterparts elsewhere.

The OIPC points out that "acceptance" of a PIA is not approval. It only reflects the OIPC's opinion that the project manager has considered the requirements of the HIA and has made a reasonable effort to protect privacy. The OIPC says "custodians" of health information should review their PIAs as new practices and technologies evolve after projects are implemented and new threats to privacy may also develop. Custodians should advise the OIPC of any resulting changes to the PIA. The OIPC says if a member of the public makes a complaint against the custodian's organisation, it may review previously submitted PIAs.

[61] Office of the Chief Information and Privacy Officer (OCIPO), *Privacy Impact Assessment Guide for the Ontario Public Service*, Queen's Printer for Ontario, Toronto, 2010.
[62] Ibid., p. 6.
[63] Ibid., p. 48.
[64] Office of the Information and Privacy Commissioner of Alberta (OIPC), *Privacy Impact Assessment Requirements*, Edmonton, 2009.
[65] Ibid., p. 5.

Unlike other PIA methodologies that say PIAs should be initiated as early as possible, the OIPC PIA Requirements say that, generally speaking, the best stage at which to do a PIA is after all business requirements and major features of the project have been determined in principle, but before completing detailed design or development work to implement those requirements and features, when it is still possible to influence project design from a privacy perspective. The PIA must include details on the project's information security and privacy policies and procedures. The Alberta PIA Requirements are unusual in making mandatory the format for HIA PIAs. The OIPC advises custodians that if they do not provide enough detail, the OIPC will ask for clarification, which will increase the overall PIA review time and delay the project.

3.3 FRANCE

In July 2012, the French DPA, the Commission Nationale de l'Informatique et des Libertés (CNIL) issued two guidance documents on security and privacy risk management.[66] These guidelines were translated into English in November 2012.[67] The first one is a *Methodology for Privacy Risk Management* (hereinafter: *Methodology*),[68] and the second is *Measures for the privacy risk treatment* (hereinafter: *Measures*).[69]

The *Methodology* thus does not concern PIAs as such, but rather, risk management techniques applied to privacy. However, this *Methodology* has a strong kinship with PIAs, since it can be argued that one of the distinctive features of a PIA is a risk assessment/risk management approach (along with public participation and decentralised responsibility in the framework of the accountability principle), as opposed to other anticipatory tools that contribute to the protection of privacy and personal data such as prior checking.[70] As evidence of this kinship, the *Methodology* is explicitly drafted for data controllers.[71]

Whereas a PIA integrates a very broad range of concerns (e.g., if PIA is a process then at which stages of the planned processing should it intervene; which stakeholders should be consulted and under what modalities should they be consulted; what are publicity and transparency requirements concerning the PIA report), the *Methodology* solely addresses the issue of risk assessment and management (which, it can be argued, is the core element of the process consisting in assessing the impacts of a planned project).

From the outset, the CNIL risk assessment methodology is grounded within a privacy risk management approach that is derived from information security risk assessment. According to the document, the legal basis for a risk assessment methodology is situated within Art. 16

[66] http://www.cnil.fr/nc/la-cnil/actualite/article/article/deux-nouveaux-guides-securite-pour-gerer-les-risques-sur-la-vie-privee/

[67] http://www.cnil.fr/english/news-and-events/news/article/the-cnil-publishes-an-english-translation-of-its-two-advanced-security-and-privacy-risk-management/

[68] http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

[69] http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Measures.pdf

[70] Wright, 2012; Le Grand, Gwendal, and Emilie Barrau, "Prior Checking, a Forerunner to Privacy Impact Assessments", in Wright and De Hert (eds.), 2012, pp. 97-116 [p. 115]. See also the Opinion of the Article 29 Working Party Group 2010, whereby it did not endorse the first draft PIA framework submitted by the RFID workgroup; one of the major reasons for the refusal was that there was no risk assessment. Risk assessment is a "key component" of a PIA process. Prior checking is provided for by Art. 20 of the EU Data Protection Directive (95/46/EC).

[71] *Methodology*, p. 4.

and 17 of the Data Protection Directive, and more in particular, in Art. 34 of the French Data Protection Act (which thus implements the former articles).[72] Further evidence is the explicit acknowledgement that the *Methodology* is an attempt to apply the EBIOS methodology to the field of privacy.[73] EBIOS is the name of a risk assessment methodology used in the area of information systems security risks, which the CNIL adapted to better serve the needs of a privacy risk analysis (broader than security analysis).[74] In this sense, there are similarities with the risk assessment methodology deployed for the RFID PIA Framework at EU level.[75]

The *Methodology* builds upon a classical, epistemic and linear account of risk understood as "a function of the likelihood of a given threat-source exercising a particular potential vulnerability and the resulting impact of that adverse event on the organisation".[76] According to the *Methodology*, a risk is then estimated in terms of severity of the damage (what the *Methodology* terms as "feared event") and of likelihood that such damage happens (what the *Methodology* terms as "threat").[77]

The risk management approach is an iterative process composed of a five steps: context of the processing, feared events, possible threats, risk level, (mitigation) measures.

The context of the processing entails describing the primary assets (i.e., the type of personal data and processing involved) that deserve protection, the supporting assets (e.g., hardware, software…), the main benefits stemming from the primary assets, or the relevant sources of risks (e.g., humans, non-humans).[78]

Once potential feared events (i.e., damages) are determined, their level of severity is obtained by adding the possibility of identification of data subjects with the extent of the prejudicial effect (or potential impacts) that would result from such feared events.[79]

Step three (entitled threat study) concerns the likelihood of damage occurrence. It is obtained by assessing the vulnerability of the supporting assets, and by adding it to the capabilities of risk sources (that is, how much harm can the latter cause).[80]

Once the severity of the damages and their likelihood have been determined, it is possible to map the risks (step four). On this basis, and depending upon the level of the risks at stake, objectives of risk mitigation can be set.[81]

Finally, risk mitigation measures that are proportionate (including in terms of costs and benefits), and compliant with the French Data Protection Act must be taken. They will be

[72] *Methodology*, p. 9.
[73] *Expression des Besoins et Identification des Objectifs de Sécurité* – Expression of needs and identification of security objectives.
[74] *Methodology*, p. 10.
[75] See Spiekermann, Sarah, "The RFID PIA – Developed by Industry, Endorsed by Regulators", in Wright and De Hert (eds.), 2012, pp. 323-346.
[76] Stoneburner, Gary, Alice Goguen and Alexis Feringa, National Institute for Standards and Technology (NIST), *Risk Management Guide for Information Technology Systems*, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-30, July 2002. In other words, a risk is the result of the probability (or likelihood) of occurrence of a harm or damage.
[77] *Methodology*, p. 8.
[78] Ibid., pp. 10-11.
[79] Ibid., pp. 12-13.
[80] Ibid., pp. 15-17.
[81] Ibid., pp. 18-19.

applied to the different constitutive elements of the risk: feared events, prejudicial effect/or potential impacts, risk sources, and supporting assets. Following these measures, a new risk mapping must be undertaken and justification must be given as to why residual risk should be accepted.[82]

3.4 IRELAND

In this section, we highlight the PIA Guidance developed by the Irish Health Information and Quality Authority (HIQA), which is an independent authority, established under the Health Act 2007, to drive improvement in Ireland's health and social care services. Among other things, it aims to ensure that service users' interests are protected, including their right to privacy, confidentiality and security of their personal health information. In this context, the Authority produced a PIA Guidance[83] following its review of PIA practice in other jurisdictions[84], which found a growing convergence in what constitutes best practice in relation to PIAs.

The Guidance says the PIA process involves the evaluation of the privacy implications of projects and relevant legislative compliance. Where potential privacy risks are identified, a search is undertaken, in consultation with stakeholders, for ways to avoid or mitigate these risks. It says that a PIA may not highlight all privacy risks or issues associated with an initiative. A PIA is a tool; it is dependent on service providers having the correct processes in place to carry out the PIA. These include identification of the correct stakeholders for the assessment, selection of those with the necessary knowledge and skills to carry out the PIA and involvement of senior managers in order to implement the PIA recommendations. It is essential that the PIA is regularly updated to reflect any changes in the direction of the initiative to ensure that all discoverable privacy issues are addressed.

The PIA should generally be undertaken by the project team. It may, however, be appropriate to consult service users as part of the PIA process. The service provider is ultimately responsible for the completion of the PIA and for implementing any changes to the project plan following recommendations from the PIA. PIAs should be reviewed and approved at a senior level with each PIA report being quality assured by senior management.

Like the Alberta PIA Requirements, the Irish Guidance says that if a PIA is conducted too early, the results will be vague as there may not be enough information available about the project, its scope and proposed information flows to properly consider the privacy implications and as such the PIA may need to be revisited. The PIA process should be undertaken when a project proposal is in place but before any significant progress or investment has been made. The findings and recommendations of the PIA should influence the final detail and design of the project.

The project manager should explain the option(s) chosen for each risk and the reasoning behind the choices. If there is a residual or remaining risk, which cannot be mitigated, the project team must decide whether or not it is acceptable to continue with the project. The

[82] Ibid., pp. 20-22.
[83] Health Information and Quality Authority (HIQA), *Guidance on Privacy Impact Assessment in Health and Social Care*, Dublin, 2010.
[84] Health Information and Quality Authority (HIQA), *International Review of Privacy Impact Assessments*, Mahon, Cork, Ireland, 2010.

Guidance says consultation with stakeholders and members of the public about the privacy risks associated with the project can prove valuable. Consultation can help in discovering the impacts of some privacy risks. Consultation is a way to gather fresh input on the perceptions of the severity of each risk and on possible measures to mitigate these risks. Feedback gained and any changes made to a project as a result of stakeholder engagement should be included in the PIA report.

The Health Information and Quality Authority favours publication of PIA reports as it builds a culture of accountability and transparency and inspires public confidence in the service provider's handling of personal health information. Completed PIA reports should be published and presented in a reader-friendly format.

3.5 NETHERLANDS

The Netherlands does not possess yet a PIA framework, but it is in the process of drafting such a framework. The Motion on an Evaluation Law concerning the Protection of Personal Data,[85] adopted on 17 May 2011, provides that particular attention should be paid to the question of whether limitations to privacy as a result of proposed legislation are justified.[86] PIAs are one of the measures to assess the privacy consequences of future legislation. Following this Motion, the Government included in its former and current Coalition Agreement (of 29 October 2012) the need to carry out PIAs as a standard procedure.[87]

In spring 2012, the Dutch Ministry of the Interior and Kingdom Relations began drafting a PIA framework. According to an official invited to present these developments at a PIA-dedicated panel at the 2013 edition of the conference on Computers, Data Protection and Privacy (CPDP) in Brussels, the drafting process is still at an early stage and is therefore subject to little publicity and transparency.

From this presentation, the audience learned that the Dutch Ministry of Interior conceives of PIAs as a process amounting to more than a box-ticking exercise that needs to be conducted as early as possible and iteratively throughout the life cycle of the project. PIAs are characterised as an accountability and co-regulatory measure: they are to be undertaken in house by data controllers, yet the government is willing to pursue a "business friendly" approach. The government wants to avoid undue administrative burdens. In this sense, it is planning to provide for the possibility of "light" PIAs. Equally, that is the reason why the possibilities for stakeholder and citizen involvement are very scarce under the current draft.

Another striking feature of this draft PIA methodology is its (pronounced) legalistic character. The core of the risk assessment is broken down into four legal topics: type of personal data and processing as well as compliance with the principles of necessity and data minimisation; purpose limitation, system-linkage and profiling; storage/deletion and security measures; transparency and data subjects' rights. Though the representative of the Ministry acknowledged that one of the features of a PIA (and *a fortiori* of a risk assessment) is to go beyond a purely legalistic framing of issues and thus the recourse to other accounts of privacy and data protection harms, he also acknowledged that such accounts have not yet found their

[85] Evaluatie Wet bescherming persoonsgegevens.
[86] https://zoek.officielebekendmakingen.nl/kst-31051-D.pdf
[87] Along with sunset clauses, greater powers for the Dutch DPA and privacy by design. http://www.government.nl/government/coalition-agreement/viii-security-and-justice

way into the draft document. Furthermore, he also discussed the possibility of integrating broader legal concerns that might turn the Dutch PIA in a full human rights PIA.[88] Might this predominantly legal approach to PIA be a factor accounting for the lack of interest for stakeholders and citizens participation? The fact that the jurists of the Ministry of the Interior are in charge of the drafting process might explain this legal emphasis. In any event, it provides an interesting contrast with the French Methodology for privacy risk management and with the EU RFID PIA framework, which are inspired by computer scientists and the correlative security risk assessments. Furthermore, it gives weight to the view that, although PIAs should clearly be distinguished from compliance checks, in practice this difference is not so evident to make, and there is certainly (quite) some overlap.[89]

3.6 NEW ZEALAND

The origins of privacy impact assessment in New Zealand date back to at least 1993, to the legislative requirement under section 98 of the Privacy Act 1993 to undertake Information Matching Privacy Impact Assessments (IMPIAs).[90] IMPIAs are legally mandatory assessments involving an examination of legislative proposals that provide for the collection or disclosure of personal information and used for an information-matching programme in terms of the information-matching guidelines.[91] The Office of the Privacy Commissioner (OPC) issued guidance on their implementation in 1999.[92]

The OPC published a *PIA Handbook* in October 2002 (reprinted in 2007).[93] The *Handbook* defines a PIA as a "systematic process for evaluating a proposal in terms of its impact upon privacy", which can help an agency to identify the potential effects of a proposal on individual privacy, examine how any detrimental privacy effects can be overcome and ensure that new projects comply with the information privacy principles. A PIA is thus a "valuable tool for businesses and governments which take privacy seriously".

The *Handbook* is useful for "projects with a technological component, especially e-commerce and e-government initiatives", though it also aims to help businesses, government departments and others operating offline. According to the *Handbook*, PIAs are an "early warning system" for agencies to enable them to detect and deal with privacy problems at an early stage so that privacy crises are averted.[94] The *Handbook* offers in-depth practical advice on how to prepare privacy impact reports.[95]

The *Handbook* outlines the following reasons for public and private sector agencies to conduct PIAs. First, PIAs are a "tool to undertake the systematic analysis of privacy issues

[88] Similar to some extent to the 2010 body scanners impact assessment conducted by the EU Fundamental Rights Agency, available at the following address: http://fra.europa.eu/sites/default/files/fra_uploads/959-FRA_Opinions_Bodyscanners.pdf.
[89] Spiekermann, op. cit., p. 337.
[90] For contents of IMPIAs, see Privacy Commissioner's Office, "Guidance Note for Departments Seeking Legislative Provision for Information Matching, Appendix B", Wellington, New Zealand, 2008.
[91] Privacy Commissioner's Office, "Operating programmes", Wellington, New Zealand, last upated 30 June 2010. http://privacy.org.nz/operating-programmes/
[92] Privacy Commissioner's Office, "Guidance Note for Departments Seeking Legislative Provision for Information Matching, Appendix B", 2008.
[93] Privacy Commissioner's Office, "Privacy Impact Assessment Handbook", 2007.
[94] Ibid., p. 6.
[95] Ibid., pp. 21-28.

arising from a project in order to inform decision-makers".[96] They thus function as a credible source of information. Second, a PIA enables a business to learn about the privacy pitfalls of a project (rather than its critics or competitors pointing them out) and helps save money and protect reputation. Third, a PIA fixes privacy responsibility with the proponent of a project – project proponents can "own" problems and devise appropriate responses. Fourth, a PIA encourages cost-effective solutions saving the expenses involved with meeting privacy concerns as a "retrofit". Fifth, a PIA leads to an initiative being privacy enhancing rather than privacy invasive. Sixth, reviews of PIA reports by the Privacy Commissioner add value to the PIA process.

The *Handbook* recommends minimising the duplication of PIA efforts by undertaking generic or overarching PIAs where planned projects are very similar.[97] It suggests the following contents for PIA reports: [98]

- Introduction and overview
- Description of the project and information flows
- The privacy analysis (collecting and obtaining information about use, disclosure and retention of information)
- Privacy risk assessment
- Privacy enhancing responses
- Compliance mechanisms
- Conclusions.

The *Handbook* outlines the following risks:

- Failing to comply with either the letter or the spirit of the 1993 Privacy Act, or fair information practices generally;
- Stimulating public outcry as a result of a perceived loss of privacy or a failure to meet expectations regarding the protection of personal information;
- Loss of credibility or public confidence when the public feels that a proposed project has not adequately considered or addressed privacy concerns;
- Underestimating privacy requirements with the result that systems need to be redesigned or retrofitted at considerable expense.

The *Handbook* recommends that the PIA report is best written with a non-technical audience in mind and that it be made publicly available either in full or summary on an organisation's website. It mentions consultation with stakeholders but does not outline the consultative process.[99] The agency conducting the PIA may consult the Privacy Commissioner. It may receive the PIA report for information only or offer feedback and constructive suggestions. PIAs are generally not mandatory in New Zealand, however, section 32 of the Immigration Act 2009 explicitly requires that PIA be conducted if biometric information is processed.

John Edwards, a PIA practitioner in New Zealand, comments that there are "different assumptions among clients, regulators and others as to what the assessment process is

[96] Ibid., p. 11.
[97] Ibid., p. 14.
[98] Ibid., p. 21.
[99] Ibid., pp. 19, 21, 26

intended to do and is capable of delivering". Assessments based primarily on compliance are not "going to be a comprehensive review of privacy issues".[100]

3.7 UNITED KINGDOM

In this section on the United Kingdom, we analyse the Information Commissioner's Office (ICO) Handbook and refer to three specific PIA reports focusing on smart surveillance technologies: (i) the draft Communications Data Bill (Annex C); (ii) Use of Smart Metering Data by Network Operators (Annex D); (iii) Phorm (Annex E).

3.7.1 The ICO PIA Handbook

The Information Commissioner's Office (ICO) is credited with launching privacy impact assessment in the UK. In 2007, the ICO commissioned a team of experts co-ordinated by Loughborough University to study PIAs in other jurisdictions (Australia, Canada, Hong Kong, New Zealand and the United States) and identify lessons to guide PIAs in the UK.[101] That same year, the ICO published a *PIA Handbook* making the UK the first country in Europe to do so. The ICO published a revised version in June 2009.

According to the ICO, a PIA is "a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions."[102]

The Cabinet Office, in its Data Handling Review, called for all central government departments to "introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start".[103] It accepted the value of PIA reports and stressed that they will be used and monitored in all departments.[104] PIAs have thus become a "mandatory minimum measure".[105]

The ICO envisages a PIA as a process, separate from "compliance checking or data protection audit processes", that should be undertaken when it can "genuinely affect the development of a project". (The *Handbook* uses the term "project" as a catch-all; it can refer to "a system, database, program, application, service or a scheme, or an enhancement to any of the above, or an initiative, proposal or a review, or even draft legislation".)

According to the *Handbook*, a PIA is necessary for the following reasons: To identify and manage risks (signifying good governance and good business practice); to avoid unnecessary costs through privacy sensitivity; to avoid inadequate solutions to privacy risks; to avoid loss

[100] Edwards, John, "Privacy Impact Assessment in New Zealand - A Practitioner's Perspective", in Wright and De Hert (eds.), op. cit., 2012.
[101] Information Commissioner's Office (ICO), *Privacy Impact Assessments: International Study of their Application and Effects*, Wilmslow, Cheshire, UK, 2007.
[102] Information Commissioner's Office (ICO), Privacy Impact Assessment - an overview", two-page leaflet. http://www.ico.org.uk/~/media/documents/library/data_protection/practical_application/privacy_impact_assessment_overview.ashx
[103] Cabinet Office, "Data Handling Procedures in Government: Final Report", London, 2008, p. 18.
[104] These are expected to become an integral part of the risk management assessment and will be checked by future "Gateway™" reviews of ICT projects. Gateway reviews are undertaken by an independent team of experienced people and carried out at key decision points in government programmes and projects to provide assurance that they can progress successfully to the next stage.
[105] Cabinet Office, "Cross Government Actions: Mandatory Minimum Measures", London, 2008, section I, 4.4.

of trust and reputation; to inform the organisation's communication strategy and to meet or exceed legal requirements.

The *Handbook* places responsibility for managing a PIA at the senior executive level (preferably someone with lead responsibility for risk management, audit or compliance). The ICO does not play a formal role in conducting, approving or signing off PIA reports. It does, however, play an informative and consultative role in supporting organisations in the conduct of PIAs. The ICO views the PIA process as including identification of and consultation with stakeholders. It distinguishes between a full-scale PIA for large and complex projects and a small-scale PIA for smaller projects. It sets out 15 questions to help determine which is appropriate for a given project.

Roger Clarke has described the UK ICO Handbook as one of the "best practice publications".[106] Despite this, Warren and Charlesworth contend that there are several problems with the UK PIA approach, one of which is the lack of review and oversight. They also point out the "apparent lack of PIA cross-fertilization across departmental boundaries" and the "relatively 'hands-off' oversight" raise doubts about the efficacy of governmental PIA processes. They also point out that there is no formal process of external review of PIAs in the UK by central agencies or by the ICO (which functions largely as an advisory body in this respect).[107]

Warren and Charlesworth further note that, in the UK, as in other places, there is:

- no consistent process for ensuring effective consultation with stakeholders, notably the general public, e.g., a register of on-going 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 statement[108]; and,
- no strategy for ensuing that, where PIA decisions and reports are made publicly available, they are easily accessible, perhaps from a centralised point, e.g., the UK Office of Public Sector Information (OPSI) or the ICO.

Wright highlights how, "In the U.K., there is currently no formal Parliamentary backing for PIAs, and the ICO can only recommend their completion." Moreover, he says that, despite Cabinet Office assurances of PIA usage in all departments, "there is no reporting mechanism in place whereby, for example, a government department is obliged to inform ICO of the PIA or the Treasury in making submissions for funding programs."[109]

[106] Clarke, Roger, "An Evaluation of Privacy Impact Assessment Guidance Documents", *International Data Privacy Law*, Vol. 1, No. 2, 2011, pp. 111-120.
[107] Warren, Adam, and Andrew Charlesworth, "Privacy Impact Assessment in the UK", in Wright and De Hert (eds.), op. cit., 2012.
[108] See, for example: Department for Transport, "Impact Assessment on the Use of Security Scanners at UK Airports: Consultation", London, 2010; Department of Communities and Local Government, "Making Better Use of Energy Performance Certificates and Data: Consultation", London, 2010.
[109] Wright, David, "Should privacy impact assessments be mandatory?", *Communications of the ACM*, Vol. 54, No. 8, 2011, pp. 121-131 [p. 127].

3.8 UNITED STATES

In this section, we first present the general US legal framework that mandates Privacy Impact Assessment, and then we analyse the specific guidance on PIA for the US Department of Homeland Security (DHS). Finally, we include in Annex F a recent DHS PIA report on a smart surveillance technology: the Automated Targeting System.

3.8.1 The US general framework

In the United States, privacy impact assessments for government agencies are mandated under the E-Government Act of 2002. This Act states that PIAs must be conducted for new or substantially changed programmes which use personally identifiable information (PII), which is defined as "any information that permits the identity of an individual to be directly or indirectly inferred".[110] The processing of PII in the US is also covered by Fair Information Practice Principles (FIPP) from the Privacy Act of 1974.

Section 208 of the E-Government Act requires that PIAs must be reviewed by a chief information officer or equivalent official, and should be made public, unless it is necessary to protect classified, sensitive or private information contained in the assessment. Finally, agencies are expected to provide their Director with a copy of the PIA for each system for which funding is requested. Each agency Director must issue guidance to their agency specifying the contents required of a PIA. Additionally, the Homeland Security Act of 2002, which created the Department of Homeland Security (DHS), mandates that the DHS conduct privacy impact assessments and created a Chief Information Officer position with responsibility for these privacy assessments.

Roger Clarke argues that some organisations are seeking to "forestall legislative provisions" for PIAs by creating and supporting industry standards. While a US standard in the form of an American National Standards Institute standard (2004) and an International Standards Organisation (ISO/IEC JTC-1 SC-27 WG-5) standard are in place, Clarke argues that "these processes have lacked the least vestige of consultation with people, or with their representatives or advocates for their interests". In relation to public consultations in general, Clarke further notes that "the ideology of the US private sector is hostile to the notion that consumers might have a participatory role to play in the design of business systems. This is of considerable significance internationally, because US corporations have such substantial impact throughout the world."[111]

On 26 Sept 2003, the Office of Management and Budget (OMB) issued a Memorandum to heads of Executive departments and agencies providing guidance for implementing the privacy provisions of the E-Government Act (OMB, 2003).[112] The guidance directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. Agencies are required to conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available. PIAs should also be performed or

[110] Department of Homeland Security (DHS), "Privacy Technology Implementation Guide", Washington, DC, 2007, p. 8.
[111] Clarke, "Privacy impact assessment: Its origins and development", 2009, p. 128.
[112] Office of Management and Budget, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002", Washington, DC, 2003.

updated when changes to an existing system create new privacy risks.[113] Agencies must also update their PIAs to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form. Government contracts "that use information technology or that operate websites for purposes of interacting with the public" or "relevant" cross-agency initiatives should also be the subject of a PIA.

OMB defines privacy impact assessment (PIA) as "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks".[114] Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected. The OMB specifies what must be in a PIA and, in doing so, it puts an implicit emphasis on the end product, the report, rather than on the process of conducting a PIA.

PIAs must be approved by a "reviewing official", e.g., the agency's chief information officer, other than the official procuring the system or the official who conducts the PIA. Only then is it submitted to the OMB. The PIA document is to be made publicly available. However, agencies are not obliged to make the PIA or a summary publicly available if publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest). Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds. Agencies are required to submit an annual report on compliance with this guidance to OMB as part of their annual E-Government Act status report.

3.8.2 Homeland Security

The Department of Homeland Security PIA guidance has undergone several revisions, and the most recent version, which is discussed here, is the 2010 version. The Department of Homeland Security Act states that the DHS Privacy Officer should also conduct a PIA in situations where one is not required by the E-Government Act, for example, in respect of proposed department rulemaking, to ensure that new rules do not adversely affect privacy, for national security systems, to ensure that such secret programmes appropriately consider and implement privacy protections and for human resources information systems.[115] The guidance describes the PIA as a "living document", which needs to be updated regularly as systems and processes are changed and updated. Here, the DHS appears to focus on PIA as a process, rather than an end result.

The use of a PIA as a form of public engagement is cited in a number of paragraphs in the PIA guidance document. According to the document, privacy impact assessment is "one of the most important instruments through which the Department creates transparency and

[113] See http://www.whitehouse.gov/omb/memoranda/m03-22.html for a list of these examples.
[114] OMB (Office of Management and Budget), 2003.
[115] Teufel III, Hugo, "Privacy Policy and Guidance Memorandum", Memorandum #2008-02, Department of Homeland Security, Washington, DC, 2008.

establishes public trust in its operations".[116] Therefore, the public nature of PIAs is integral to one of its primary functions. The PIA guidance notes and the associated PIA Template describes the components of a DHS PIA.[117] In one of these, officials must describe the procedures to allow individuals access to their information and to correct inaccurate information. Officials must also describe how the project notifies individuals about the procedures for correcting information. Another section discusses auditing and accountability.

According to the guidance, PIAs should be made publicly available as mandated by the E-Government Act. The guidance states that PIAs should be understandable to the general public, although the length and breadth of the report should vary according to the size and complexity of the project. Making the report publicly available demonstrates that the system has privacy protections built in, which were the result of an in-depth analysis.[118] Unlike other agencies, the DHS has an external oversight body that evaluates PIAs and other privacy activities. Independent, third-party review and/or audit of privacy impact assessments is a key factor in the success of PIAs and how they should be conducted to maximise their value. Unfortunately, the number of PIAs that have been subject to such review or audit seems to be rather low.

3.9 EU: RFID PIA FRAMEWORK

The so-called RFID PIA Framework[119] was adopted by industry representatives in January 2011, and was endorsed by the Art. 29 Working Party in February 2011.[120] This document deserves special attention for several reasons. First, the RFID PIA Framework was the first attempt to develop an EU-wide PIA system, so that some might regard it as a precursor and potential model for the development of privacy impact assessments in the EU (cf. also sections 1.1 and 5.2). Its roots lie in the text of the Commission Recommendation on RFID published in May 2009,[121] in which the Commission recommended to "Member States [that they] should ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments".[122] The goal was to trigger a form of self-regulation, but at the same time maintain a form of control on the eventual document via the required endorsement of the Art. 29 WP.

The 2009 Recommendation provided also raw guidelines on the core elements of the framework, concerning in particular the scalability of the assessment exercise, the measures to mitigate risks, the designation of a person responsible for the follow-up and update of the assessment and the consequent solutions, and the communication of the report to competent

[116] DHS (Department of Homeland Security), "Privacy Impact Assessment Template", Washington, DC, 2010.
[117] Ibid.
[118] Ibid., p. 9
[119] *Privacy and Data Protection Impact Assessment Framework for RFID Applications*, 12 January 2011. Herein after: RFID PIA Framework.
[120] Art. 29 WP, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180, Brussels, 2011. It is worth mentioning that the Art. 29 WP had previously rejected a first proposal for a RFID PIA Framework: cf. Art.29 WP, Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 175, Brussels, 2010.
[121] Commission of the European Communities, Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C(2009) 3200 final, Brussels, 2009.
[122] Ibid., § 4.

authorities if it was requested.[123] Furthermore, the Recommendation insists on the specific relevance of the retail sector, and explicitly links the outcome of the impact assessment to the possible de-activation of RFID tags.

The main elements of the Commission guidelines are translated and clarified in the RFID PIA Framework, especially the scalability of the assessment itself and the related "decision tree".[124] This is the core of the RFID PIA Framework, as it introduces a sort of two-step approach, or a "two-phase" PIA process. The first step is the initial analysis of the RFID system, focusing on "the nature and sensitivity of the data it deals with, the nature and type of processing or stewardship of information it engages in, and the type of RFID Application in question".[125] On the basis of this evaluation, a decision has to be taken on the need or not to conduct a PIA, and on which scale ("full" or "small scale PIA").[126] The document also provides guidance on the risk assessment procedure to complete a PIA, leading to the drafting of a PIA report: "characterisation of application", "identification of risks", "identification and recommendation of controls", "documentation of resolution and residual risks".[127] The PIA Framework includes a set of annexes that provide for a list of "privacy targets", "privacy risks" and "examples of RFID application controls and mitigating measures",[128] so that the document can be considered a quite ready-to-use manual or introduction to privacy impact assessment. Furthermore, the prominence accorded to the scalability of the assessment can be considered in itself an argument to promote a wider diffusion of the practice, especially given the lack of binding force of both the Framework and the Commission Recommendation. The two-phase process underlines a potential weakness of the scheme: the conduct of the initial analysis. This part of the PIA process is much less defined than the following risk assessment, and is largely left in the hands of the proponents of the new system. Surely, this is consistent with a self-regulating, voluntary approach to PIA: it reduces the burden of the exercise for many stakeholders and potentially increases the acceptability and the uptake of the practice. The two-step approach is also becoming a common strategy of impact assessment, and for this reason further attention should be dedicated to the design of the initial analysis, and to the introduction of guarantees for other concerned stakeholders to provide inputs at this stage.

Finally, it should be noted that, despite the explicit reference to privacy, the RFID PIA Framework is largely, if not only, built on data protection principles and legislation. The shift towards a conflation of privacy into data protection is a rather typical phenomenon in the EU (cf. section 5.2), but it still raises questions concerning the effective scope of PIA, especially in relation to forms of smart surveillance that operate at the borders of the definition of personal data. The RFID PIA Framework is potentially interesting, as it is partially the result of intense societal and institutional debate about the potential risks of a technology that has often questioned the definition of personal data. From this perspective, there is value in development of a PIA system aimed at tackling these potential risks, both in terms of privacy and data protection.

[123] Ibid., § 5.
[124] RFID PIA Framework, pp. 5-11.
[125] RFID PIA Framework, p. 6.
[126] RFID PIA Framework, pp. 6-7.
[127] RFID PIA Framework, pp. 9-10.
[128] RFID PIA Framework, pp. 13-20.

3.10 A COMPARISON OF PIA POLICIES AND METHODOLOGIES IN THE SURVEYED COUNTRIES

The table on the following two pages identifies the principal similarities and differences between the various PIA guidance documents analysed in this chapter, based on the recommendations and features that make a "good" PIA (i.e., the 18 criteria identified in section 2.3). These features help us toward our ultimate goal of an optimised PIA methodology suitable for assessing proposed smart surveillance systems and practices in Europe.

Features The PIA guide…	Australia		Canada			Ireland	NZ	UK	US	
	National	Victoria	National	Ontario	Alberta				OMB	DHS
reviewed here, was published in	May 2010	Apr 2009	Aug 2002	Dec 2010	Jan 2009	Dec 2010	Oct 2002-2007	June 2009	Sept 2003	June 2010
says PIA is a process	✓	✓	✓	✓		✓	✓	✓	✓	✓
contains a set of questions to uncover privacy risks (usually in relation to privacy principles)	✓	✓	✓	✓		✓	✓	✓		✓
targets companies as well as government	✓	✓			✓	✓	✓	✓		
addresses all types of privacy (informational, bodily, territorial, locational, communications)	✓	✓		✓						
regards PIA as a form of risk management	✓		✓	✓		✓		✓	✓	✓
identifies privacy risks	✓	✓	✓	✓		✓	✓	✓		
identifies possible strategies for mitigating those risks		✓					✓			
identifies benefits of undertaking a PIA	✓	✓	✓			✓	✓	✓		
supports consultation with external stakeholders	✓	✓				✓		✓		
encourages publication of the PIA report	✓	✓	summary		summary		✓	✓	✓	✓
provides a privacy threshold assessment to determine whether a PIA is necessary	✓	✓	✓			✓		✓	✓	✓
provides a suggested structure for the PIA report	✓	✓	✓		✓		✓	✓	✓	✓
defines “project” as including legislation and/or policy		✓								
says PIAs should be reviewed, updated, ongoing throughout the life a project	✓	✓			✓	✓	✓	✓	✓	✓
explicitly says a PIA is more than a compliance check	✓	✓	✓	✓				✓		

Features The PIA guide…	Australia		Canada			Ireland	NZ	UK	US	
	National	Victoria	National	Ontario	Alberta				OMB	DHS
The PIA policy provides for third-party, independent review or audit of the completed PIA document.			✓		✓		✓		✓	✓
PIA is mandated by law, government policy or must accompany budget submissions.			✓	✓	✓	✓		✓	✓	✓
PIA reports have to be signed off by senior management (to foster accountability).		✓	✓	✓	✓	✓			✓	✓

4 BEST ELEMENTS AND KEY CHALLENGES

From our review and analysis of the above-referenced PIA methodologies, we have identified elements (practices) that could be used to construct a state-of-the-art European PIA policy and methodology. Following the structure of the discussion of "good" PIA criteria above, this section briefly categorises our recommendations for an optimised PIA methodology for the EU in terms of what a PIA should be, how it should be carried out, what it should contain and how organisations undertaking PIAs should be supported or encouraged. Several of these "best elements" are mentioned, albeit briefly, in Article 33 of the European Commission's proposed Data Protection Regulation. We refer to those. Where the best elements are absent, we recommend that decision-makers in the European Commission, Member States and industry take into account the "best elements" identified here in formulating an optimal PIA policy.

The final section of this chapter discusses the suitability of these elements for assessing smart surveillance projects and points out some key open issues and limitations of PIAs in this respect.

4.1 WHAT A PIA SHOULD BE

A PIA is more than a check that a project complies with existing legislation or privacy principles – it should engage stakeholders in identifying risks and privacy impacts that may not be caught by a compliance check. Article 33(4) of the proposed Data Protection Regulation support this too; it says a data controller "shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations".

The needs and rights of individuals whose personal information is collected, used or disclosed should be the focus of the corresponding PIA report. Article 33(4) of the proposed Regulation provides this focus: "The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned." Yet the objective of a PIA is not simply to produce a PIA report. The report documents the PIA process. A PIA should continue after the report is published. PIAs should be embedded as part of the project management framework. The PIA should be reviewed and updated throughout the duration of a project. Article 33, as currently drafted, seems to place its emphasis on preparation of the PIA report. If Article 33 is revised before the proposed Regulation is adopted, then the EC could add some wording that emphasises PIA as a process.

A successful PIA is only a tool; its utility depends on how it is used and who uses it. It depends on organisations having the correct processes in place to carry out and follow up the PIA. Ultimately, the proponent of a proposal should be responsible for privacy. The proponent should "own" the identified problems and devise appropriate responses in the design and planning phases.

4.2 HOW AND UNDER WHAT CIRCUMSTANCES IT SHOULD BE CARRIED OUT

PIAs should be undertaken with regard to any project, product, service, programme or other initiative, including legislation and policy, as explicitly referenced in the Victoria *Guide* and the UK Information Commissioner's Office (ICO) *Handbook*. Article 33 says a PIA (or rather a data protection impact assessment) should be carried out "where processing operations present specific risks to the rights and freedoms of data subjects". (The Article 29 Data Protection Working Party has suggested amending this provision by inserting the words "likely to" before "present".[134])

A PIA should be started early, so that it can evolve with and help shape the project, so that privacy is "built in" rather than "bolted on". A PIA should be initiated when it is still possible to influence the design of a project. The findings and recommendations of the PIA should influence the final detail and design of the project. Article 33 implies that a PIA should be conducted early when it refers to "the envisaged processing operations".

The Victoria *Guide* points out that a project need not be large to be subject to a PIA, nor is the size or budget of a project a useful indicator of its likely impact on privacy. The project does not even need to involve recorded "personal information"; for example, a program that may include the need for bodily searches can still impact on privacy even if no personal information is recorded.

PIAs should be applied to cross-jurisdictional projects as well as any other project that impacts privacy. PIAs should invite comments from privacy commissioners of all jurisdictions where projects are likely to have significant privacy implications and ensure that such projects meet or exceed the data protection and privacy requirements in all of the relevant countries. Article 33 makes no mention of cross-jurisdictional projects, although Article 33(6) says the EC shall be empowered to adopt delegated acts "for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks" which would give the EC some scope for including cross-jurisdictional projects within the PIA purview. It should also be noted that recital 72, while it does not include cross-jurisdictional projects per se, does say "There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity." The EC's proposed Data Protection Regulation should include a reference to PIAs for cross-jurisdictional projects.

4.3 WHAT IT SHOULD CONTAIN

The PIA should identify information flows, i.e., who collects information, what information do they collect, why do they collect it, how is the information processed and by whom and where, how is the information stored and secured, who has access to it, with whom is the information shared, under what conditions and safeguards, etc. Information privacy is only one type of privacy. A PIA should also address other types of privacy, e.g., of the person, of personal behaviour, of personal communications and of location. Article 33 focuses on "data

[134] Article 29 Data Protection Working Party, "Opinion 1/2012 on the data protection reform proposals", Working Paper 00530/12/EN, WP 191, Brussels, 2012, p. 15.

protection" only. Hence, this is a major limitation of the proposed Regulation as currently framed.

A PIA guidance document should include an indicative list of privacy risks an organisation might encounter in initiating a new project, but should caution project managers and assessors that such a list is not exhaustive. The questions most PIA guidance documents include can help stimulate consideration of possible privacy impacts. Article 33(2) contains a list of risks. The PIA should also include a discussion of what solutions to the privacy risks were identified, what potential changes were considered to mitigate those risks and how the system or technology was modified or changed to address those risks. Article 33(3), already cited above, addresses this point. The PIA should specify who undertook the PIA, how they can be contacted for more information and where to find further information and other sources of help and advice. Article 33 does not go into this detail.

4.4 HOW ORGANISATIONS SHOULD BE SUPPORTED OR ENCOURAGED TO UNDERTAKE PIAS

PIA guidance documents should be aimed at not only government agencies but also companies or any organisation initiating or changing a project, product, service, programme, policy or other initiative that could have impacts on privacy. Article 33 refers to data controllers and does not limit itself to just government agencies. Hence, companies would also have to adhere to its provisions.

A guidance document aimed at a broader set of stakeholders should contain the following information:

- It should identify the variety of skills required for undertaking a privacy impact assessment and completing a privacy impact report. This will help the project manager as it highlights the importance of bringing together people with the right competencies to be members of the PIA team and to conduct a PIA. Article 33 does not go into this level of detail.
- It should offer a structured approach to the PIA process and preparation of a PIA report, allowing organisations to use the document to guide their PIA process in a manner "appropriate to their circumstances". Article 33 does not go into this level of detail, other than to identify the risks whereby a PIA should be conducted, and describing what a PIA report should contain "at least".
- It should not only set out various risks, but also possible strategies for mitigating those risks, as the ICO and Victoria PIA guidance documents do. But, again, such lists of risks should only be regarded as indicative, not exhaustive. Article 33 does not go into this detail.
- It should include a threshold assessment, the aim of which is to help project managers determine whether a PIA is needed. Service providers should routinely undertake a threshold assessment for every new project as well as proposals to amend existing information systems, sources or processes to determine whether its potential privacy impact necessitates a PIA. While Article 33 does not refer to a threshold assessment specifically, it does identify the risks whereby a PIA should be conducted.
- It should highlight the benefits of undertaking PIAs and how they will help an organisation, since many organisations may resist undertaking a PIA. For example, in New Zealand, PIA is regarded as an "early warning system". Other PIA guidance documents have picked up on the same wording. Article 33 refers only to the risks. There is no mention of the benefits.

- It should include a list of references to other PIA guidance documents and actual PIA reports. It should draw on the experience of others to make the guidance more practical and effective. The New Zealand handbook has a useful bibliography of national and international PIA resources. Article 33 does not go into this level of detail.

Data protection authorities and privacy commissioners should make it easy for project managers, assessors and others to find a link for downloading the PIA guidance, preferably on their home page. Governments especially should create a central registry of PIAs, so that particular PIA reports can be easily found. Publication of PIA reports will enable organisations to learn from others. Article 33 does not contain such a provision.

We can also identify a number of requirements for the actual PIA report, such as:

- It should normally be publicly available and posted on an organisation's website so as to increase transparency and public confidence. If there are security, commercial-in-confidence or other competitive reasons for not making a PIA public in full or in part, the organisation should publish a redacted version or, as a minimum, a summary. A properly edited PIA report can balance the security and transparency interests. Article 33 makes no explicit mention regarding publication of the PIA report, but presumably the Commission could make publication mandatory as a delegated act for which it shall be empowered (assuming the legislation is adopted, of course).
- It should be updated from time to time, as happens in several countries. Article 33 is silent on this.
- A PIA should be part of an organisation's overall risk management practice. The PIA should have up-front commitment from an organisation's senior management. Senior management should be held accountable for the proper conduct of a PIA and should sign off the PIA report, as the Treasury Board Secretariat (TBS) of Canada requires. Funding submissions should be accompanied by a PIA report. TBS policy also requires that government departments and agencies copy the PIA report to the Privacy Commissioner, which we also find to be a good practice. Article 33 does not contain such a provision.
- PIA reports and practices should be audited, just as a company's accounts are audited. An audit will help improve PIA practice, as the Office of the Privacy Commissioner of Canada found following its major audit of PIAs in 2007. To increase their effectiveness, PIAs should be subject to external oversight. Article 33(7) says "The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment". In addition to PIA guidance documents, the government of Canada has developed a PIA Audit Guide, "intended as a reference tool for Internal Auditors in the Government of Canada and may also be of assistance to the privacy community, including PIA Coordinators". European data protection authorities or the Art. 29 WP could also develop PIA audit guides, too.
- The PIA should be reviewed and approved at a senior level with each PIA report being quality assured by senior management. US experience suggests the value of ensuring the chief privacy officer has a senior position, has a high degree of independence within the organisation and participates in high-level deliberations. A chief privacy officer, privacy office and/or PIA process should be statutorily mandated by an external agency. An adequate number of specially trained, privacy-focused staff members should be embedded throughout the organisation.

Data protection authorities or other leaders should identify and publish particular PIA reports as examples of good practice. Also, while DPAs may not generally approve PIAs, they may

review them and provide guidance on improving them. Article 33 does not contain such provisions.

4.5 CHALLENGES FOR PIAS TARGETED TO SMART SURVEILLANCE

Surveillance technologies and applications raise critical data protection and privacy issues, and are thus a prime target for a PIA. Mandating a (properly fashioned) PIA for surveillance-rated projects would support what James Rule calls "to *politicize* the working and extension of surveillance".[135] The emergence of smart surveillance projects makes such PIAs particularly important due to their extended reach, coverage and the high levels of automated decision-making. Wright et al. define smart surveillance as follows (our emphasis added):[136]

> Smart surveillance systems are those capable of extracting application-specific information from captured information (be it digital images, call logs or electronic travel records) in order to generate high-level event descriptions that can ultimately be used to **make automated or semi-automated decisions**. Smart surveillance systems inherently offer **a high level of scalability**, as they in turn can act as input to other surveillance systems. Smart surveillance systems contribute to social reconfigurations in ways that essentially differ from previous surveillance techniques, especially by introducing new folding processes of the spatial and temporal dimensions with the purpose to go beyond "mere" re-action.

However, developing a PIA for smart surveillance entails challenges that derive from: (1) the uncertainty and complexity surrounding the object of the assessment (smart surveillance technologies), as well as the multitude of actors involved; and (2) the definition of the criteria used to make the assessment (the application of DP principles, privacy and other rights in smart surveillance practices).

4.5.1 Uncertainty and complexity surrounding smart surveillance technology

As discussed in SAPIENT deliverable D1, surveillance systems are increasingly using a heterogeneous "assemblage" of technologies.[137] Instead of a single technology, e.g., video, a PIA for a smart surveillance project will most likely need to address a wide variety of technologies and corresponding technical capabilities (and limitations). It will be challenging to ensure that analysts have the expertise to properly understand the increasingly complex systems. PIA guidance documents (cf. section 4.4) should provide sufficient technical background and discuss the various capabilities and limitations of such technologies, in order to aid both government agencies and commercial data controllers to perform meaningful PIAs on surveillance projects.

A wide range of technologies will also imply a much broader set of privacy threats beyond information privacy, such as communication privacy or bodily privacy, as well as fundamental rights and ethical values (cf. Chapter 5). This not only complicates the analysis, but will also have implications for the selection of stakeholders, as it might significantly enlarge the number of involved parties.

[135] Rule, James B., *Privacy in Peril*, Oxford University Press, 2007, p. 195.
[136] Wright, David, Michael Friedewald, Serge Gutwirth, Marc Langheinrich, Emilio Mordini, Rocco Bellanova, Paul De Hert and Kush Wadhwa, "Sorting out smart surveillance", *Computer Law & Security Review*, Vol. 26, No. 4, 2010, pp. 343-354.
[137] Gutwirth et al. 2012, pp. 79-84.

Smart surveillance relies on advanced sensing technologies and sophisticated analytical algorithms, in order to collect, process, and interpret the direct and indirect actions of people. The capabilities of such hardware and software might not be known at the start of a surveillance project, making it difficult to draw up a conclusive set of implications in a PIA. This is a basic characteristic of any emerging technology, requiring the need to be proactive in asserting the underlying technological development or when imagining future impacts. While a certain level of uncertainty is inherent in any impact assessment, smart surveillance systems exacerbate such uncertainty. Methods from technology impact assessment, such as the precautionary principle, may provide inspiration for a more forward-looking PIA methodology in such situations.[138]

A discussed, the true power of future smart surveillance systems lies in the combination of a large range of data collection and processing capabilities into an ever expanding array of interconnected surveillance tools, where the output of one system is the input to another. This interconnectedness not only increases the number of technologies, but also the number of actors involved in both the envisioned surveillance system, and in future extensions and alterations of the system. PIAs focused on surveillance systems will need to pay particular attention to the combinability of individual systems into larger systems, as this might greatly influence the capabilities and subsequently implications of such "assemblages".

[138] Wright, David, Raphaël Gellert, Serge Gutwirth and Michael Friedewald, "Minimizing technology risks with PIAs, precaution and participation", *IEEE Technology & Society*, Vol. 30, Issue 4, Winter 2011, pp. 47-54.

5 HUMAN RIGHTS ISSUES IN SMART SURVEILLANCE

5.1 FUNDAMENTAL RIGHTS IMPACTS OF SURVEILLANCE

5.1.1 Privacy may not be enough to tackle surveillance

As argued in the first deliverable of the SAPIENT project, surveillance raises issues that potentially go beyond privacy. The deliverable adequately recalled the debate organised by the journal *Surveillance & Society* (Issue 4 of 2011) around the adequacy of privacy as the "organising matrix of the field". Without restating the debate (already accurately outlined in the deliverable), it suffices to say that, at least in the context of surveillance, privacy has been criticised for being too narrow, therefore impeding scholars to take stock of the many complexities of current surveillance practices.[139]

If such an assumption were to be proved correct, then the point could be made that (D)PIA would not be enough to address the risks posed by surveillance practices to individuals, since precisely, these risks would go beyond the right to privacy.

The fundamental rights analysis carried out in the same deliverable seems to confirm such a stance. The analysis identifies two issues: discrimination and the reversal of the presumption of innocence as an element of the right to fair trial and due process.[140]

This chapter addresses three distinct issues: discrimination, reversal of the presumption of innocence (which can actually be a form of discrimination and a violation of the right to a due process), and violation to the right of a fair trial and due process as such.

5.1.2 Discrimination

Discrimination might well be one of the most important and distinctive legal outcomes of smart surveillance. As explained in SAPIENT D1.1, one of the characteristic features of contemporary surveillance is dataveillance. This in turns enables profiling activities that are instrumental for the purposes of proactivity and prevention.[141]

The proactive, preventive, *ex ante* nature of smart surveillance has led David Lyon to qualify it as a process of social sorting.[142] In fact, preventing crimes from happening entails categorising people on the basis of the potential threat they might pose, that is, predicting events on the basis of predetermined patterns, in this case, suspect, threatening or abnormal behaviours.

Yet, because the accuracy of such criteria is far from proven, and relies upon a wide variety of factors, the point can be made that sorting people according to predetermined patterns amounts to an unjustified and not proportional difference of treatment, that is, discrimination.

[139] Gutwirth et al. 2012, pp. 18-19.
[140] Gutwirth et al. 2012, pp. 85-126.
[141] Gutwirth et al. 2012, pp. 14-15.
[142] Lyon, David (eds.), *Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination*; Gutwirth et al. 2012, p. 102.

The discrimination can be direct or indirect. Direct discrimination is a difference of treatment based upon factors such as ethnicity, gender, age, disability, etc. Indirect discrimination can be defined as a difference of treatment based upon apparently neutral provisions, criteria or practices that have the "side effect" of discriminating against one of the specific forbidden grounds. Apparently neutral proxies such as specific movements, meal choices (in the case of airplanes) can actually be linked to a specific ethnicity or faith.[143]

Finally, in its Hüber case, the European Court of Justice (ECJ) acknowledged that the secondary use for law enforcement purposes of non-nationals data stored in a population register amounted to discrimination.[144]

5.1.3 The nexus between discrimination and reversal of the burden of proof

Smart surveillance may lead to a reversal of the presumption of innocence. Because of the constant, pervasive and indiscriminate surveillance citizens have to endure, the point has been made that the presumption of innocence has been turned into a presumption of guilt. In this sense, everybody is guilty until proven innocent. The Marper case provides a good example.[145] The European Court of Human Rights (ECtHR) ruled that the storing of personal data such as fingerprints, DNA profiles and cell samples belonging to potentially innocent citizens bore a risk of stigmatisation in that it created a shadow of suspicion. The storage of innocents' data in databases dedicated to criminal identification (and mainly dedicated to the storage of data of convicted offenders) for preventive purposes tends to reverse the presumption of innocence.[146]

This *shadow of suspicion*, this reversal of the presumption of innocence into a presumption of guilt can be analysed as a stigmatisation akin to a form of discrimination (as the ECtHR did).[147] However, it can also be interpreted in the light of a right to a fair trial and due process.[148]

5.1.4 Right to fair trial and due process

The right to a fair trial is enshrined in Art. 6 of the European Convention for Human Rights (ECHR). It concerns both civil and criminal proceedings.[149]

---

[143] See Gellert, Raphaël, Katja de Vries, Paul De Hert, Serge Gutwirth, "A Comparative Analysis of Anti-Discrimination and Data Protection Legislations", in Bart Custers, Toon Calders, Bart Schermer and Tal Zarsky (eds.), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2012, pp. 61-89.

[144] ECJ, *Huber*, C-524/06, 2008.

[145] S. and Marper v. The United Kingdom, Applications nos. 30562/04 and 30566/04, European Court of Human Rights, Judgment of 4 December 2008, § 122.

[146] Gonzalez Fuster, Gloria, Paul De Hert, Erika Eva Ellyne and Serge Gutwirth, "Huber, Marper and Others: Throwing new light on the shadows of suspicion", *INEX Policy Brief*, No. 11, Centre for European Policy Studies (CEPS), 2010, pp. 4-6.

[147] On the difference between discrimination and stigmatisation, see Quinn, Paul, and Paul De Hert, "Self-Respect – A Rawlsian Primary Good unprotected by the European Convention on Human Rights and its lack of a coherent approach to stigmatisation?", on file with the authors.

[148] As was the case in Gutwirth et al. 2012, p. 104.

[149] Art 6.1 states that: "In the determination of his civil rights and obligations or of any criminal charge against him".

It can be argued that smart surveillance potentially violates such a right. Art. 6.2 contains the right to the presumption of innocence. So in this sense, the reversal of the presumption is not discrimination anymore, but a violation of Art. 6 ECHR.

But Art. 6 can be violated in other ways too. Whereas Art 6.1 contains the general provision on the right to a fair trial, Art 6.3 contains defence rights that are to be respected in the course of criminal proceedings.[150]

Inscribing people on a list of terrorist suspects is a pre-emptive measure that can violate the right to a fair trial. In the Kadi case, the ECJ found that the Council of the European Union Decision implementing United Nations Security Council Resolutions 1267 and 1333 putting Kadi on a list of terrorist suspects and ordering the freezing of his assets breached the right to a fair trial since no evidence (justifying his inclusion on the list and subsequent freezing of assets) was communicated to him.[151]

But the right to a fair trial can be violated in other ways too. One can think of the opaque functioning of profiling algorithms used to decide whether a person is a suspect or not. How do they fit with the right of citizens "to be informed promptly, in a language which [the citizen] understands and in detail, of the nature and cause of the accusation against [the citizen]"?

Equally, it must not be taken for granted that Courts will accept the validity of evidence gathered through such smart surveillance measures.

5.2 THE PROPOSED DATA PROTECTION REGULATION AND THE POSSIBILITY FOR SIAS

As already mentioned above, Art. 33 of the proposed General Data Protection Regulation (GDPR) provides for data protection impact assessments.[152]

---

[150] Art 6.3 states that:
Everyone charged with a criminal offence has the following minimum rights:
a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
b) to have adequate time and facilities for the preparation of his defence;
c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

[151] Joint cases C-402/05 P and C-415/05 P Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities. See Julian Kokott, Sobotta, Ch., "The Kadi Case – Constitutional Core Values and International Law – Finding the Balance?", *The European Journal of International Law*, Vol. 23, No. 4, 2012, pp. 1015-1024.

[152] Art. 33 reads as follows:
"1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
2. The following processing operations in particular present specific risks referred to in paragraph 1:
(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).
3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks,

In the following paragraphs, we will undertake an analysis of this article in light of the findings of the previous section, namely, that (smart) surveillance practices may have fundamental rights impacts that go beyond the rights to data protection and privacy. Hence, the main question to be addressed is whether Art. 33 GDPR can serve as a "legal hook" for SIAs.[153] In answering this question, we will touch upon the issue of delegated and implementing acts. Finally, the proposed Directive will also be included in the analysis, as smart surveillance systems are first a matter of law enforcement practices (though not exclusively, cf. SAPIENT, D3.1). In this respect, what are the SIA possibilities for which the proposed Directive provides (if any)?

This article is a general provision on impact assessments. Rather than spelling out the specific methodology according to which such assessments should be lawfully carried out,[154] the provisions of the article specify the conditions that require undertaking the assessment.

According to Art 33.1, the assessment should be carried out when "Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes".

Art. 33.2 spells out more in details what these specific risks may be. Some of the risks included have a very strong kin with smart surveillance practices that have been examined in SAPIENT D1.1. Namely they are:

> (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;
> (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;
> (c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;

---

safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.
4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.
5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.
6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.
7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)."

[153] Entailing it does not provide for their content, which is the point of the SIA methodology in D3.2.

[154] For (D)PIA methodologies and best practices, see, e.g., Wright, David, "Privacy and Ethical Assessment Framework", in Silvia Venier and Emilio Mordini (eds.), *PRESCIENT Deliverable 4 : Final Report — A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies*, 2013, pp. 87–103.

(d) personal data in large scale filing systems on children, genetic data or biometric data.

Art. 33(2)(a) concerns profiling measures, Art 33(2)(b) concerns the use of sensitive information for taking decisions concerning individuals. This might pertain to profiling (automated decisions), but not necessarily. However, it puts the emphasis on the processing of sensitive data. Art. 33(2)(c) explicitly mentions surveillance, and Art 33(2)(d) is about the storage of personal data in databases.

It is interesting to see that all the risks (but for one) that will trigger a DPIA deal with risks associated with smart surveillance activities.

So even if a specific methodology for surveillance impact assessments (SIAs) has to be devised, one which would take into account infringements on issues in addition to privacy and data protection issues (precisely because Art. 33 does not provide for any specific methodology), the point can be made that Art. 33 provides a legal basis for doing so. Furthermore, Art. 33 spells out only the situations where DPIAs are mandatory, but it does not preclude data controllers (or processors) to carry out SIAs on a voluntary basis.

Another issue to touch upon is that of the European Commission's delegated and implementing acts. Art. 33(6) provides that the Commission shall be empowered to adopt delegated acts that will clarify the criteria according to which a DPIA is mandatory. It will also adopt delegated acts that will further clarify how the impact assessment should be conducted.[155] Such delegated acts could provide for the specificity of a surveillance impact assessment.

Delegated acts are based on Art. 290 of the Treaty on the Functioning of the European Union (TFEU). According to the latter, they can be adopted to supplement or to amend non-essential parts of the legal act at stake.[156,157]

[155] Art. 33(6) reads as follows: "The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises."

[156] Art. 290 TFEU reads as follows:

"1. A legislative act may delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of the legislative act. The objectives, content, scope and duration of the delegation of power shall be explicitly defined in the legislative acts. The essential elements of an area shall be reserved for the legislative act and accordingly shall not be the subject of a delegation of power.

2. Legislative acts shall explicitly lay down the conditions to which the delegation is subject; these conditions may be as follows:

(a) the European Parliament or the Council may decide to revoke the delegation;

(b) the delegated act may enter into force only if no objection has been expressed by the European Parliament or the Council within a period set by the legislative act.

For the purposes of (a) and (b), the European Parliament shall act by a majority of its component members, and the Council by a qualified majority.

3. The adjective 'delegated' shall be inserted in the title of delegated acts."

[157] See also Article 29 Data Protection Working Party, Input on the proposed implementing acts adopted on 22 January 2103, WP 200, Working Document 01/2103. See in particular the section on "the difference between delegated and implementing acts", p. 2. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp200_en.pdf

Art. 33(7) concerns the implementing acts.[158] Implementing acts are based upon Art. 291 TFEU.[159] Contrary to delegated acts, their purpose is more limited as they aim at specifying the technical conditions for implementing provisions already to be found in an instrument of legislative status (e.g., Directive or Regulation).[160]

The question to be asked here is the role that these acts will play. Will the delegated (and implementing) acts be full guidelines explaining at length how all the constitutive elements of a DPIA should be conducted (as is the case in Canada, for instance, discussed above in Chapter 3)? Or will they, on the contrary, follow a contemporary trend that consists in having regime-specific guidance material, and therefore only provide for basic indications on how to conduct an assessment?[161]

Last, the relationship with the proposed Directive has to be analysed.

Contrary to the Proposal for a Regulation, the Proposal for a Directive contains no such provisions on DPIAs.[162]

Yet, and similarly to the proposed Regulation, the Directive contains a provision on data protection by design (DPbD).[163] In this respect, one has to keep in mind the intricate relation between DPIA and DPbD. One could say indeed that they are, if not coextensive, at least part of the same process of technology improvement. In this respect, it is no surprise if the Art. 29 WP has argued in its opinion on the RFID PIA framework that, among its many goals, "A PIA is a tool designed to promote 'privacy by design'".[164]

Furthermore, one should keep in mind (as evidenced above) that many of the privacy risks deemed to trigger a DPIA according to Art. 33 have a strong link with smart surveillance

[158] Art. 33(7) reads as follows: "The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)."

[159] Art. 291 TFEU reads as follows:

"1. Member States shall adopt all measures of national law necessary to implement legally binding Union acts.

2. Where uniform conditions for implementing legally binding Union acts are needed, those acts shall confer implementing powers on the Commission, or, in duly justified specific cases and in the cases provided for in Articles 24 and 26 of the Treaty on European Union, on the Council.

3. For the purposes of paragraph 2, the European Parliament and the Council, acting by means of regulations in accordance with the ordinary legislative procedure, shall lay down in advance the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers.

4. The word 'implementing' shall be inserted in the title of implementing acts."

[160] See again, WP 200, op. cit., p. 2.

[161] As is the case with the Art. 29 WP-endorsed RFID PIA framework and the proposed smart grids PIA framework. The Art. 29 WP has recently issued an Opinion on the latter. See Art. 29 Working Party, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force, WP 205, Adopted on 22 April 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf

[162] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM/2012/010 final - 2012/0010 (COD), 25 January 2012.

[163] Respectively, Art. 19 of the proposed Directive, and Art. 23 of the proposed Regulation.

[164] Article 29 Working Party Group, WP 180, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, adopted on 11 February 2011, p. 7. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

practices, not least of which are profiling operations, which have now a dedicated Article in both instruments (Art. 20 of the Regulation and Art. 9 of the Directive).[165]

Finally, it is important to remember the hybrid nature of data processing operations for law enforcement purposes, as they often involve private parties that are normally subject to the current Directive (and future Regulation).[166] In SAPIENT D1.1, we have alluded to this blurring of legal realms.

Taking all these elements into considerations, the point could be made, *contra legem ferenda*, that a DPIA could be required for data processing operations for law enforcement purposes.

As a conclusion, it can be argued that, though a specific SIA methodology still needs to be crafted (since PIAs cannot alone address all the surveillance-related issues), Art. 33 GDPR provides nonetheless a "legal hook" for such future SIAs. Furthermore, a daring analysis of the proposed Directive can extend the same conclusions to the latter instrument.

[165] Both instruments fall short of defining profiling, but rather, make explicit the rights of data subjects with regard to these operations.
[166] Cf. Gutwirth et al. 2012.

6 CONCLUSION

Europe has an opportunity to develop a state-of-the-art PIA and SIA policy and methodology. It should benefit from the experience of others, notably the countries analysed in this paper, and construct a PIA framework based on the "best" elements of existing policies and methodologies, i.e., those elements recommended by the authors as well as other PIA experts. This paper has provided a comparative analysis of different PIA methodologies in eight countries that have the most experience of PIA and identified some of the elements that could be used in a European PIA policy and methodology. To our knowledge, this paper is one of the first to make a comparative analysis of different PIA methodologies (while drawing on papers produced by leading PIA experts and pioneers) with a view to extracting the elements that can be used in constructing a best practice or optimised PIA for use in the European Union and that can form the basis for a surveillance impact assessment methodology. The findings of this paper can be used by policy-makers and industry decision-makers to "flesh out" the rather sketchy provisions for PIA in Article 33 of the proposed Data Protection Regulation. In the preceding section of this paper, we have identified which of our findings correlate with Article 33 and where there are lacunae in Article 33 that could be filled by our recommendations.

Article 33 of the EC's proposed Data Protection Regulation makes PIA mandatory "Where processing operations present specific risks to the rights and freedoms of data subjects". While Article 33 has much to commend it, its emphasis seems to be more on the PIA report rather than on the PIA process. The Art. 29 Working Party has suggested some helpful improvements to Article 33. In addition to those, the EC (and an SIA handbook) could usefully highlight the benefits of a PIA and/or SIA.

A key question for the SAPIENT consortium has been the adequacy of a PIA to address the range of issues raised by the deployment of surveillance technologies and systems. To help address this question, the consortium analysed several PIA reports focussed on surveillance systems (see the Annex). In the following paragraphs, we highlight our key findings:

From our analysis of the Australian Privacy Impact Assessment: Preliminary Report: Telecommunications (Interception and Access) Act 1979 [TIA] Reform, it seems that a PIA with its focus on privacy was not by itself adequate to examine the implications of the TIA Act Reform – at least in the sense that the PIA not only takes into account the Information Privacy Principles, but it draws on a broader framework aimed "at making decisions about the use of intrusive powers".

The Canadian Automatic License Plate Recognition (ALPR) system is a surveillance system but it appears that a PIA is adequate is adequate to address the risks such a system could raise. One can question how adequate is the specific PIA in this instance, but there do not appear to be any non-privacy surveillance issues that would require a special surveillance impact assessment in this case.

The privacy impact assessment of the UK draft Communications Data Bill can be criticised for its inadequacies. It wasn't very thorough, it didn't engage stakeholders, there is no evidence that it has been subject to third-party review or audit. But more than that, as the monitoring, storage and retention of communications data raises many surveillance issues, one can argue that a PIA does not address adequately these various issues and that a surveillance impact assessment would be better in this case than a PIA. Retention of

communications data can be used for profiling and tracking the individual as well as those with whom the individual associates.

Smart metering is a form of surveillance. By monitoring smart meters, energy network operators can associate the data collected with particular customers or at least the households of their customers. Such monitoring can contribute to profiling practices that are more likely to be addressed by an SIA than a PIA.

Phorm received a lot of criticism some years ago for its plans to support targeted, personalised advertising based on deep packet inspection, i.e., tracking users as they went from one website to another in order to build profiles of consumers so that other service provides could better target their advertising according to the profiles. The European Commission in particular was critical of its targeted advertising without users' consent. The Phorm technology clearly supports dataveillance and profiling. A surveillance impact assessment would better address issues beyond privacy and data protection.

The US Department of Homeland Security's Automated Targeting System is a particularly wide-ranging and potentially intrusive smart surveillance system. As it includes non-US citizens, there are political dimensions that could be caught by an SIA, but not likely by a PIA.

The European Union Agency for Fundamental Rights (FRA) produced a document "The use of body scanners: 10 questions and answers", which is not a PIA but performs somewhat similar functions. The key question here is whether a PIA is adequate to address the range of issues raised by body scanners. As body scanners raise issues relating to fundamental rights, it is clear that a PIA would not be adequate, that an SIA would be more appropriate.

In sum, the consortium concludes that a PIA especially tailored for surveillance systems and technologies or, if you will, a surveillance impact assessment methodology is warranted to adequately address all of the issues raised by surveillance systems. Hence, the consortium will turn its attention to the development of such an SIA guidance document in its D3.2 deliverable.

ANNEX: SURVEILLANCE-ORIENTED PIA REPORTS

This annex presents an analysis of PIA reports in Australia, Canada, the UK and US. Each of these summarised PIA reports deal with surveillance technologies or systems. The SAPIENT partners analysed these PIA reports to see what lessons could be learned and, in particular, to see if there were some points that could be derived from these PIA reports which could be relevant for the development of a surveillance impact assessment methodology.

A. AUSTRALIA'S TELECOMMUNICATIONS INTERCEPTION AND ACCESS ACT (TIA)

Official name of the document

Privacy Impact Assessment: Preliminary Report: Telecommunications (Interception and Access) Act 1979 [TIA] Reform.

Name of the agency responsible for the PIA

Information Integrity Solutions Pty Ltd (IIS) commissioned by the Attorney-General's Office (Australia) (AGD)

Date of release and *(if relevant)* frequency of updates/other releases

PIA initially submitted in December 2011.
PIA made publicly available first in August 2012 following a freedom of information request.
Follow-up reports are not publicly available, nor is it stated when the final PIA will be submitted.
The current PIA contains statements possibly indicating continuing reporting as the TIA reform process progresses (see point 7, below).

Main steps in the PIA process

The whole process (of which the current document is just one part) is split into seven steps [p.14]:

1. A threshold analysis of the TIA reform proposals by the AGD confirms that a PIA is necessary (this is not explicitly stated in the PIA document).
2. IIS consulted with AGD and finalised a work plan. IIS discussed the project approach and finalised a work delivery plan.
3. IIS gathered information about the reform project. They particularly considered the AGD's drafting instructions for the proposed amendments and discussions with stakeholders. Other relevant research was also considered.[167]
4. IIS analysed the current situation and the proposals for reform (in particular, the intended data flows) with the aim of identifying possible privacy (and 'other more general risks and community concerns that tend to arise in the context of the use of intrusive powers') risks and benefits. Privacy risk identification takes particular account of the Information Privacy Principles laid out in the Privacy Act 1988.[168]
5. IIS prepared a draft preliminary report and provided this to the AGD for consideration.

[167] The sources of other research are listed in Appendix 2, pp. 60-61.
[168] Australian Government, "Privacy Act 1988," No. 119. http://www.comlaw.gov.au/Details/C2012C00903.

6. IIS finalised the report following comment and feedback (one presumes this is the report referred to as finalised).
7. Ongoing input and review of proposals for further amendments to the TIA as they are developed (this is stated in the purpose and scope of the PIA [pg.13]). This could imply follow-up work to the PIA as the reform process moved ahead, although this is not made explicit.

Legal or administrative basis for the PIA

- The PIA states explicitly that it is "not intended to be and should not be regarded as constituting legal advice". The PIA is intended as general policy advice [p.13].
- Legal qualification of the PIA: Government agencies and government agency projects in Australia fall under the Privacy Act 1988.[169] The Act does not require the execution of PIAs, but they have been strongly encouraged by the Attorney-General as a tool for ensuring privacy compliance.[170]

Name and short description of the smart surveillance technology at stake

The current TIA provides a regime basically making it an offence to intercept communication passing over a telecommunications system, but also provides a framework under which interceptions can be legitimate in limited circumstances, under certain conditions and by a limited number of actors.

The reform of the TIA follows a perceived change in technology and society which challenges the effectiveness of the current regime, originally constructed in 1979, and the consideration that the current TIA has structural and drafting issues which make its application difficult.

Certain aspects of the reform proposals would mandate broad retention of communications data with a weakened oversight regime and greater leeway for information sharing between government agencies.

Names of the main stakeholders involved

For the PIA report: IIS and AGD

In preparing the PIA, IIS met with three further groups of stakeholders [pp.29-31].
1. State and Federal law enforcement agencies, including the State Police and the Australian Federal Police, and the Australian Security Intelligence Organisation.
2. Telecommunication organisations and service providers.
3. Senior members of the Administrative Appeals Tribunal.

Main elements of the PIA

The report roughly follows the template laid out by the Australian Office of the Privacy Commissioner in 2006.[171]

[169] Ibid.
[170] Clarke, Roger, "PIAs in Australia: A work-in-progress report", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, p. 123.
[171] Office of the Privacy Commissioner, "Privacy Impact Assessment Guide", 2006.

In synthesis, the report is divided into five main parts. The first part offers an overview of the PIA process and of the PIA itself (scope, methodology, etc.). The second part elaborates the TIA, giving an overview of the Act itself (particularly its oversight and accountability mechanisms) and elaborating the background to, and drivers of, the proposed reforms (including changing communications technology and usage, changing patterns of criminal behaviour and the problems in the drafting and structure of the TIA itself). The third part describes the process and result of the stakeholder consultation. Finally, the fifth part consists of the outcome of the recommendations which form the core of the report. There are seven categories of recommendation. These categories cover a broad area, including recommendations relating to the legal aspects (structure, formulation and accountability and transparency mechanisms), to the on-going practical implementation of the proposals (training of staff and on-going monitoring) and to potential obligations on industry.

Main criteria used for the privacy impact assessment

In terms of legal criteria, the PIA takes particular account of the Information Privacy Principles laid out in the Privacy Act 1988 [p.14].

The PIA goes further, however, and draws on a broader framework aimed at "making decisions about the use of intrusive powers". This is the 4As framework (Authority, Analysis, Accountability, Appraisal) laid out by the Office of the Australian Information Commissioner [p. 15].[172]

Only the preliminary PIA is available.

The document is available online directly from the Australian Government (Attorney-General's Department), in the freedom of information section.
http://www.ag.gov.au/RightsAndProtections/FOI/Pages/Freedomofinformationdisclosurelog/PrivacyImpactAssessmentPreliminaryReportTelecommunications%28InterceptionandAccess%29ACT1979Reform.aspx The document is directly accessible at:
http://www.ag.gov.au/RightsAndProtections/FOI/Documents/Privacy%20Impact%20Assessment%20Preliminary%20Report%20Telecommunications%20%28Interception%20and%20Access%29%20ACT%201979%20Reform.pdf

Further uses of the PIA

The final version of the PIA is not publicly available.
The legislator does not seem to have made any facility to directly comment upon, or influence the final PIA or how it is used. However, it is explicitly pointed out that, '[t]his privacy assessment comes at an early stage in the review of the TIA Act, prior to any wider public consultation' [p. 13]. The PIA does not have binding status, nor does it constitute legal advice. However, it is not impossible that it could be used as evidence in proceedings before Court.

http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CEUQFjAB&url=http%3A%2F%2Fwww.privacy.gov.au%2Fmaterials%2Ftypes%2Fdownload%2F9349%2F6590&ei=PCIdUaajMYbHtAaj5IGICw&usg=AFQjCNHt7yQF4GHXQZIDaWJJ3pwAbJQs4A&bvm=bv.42452523,d.Yms

[172] Office of the Australian Information Commissioner, "Privacy fact sheet 3: 4A framework – A tool for assessing and implementing new law enforcement and national security powers," 2011. http://www.oaic.gov.au/publications/privacy_fact_sheets/Privacy-fact-sheet3_4Aframework.pdf

General remarks

This is a relatively lengthy document (at 61 pages) and contains broad reaching recommendations. However, when compared with the PIA "gold standard", it falls somewhat short.[173]

1. It has been conducted very early in the project lifecycle (and its continuation is not clear from the text) – meaning it has more in common with a Privacy Issue Analysis. PIAs are "performed in depth and extend through the life-cycle of a project".[174]
2. It has been conducted without multi-stakeholder dialogue and indeed was initially not even made public – meaning it has more in common with an Internal Risk Assessment. Consultation has been described as a feature central to Australian PIAs, "[t]he objectives of a PIA cannot be achieved if the process is undertaken behind closed doors"[175]. Equally, PIAs "should adopt a multi-stakeholder perspective, taking into account the risks as perceived by all stakeholders".[176]

[173] Clarke, Roger, "PIAs in Australia: A work-in-progress report", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, p. 124.
[174] Ibid.
[175] Clarke, Roger, "Privacy Impact Assessment Guidelines," Xamax Consultancy Pty Ltd, February 1998. http://www.xamax.com.au/DV/PIA.html
[176] Clarke, op. cit., 2012, p. 124.

B. CANADIAN AUTOMATIC LICENCE PLATE RECOGNITION SYSTEM

Official name of the document

Privacy Impact Assessment Automatic License Plate Recognition (ALPR)

Name of the agency responsible for the PIA

According to the PIA report, the Royal Canadian Mounted Police (RCMP) is the agency responsible for the PIA. HRH Howe Consulting Services, a consulting firm, assisted the agency (PIA, p. 16). However, interviews held by Canadian privacy activists have revealed that most of the job was done by the consulting firm and that RCMP agents were merely aware of the content of the PIA.[177]

Date of release and *(if relevant)* frequency of updates/other releases

The consultancy firm issued an initial draft of the PIA on 20 December 2007. It remains unclear whether the publicly available version is indeed the final version since it is labelled "Final Revision". In any event, senior RCMP official Supt Norm Gaumont approved it on 17 October 2009. On his website, Canadian privacy activist Rob Wipond indicated that as of January 2012 a new PIA was being drafted.[178]

Main steps of the PIA process

The main steps to be taken in the course of a PIA are to be found in the TBS PIA Guidelines, which are composed of four steps. The first step ("project initiation") is about determining whether a PIA is needed (the list of questions provided resembles those used in a privacy threshold assessment in Australia for instance) and, if so, what is the scope of such PIA, what are the resource requirements (legal expertise, technical expertise, etc.). The second step (data flow analysis) aims at describing the data flows that would take place. This is done through a diagram (called business process diagram), and data flow tables that document each data flow in greater detail. The third step ("privacy analysis") examines the data flows in the context of applicable privacy policies and legislation through a questionnaire with a checklist. The publication of a privacy impact analysis or assessment report is the fourth step. In addition to the information it should contain,[179] the report should feature a description of the specific privacy risks that have been identified, and of the strategies to mitigate them (if any).

Legal or administrative basis for the PIA

- Legality of the PIA: the PIA was conducted in 2009, and follows thus the federal[180] 2002 Privacy Impact Assessment Policy,[181] as well as the 2002 PIA guidelines.[182] In 2010, the

[177] http://www.focusonline.ca/?q=node/312

[178] http://robwipond.com/. During the course of an e-mail exchange, he outlined that so far the PIA hasn't been completed and that, as such, it is precluded from publication and from access to information request, cf. E-mail correspondence with the author, 7 February 2013.

[179] Just as for any PIA report, see sec. 6.3 of the Guidelines for more information.

[180] The RCMP has completed the PIA, since the further use of ALPR by provincial police forces always depends upon the federal RCMP database. The PIA must comply with Canadian federal law.

[181] Treasury Board of Canada Secretariat, "Privacy Impact Assessment Policy", Ottawa, 2002. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450&section=text; see also, the data matching components of the 1993 Privacy and Data Protection Policy, http://www.tbs- sct.gc.ca/pol/doc-eng.aspx?id=12450&section=text

Directive on Privacy Impact Assessment replaced previous PIA related policy,[183] including the Guidelines.[184]

- Legal qualification of the PIA: PIAs are formally referred to in the TBS policy (Privacy Impact Assessment Policy).

Name and short description of the smart surveillance technology at stake

ALPR is a governmental programme run jointly by the RCMP and any provincial law enforcement agency willing to benefit from the system. ALPR technology is used for law enforcement purposes. Through their on-board cameras, provincial police department cars scan licence plates (as well as time and location) and compare them against a database of plate numbers that are of interest (the latter is run by the RCMP). Once the scanned licence plate is matched against the database, it will result in a "hit" or a "non-hit". When it started as a project pilot in 2006, the ALPR was used in matters of stolen vehicles.[185] By 2010, its scope was extended to road safety purposes – prohibited, unlicensed or uninsured driving (p. 11). ALPR equipped patrol cars have two forward-facing cameras and a third, sideways camera. Though they scan every vehicle within range, the system is not run continuously, but rather, during organised traffic safety projects (pp. 12-13). When a plate matches a plate number in the database, the computer notifies the officer of the hit. To investigate a hit, the officer needs to manually query the plate number in one of the three databases (ICBC, PRIME or CPIC). Whether the police officer proceeds to a traffic stop (and eventually further investigation) is left to her discretion. Different data flows are involved. First, the daily updated RCMP database must be transferred into the law enforcement agency's mobile workstation. Second, at the end of a shift, the record of the mobile station is transferred back into the RCMP database (containing images of every scanned plate, location, time and the "hit" or "non-hit" results). "Non-hit" results are deleted from the RCMP database within 30 minutes after upload, though location and time data are kept as well as a handwritten copy retained indefinitely (p. 14).

Names of the main stakeholders involved

The PIA process provides for stakeholders' participation. It is evidenced by question 1.11 of the privacy analysis questionnaire that asks whether they have been consulted, and by question 1.12 that asks whether public consultation has taken place re the privacy risks and the ensuing mitigation solutions. Furthermore, the Guidelines clearly indicate that the PIA report should contain a list of all stakeholders and their roles and responsibilities (sec. 6.3, point 3). Finally, the Guidelines clearly mention that a PIA should serve as the basis for a consultation with stakeholders (sec. 1). Yet, nowhere in the PIA report are stakeholders mentioned. Questions 1.11 and 1.12 are simply absent from the privacy analysis (indicating that no such consultation has been undertaken). The report contains no list of stakeholders, nor are they mentioned in the communication plan. We can thus infer that no stakeholders were consulted.

---

[182] Treasury Board of Canada Secretariat, Privacy Impact Assessment Guidelines: A framework to Manage Privacy Risks, Ottawa, 31 August 2002. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp.

[183] Treasury Board of Canada Secretariat, Directive on Privacy Impact Assessment, Ottawa, 1 Apr 2010. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text

[184] http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12451&section=replacedby

[185] Denham, Elizabeth, Information and Privacy Commissioner [of British Columbia], Investigation Report F12-04, "Use of automated Licence plate recognition technology by the Victoria Police Department", 15 Nov 2012, p. 11. http://www.oipc.bc.ca/report/investigation-reports.aspx

Main elements of the PIA

The PIA report is composed of no less than 18 sections that follow very closely Annex A of the Guidelines that indicate what should be contained in a PIA report.[186] The first 17 sections (until section 17.1) describe the project (including objectives, project definition, requirements, etc.), and roughly correspond to steps 1 and 2 of the PIA process; section 17.2 contains the questionnaire for purposes of privacy analysis; and section 18 contains the privacy management plan (cf. section 4 of the PIA: evidence risks and mitigation strategies).

Availability of the PIA report

The Guidelines mention that department and agencies should provide a copy of the final PIA report to the Privacy Commissioner as well as prepare an executive summary for public use (sec. 6.3). However, we were not able to find such a summary on the RCMP's website.[187] However, we were able to download a copy of the full PIA from the website of Canadian privacy activist Rob Wipond.[188]

Further uses of the PIA

The Guidelines view a PIA report as an effective communication tool that is at the stakeholders' disposal for further use (section 4, step 4). We have evidenced such use through the work of Canadian privacy activist Rob Wipond. To our knowledge, the PIA has not been used in legal proceedings.

General remarks

ALPR is a smart technology because it relies upon the indiscriminate collection of information, i.e., the system photographs and scans every vehicle and licence plate that comes within range of its cameras. It therefore collects the information of innocent civilians (according to Wipond, 95% of the scanned licence plates are "non-hit" targets). Furthermore, information that is non-necessary for the purposes of the system is also collected (e.g., time and location), and stored (non-hit is stored indefinitely on paper, and claims have been made that it is digitally stored up to a year). The latter is function creep and the question is whether the goal of "fight against car thieves" is not just an excuse to put in place an extended surveillance system of Canadian citizens. This is confirmed by the privacy analysis that discusses the processing of sensitive data (how does it fit with the ambition to solely scan licence plates?). [189]

There exist serious doubts as to the will of the RCMP to make genuine efforts towards a more privacy compliant system. The RCMP has made pledges to take due account of the criticisms contained in the British Columbia Privacy Commissioner's report (cf. *supra*, in particular, in the upcoming PIA). Yet, whilst pledging to abide by such criticisms, the RCMP was simultaneously contesting the legitimacy of the report (a report from the federal Privacy Commissioner would also prove necessary). Furthermore, it is reported that as early as 2010,

[186] And in doing so, is consistent with section 6.3 of the Guidelines.
[187] The RCMP's website contains a page dedicated to PIAs summaries, but the one on ALPR could not be found. http://www.tpsgc-pwgsc.gc.ca/aiprp-atip/efvp-pia/efvp-pia-eng.html
[188] http://robwipond.com/. The PIA can be downloaded at the following address: http://robwipond.com/ref/RCMP%20ALPR%20PIA.pdf
[189] http://www.focusonline.ca/?q=node/312

the RCMP has shown the same ambivalent attitude towards criticisms addressed at the ALPR system (i.e., pledging to take them into consideration, but retreating at the last minute).[190]

In the light of the previous remark, the fact that the PIA was mainly conducted by a consultancy firm with very little involvement by the RCMP makes it appear as a self-legitimation exercise.[191] It also appears that the PIA provides a very lenient description of the data processing operations that are actually taking place. In this sense, the PIA is totally excluded from the project, whereas, as a process, it should be embedded in it.[192]

In the risks mitigation section of the PIA, the only privacy risk the RCMP seems to acknowledge is linked to the trans-jurisdictional nature of the system, and the ensuing questions concerning what law enforcement agency has control over the information processed. However, it never acknowledges issues related to the proportionality of the system, or to the possibilities of "function creep" – what the EU legal tradition regards as compliance with the purpose specification principle (p. 73).

[190] http://www.christopher-parsons.com/blog/privacy/another-step-closer-to-reining-in-alpr-in-bc/
[191] http://www.focusonline.ca/?q=node/312; Investigation Report F12-04, "Use of automated licence plate recognition technology by the Victoria Police Department", 15 Nov 2012, p. 11. This is confirmed by the fact that the RCMP claims to have been given approval by the BC and federal Privacy Commissioners while in fact the latter merely received a copy of the PIA report.
[192] http://www.focusonline.ca/?q=node/312

C. THE UK DRAFT COMMUNICATIONS DATA BILL

Official name of the document

Privacy Impact Assessment of the Draft Communications Data Bill

Name of the agency responsible for the PIA

UK Home Office

Date of release

14 June 2012

Main steps in the PIA process

The PIA report has seven chapters, including an executive summary, the case for legislation, PIA approach, overview of current and planned safeguards, privacy risks, a PIA statement, relevant legislation. It also has four annexes, including a glossary, types of communications data, relevant legislation, PET assessment.

Legal or administrative basis for the PIA

The PIA report refers to the PIA Handbook published by the UK Information Commissioner's Office in December 2007 (revised in June 2009). The Cabinet Office, in its Data Handling Review, called for all central government departments to "introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start". It accepted the value of PIA reports and stressed that they will be used and monitored in all departments as a means of protecting personal data and tackling identity management challenges from July 2008 onwards. PIAs have thus become a "mandatory minimum measure".

Name and short description of the smart surveillance technology at stake

This PIA concerns the retention of communications data by communications service providers (in the wake of the EU Data Retention Directive). The PIA refers to the difficulties encountered by the police and other authorities as communications has moved to the Internet.

Names of the main stakeholders involved

The report mentions that the Interception of Communications Commissioner will have oversight of auditing and inspections, and individuals will have "a proper avenue [to the Independent Investigatory Powers Tribunal] of complaint and independent investigation if they think the powers have been used unlawfully". The report also mentions communications service providers (CSPs). However, it does not discuss consultation with other stakeholders (e.g., civil society organisations, academia).

Main elements of the PIA

This PIA says it followed the approach and guidelines recommended by the Information Commissioner's Office (ICO). However, from the report, it is not obvious that they did so (e.g., there is no mention of having consulted stakeholders). Essentially, the PIA report says it will be updated and published to take account of the strategy of phased delivery of new capabilities. The PIA identifies risks to both individuals and the organisation. The PIA identifies existing and new safeguards. It identifies legislation which it has theoretically taken into account.

Main criteria used for the privacy impact assessment

Identifying risks and safeguards.

Availability of the PIA report

The report is publicly available at: http://www.homeoffice.gov.uk/publications/counter-terrorism/comms-data-bill/communications-data-privacy-ia?view=Binary.

Further uses of the PIA

Stakeholders can certainly comment on the PIA, although it's not apparent that their comments will be taken into consideration.

General remarks

There are many lacunae in this PIA report, e.g., it is not apparent that the PIA was undertaken when it was possible to influence the draft legislation. It's not apparent that the Home Office developed a plan for the PIA or its terms of reference. It is not apparent that there was a consultation strategy appropriate to the scale, scope and nature of the project. It is not apparent that any determination was made regarding whether a full-scale or small-scale PIA was needed. The PIA makes no reference to seeking out and engaging stakeholders. It is not apparent that the Home Office put in place measures to achieve clear communications between senior management, the project team and representatives of, and advocates for, the various stakeholders. It is not apparent that the Home Office sought to assess the project's privacy risks from the perspective of all stakeholders. It is not evident that the Home Office has made any effort to circulate the PIA to a diversity of stakeholders. There is no provision regarding any intention to submit the PIA report for an audit.

D. USE OF SMART METERING DATA BY NETWORK OPERATORS

Official name of the document

Privacy Impact Assessment: Use of Smart Metering data by Network Operators

Name of the agency responsible for the PIA

Energy Networks Association

Date of release

October 2011

Main steps of the PIA process

In undertaking this PIA process, Engage Consulting (who prepared the report for the Energy Networks Association) considered the benefits that network operators could deliver using data from smart meters; identified what data is required to deliver these, now and in the future; consulted stakeholders, distilled the privacy risks and issues; and identified how network operators might mitigate privacy concerns. It appears that all stakeholder views were captured, which were then analysed and grouped by area of concern. These are summarised in sections 9 and 10 of the report. The detailed feedback and concerns from stakeholders are included in an appendix. These concerns have then been further considered and recommendations made for addressing them.

Legal or administrative basis for the PIA

There is generally no obligation for the private sector to carry out PIAs. The PIA was carried out and made public in order to demonstrate to stakeholders that the ENA and its members are taking the issue of privacy seriously. This is one of only two UK industry-prepared, publicly available PIAs discovered by the SAPIENT consortium.

Name and short description of the smart surveillance technology at stake

Smart meters (and the associated smart grids) which enable frequent (every half hour – if not more frequently) monitoring of energy consumption data from homes and offices.

Names of the main stakeholders involved

Engage consulted with various stakeholders, including

- the Information Commissioner's Office;
- Department of Energy and Climate Change;
- consumer organisations and privacy groups (who represent consumers);
- energy suppliers;
- the Energy Retail Association;
- network operators;

- ELEXON[193]; and
- research companies and consultancies.

Main elements of the PIA

A concern is that through the processing of detailed energy consumption data, organisations may be able to deduce detailed information relating to an individual or household's behavioural habits, daily routines and lifestyle.

Main criteria used for the privacy impact assessment

Engage examined the different types of data that would be generated by the smart meters and the potential privacy risks posed by the different types of data and how those risks could be minimised. As mentioned above, it consulted widely with different types of stakeholders. The main criteria used in the PIA relate to the stakeholder concerns, which included access to data, security of data, communications (with customers), privacy, customer consent, and "other" (i.e., disclosure of customer data to the police). For the various concerns, Engage included stakeholder suggested actions for addressing their concerns.

Availability of the PIA report

The report is available on the Energy Networks Association website:
http://www.energynetworks.org/modx/assets/files/news/consultation-responses/Consultation%20responses%202011/ENA%20Privacy%20Impact%20Assessment%20Use%20of%20Privacy%20Impact%20Assessment%20Use%20of%20Smart%20Metering%20data%20by%20Network%20Operators_Oct%202011.pdf

Further uses of the PIA

The PIA is being used as the basis for development of a "Privacy Charter" and a privacy guide.

General remarks

Relatively speaking, this is quite a good PIA. It addresses most of the key points mentioned in the ICO PIA Handbook.

[193] ELEXON plays a role in balancing and settling arrangements in the wholesale electricity market. It administers the Balancing and Settlement Code (BSC). It compares how much electricity generators and suppliers said they would produce or consume with how much electricity they actually generated and supplied. After calculating these volumes, ELEXON work out a price for the imbalances and charge organisations accordingly. It takes 1.2 million meter readings every day and handles more than £1.5 billion of customers' funds each year. http://www.elexon.co.uk/about/what-we-do/

E. PHORM AND THE ANALYSIS ON USERS' INTERNET TRAFFIC

Official name of the document

Privacy Impact Assessment for Phorm

Name of the agency responsible for the PIA

80/20 Thinking Ltd. commissioned by Phorm Inc.

Date of release and (if relevant) frequency of updates/other releases

Interim PIA completed in February 2008
Final PIA released October 2008
Ongoing work is mentioned, but evidence of this is lacking.

Main steps of the PIA process

80/20 Thinking states that, as the PIA is being carried out late in the development stage of the technology, they have "developed a 'late stage implementation' PIA model that aims to satisfy most of the key criteria of a 'full product cycle' PIA" [p.1]. What this late stage model precisely entails is not made clear, nor is it made clear what, how or which main criteria of a "full product cycle" PIA are fulfilled.

The PIA states that the work will consist of four parts:
- Scoping the technology and engineering elements to assess privacy functionality,
- Assessment of due diligence and compliance aspects,
- Conducting a full risk assessment of presentational and other elements of the product launch and deployment,
- Auditing the privacy policies.

A further set of elements of ongoing work are also laid out.
- Working collaboratively with Phorm to develop a sustainable privacy framework within the organisation,
- Conducting privacy training for Phorm staff,
- Creating a rapid response privacy reporting and response regime.

Legal or administrative basis for the PIA

The PIA is not a legal document.

The Phorm PIA is one of the first to have been done in the UK following the release of the Information Commissioner's Office PIA "launch campaign". This does not constitute a legal requirement. Indeed, the Phorm PIA presents PIAs generally as an exercise in risk assessment for businesses and accordingly as an exercise bringing economic benefit rather than as a way to safeguard privacy.

Name and short description of the smart surveillance technology at stake

Phorm's technology functions with Internet service providers. The technology performs an analysis of users' Internet traffic, with the intention of providing personalised advertising. This analysis involves an interception of all the Web pages users visited and a scanning of their content for keywords (including search terms). The analysis of the frequency of keywords is used to build profiles of users. These profiles are then used for targeted advertising on websites which have signed up with Phorm.

Names of the main stakeholders involved

For the PIA report: Phorm and 80/20 Thinking.

For the PIA process: It seems that no other stakeholders were involved in the PIA process. This might have been because the PIA was conducted late in the technology development cycle. The stakeholder consultation performed by Phorm prior to the PIA was evaluated very positively. The PIA document states that Phorm engaged with a wide range of stakeholders including parliamentarians, privacy advocates and the general public. The PIA comments on Phorm's holding a public meeting and the fact that it allowed a computer security specialist (who was also a critic of the technology) to conduct a deep inspection of the technology.

Main elements of the PIA

The report is divided into four main parts. The first part is an extended executive summary, including an overview of developments between the release of the interim PIA and the final document, an overview of some of the core issues and a set of recommendations. The second part elaborates the role and function of a PIA and certain elements of the PIA process. This is done on a very general level, not necessarily with reference to the Phorm PIA itself. The third part considers the stakeholder consultations conducted by Phorm prior to the PIA process. Finally, the fourth part consists of the privacy risk analysis.

Main criteria used for the privacy impact assessment

Once again, the specific criteria for assessment are not explicit, although it is clear that the Phorm system was evaluated for compliance with the UK Data Protection Act and was regarded as not collecting "personal data" within the meaning of the Act. Elsewhere in the document, a set of lengthy operational aims for PIAs generally are laid out [p. 11]. It is not clear how precisely these were followed in this case.

Availability of the PIA report

The interim PIA is available at:
http://blogs.guardian.co.uk/technology/Phorm%20PIA%20interim%20final%20.pdf.
The final PIA is not publicly available. It appears to have been removed from Phorm's website.

Further uses of the PIA

The PIA is not a legal document and does not lay down any legal obligations.

The final PIA is not publicly available and is not available for comment.

The PIA states that a PIA means that a company (Phorm) cannot "claim ignorance about the impact of its proposals" [p. 10].

General remarks

It is hard to evaluate this PIA. The authors themselves state that it was done only in the very late stages of the technology development process which made it hard to implement all features of a PIA. However, there are certain negative points that should be mentioned: It lacks information on its methodology and a description as to how it came to its eventual findings. Its findings often seem overly positive and apologetic to Phorm. Indeed, it seems rather biased. As mentioned above, this is only an interim report; we do not have access to the final report.

F. THE US DHS AUTOMATED TARGETING SYSTEM

Official name of the document

Privacy Impact Assessment for the Automated Targeting System DHS/CBP/PIA-006(b). Hereinafter: 2012 ATS PIA.

Name of the agency responsible for the PIA

Department of Homeland Security. The "responsible officials" are the CBP (Customs and Border Protection) Privacy Officer and the Executive Director, Targeting Division of the Office of Intelligence and Investigative Liaison of the US Customs and Border Protection [p. 34]. The "reviewing official" is the Chief Privacy Officer of the Department of Homeland Security (who provides the "approval signature") [p. 34].

Date of release and frequency of updates/other releases

The latest ATS PIA was released 1 June 2012. The 2012 ATS PIA is the fourth privacy impact assessment completed and released on the Automated Targeting System. The previous three PIAs were released in November 2006, August 2007 and December 2008. The 2006, 2007 and 2012 ATS PIAs have been published in conjunction with a new release of the relevant System of Records Notice (SORN) and the relative changes in the scope and functioning of the Automated Targeting System.

Main steps in the PIA process

1st step: decision re the need to conduct a PIA, based on the criteria set by statute and by internal guidance. From a practical perspective, the process starts with a privacy threshold analysis (PTA) and the completion of a PTA template.[194] The PTA for the ATS is not publicly available.

2nd step: according to the DHS guidelines, "if a PIA is required, the Department program manager works closely with the component privacy officer to complete the PIA, utilizing the guidance document listed below. Once completed, the PIA is sent to our office for review and approval by the Department's Chief Privacy Officer".[195]

3rd step: publication of the PIA report (unless this is not "practicable" according to the wording of section 208(b)(1)(B)(iii) of the E-Government Act of 2002). In the case of the 2012 ATS PIA, the PIA report is available online.

Legal or administrative basis for the PIA

The legal basis of the 2012 ATS PIA is to be found in the E-Government Act of 2002 (section 208(b)), the Homeland Security Act 2002 as amended (Section 222), and the Congress requirement (as mentioned in the 2008 DHS Policy Regarding Privacy Impact Assessment.[196]

[194] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pta_template.pdf
[195] http://www.dhs.gov/privacy-compliance#2
[196] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf

The 2012 ATS PIA report is legally a privacy impact assessment as defined by the statutes and authority mentioned above.

Name and short description of the smart surveillance technology at stake

The Automated Targeting System (ATS) is a US government system operated by the Customs and Border Protection (CBP) of the Department of Homeland Security. It is formally defined as a "decision support tool [that] compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments" [p. 2]. The system offers three main "functionalities" to users: (i) a comparison between information on US-bound travellers or cargo and information already stored in pre-defined databases ("Comparison"); (ii) a comparison between information on travellers and cargo and "patterns identified as requiring additional scrutiny" ("Rules"); the possibility to "search data across many different databases and systems to provide a consolidated view of data responsive to a query about a person or entity" ("Federated Query") [p. 2]. Not all of the data to be searched and compared are "fully" stored in the ATS. The system only maintains a limited number of "official record(s)", and it mostly relies on other several source systems [p. 3]. Of these "external" sources, either the ATS stores "copies of key elements of certain databases" (the "ingestion of data") to reduce the impact of ATS searches on the source databases or it directly "accesses and uses" the databases without previously ingesting their data ("pointer system") [p. 3]. Finally, users can also use the ATS to "manually process certain datasets" [p. 4]. The areas covered by the ATS range from cargo movements to travellers' border crossings. The division of the system in "modules" or "sub-systems" partially mirrors these areas of competence (e.g., the Automated Targeting System-N focuses on cargo, while the Automated Targeting System-Passenger focuses on travellers) [pp. 4-8]. A special module, the ATS-Targeting Framework, allows a restricted group of users to "search across the data sources available in other modules of ATS based on role-based access for research and analysis purposes" [p. 7].

Names of the main stakeholders involved in the PIA process and in the PIA report

For the PIA report: Office of Intelligence and Investigative Liaison of the US Customs and Border Protection (CBP), the CBP Privacy Officer, the DHS Chief Privacy Officer.

For the PIA process: It appears that no "external" stakeholders (e.g., citizens, passengers, private companies providing data, etc.) were involved in the PIA process. However, after the release of the PIA report, at least one external stakeholder (the Electronic Privacy Information Center) provided and published comments.[197]

Main elements of the PIA

The report strictly follows the template put at disposal of the DHS[198] and defined by the DHS Chief Privacy Officer in the 2010 Privacy Office Official Guidance.[199] The report is divided into three main parts. The first offers an overview of the system, introducing its main goal, its core functionalities, its different sources of data and its general architecture. The second part is the core of the PIA report: eight sections, structured as questionnaires with standard questions, touch upon different issues such as the legal base of the system or the level of

[197] https://epic.org/privacy/travel/ats/EPIC-ATS-Comments-2012.pdf
[198] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_template.pdf
[199] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf

security in the storage of information. Most of these sections have a dedicated question introduced as "Privacy Impact Analysis" (e.g., p. 17) in which specific privacy risks are highlighted and forms of mitigation are presented. The third element of the report is constituted by a series of four appendixes.

Availability of the PIA report

The 2012 ATS PIA is freely available online.[200] The previous versions of the PIAs of the same system, and of other US Customs and Border Protection systems, are available in a dedicated webpage of the DHS website.[201] On the same page are also available electronic copies of the relevant Final Rules and Systems of Records Notices (SORN). In the case of the 2012 ATS PIA, the online copy is not redacted.

Further uses of the PIA

According to the 2008 DHS Policy Regarding Privacy Impact Assessment, PIAs are meant to ensure transparency to both the public and "external oversight bodies, including the Congress and the Government Accountability Office" (p. 2). According to the same document, PIAs also ensure accountability and contribute to the determination of the DHS Federal Information Security Management Act (FISMA) score.

General remarks

The Automated Targeting System is a particularly wide-ranging and potentially intrusive smart surveillance system, with direct consequences on non-US citizens (e.g., PNR data are stored in one of its modules, and processed by at least two different modules). Furthermore, it relies not only on government-collected information, but also on commercial data sources.

Despite such far-reaching features, the privacy impact assessment process is practically dealt within the Department of Homeland Security. Even if external authorities can use the document to assess the transparency and accountability of the Department, and even if concerned people and institutions can release comments on the report, they do not directly participate in the PIA process.

According to the wording of the 2010 Privacy Office Official Guidance, “the PIA is a living document that needs to be updated regularly as the program and system are changed and updated, not just when the program or system is deployed” (p. 2). The fact that the 2012 ATS PIA is the fourth PIA report published confirms this statement, and the comparative analysis of the ATS PIAs permits a better understanding of the main evolutions and changes of the program. However, given that public comments to the ATS are published and addressed in a System of Record Notice,[202] it is difficult to clearly understand how much these comments are taken into account in the privacy impact assessment process.

In the “questionnaire” sections of the PIA report, most of the remedies and solutions to mitigate privacy threats rely on the security of the technological architecture, the differential and controlled access to the different modules and functions of the ATS, and the security of

[200] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf
[201] http://www.dhs.gov/privacy-documents-us-customs-and-border-protection
[202] e.g., the 2010 ATS SORN: http://www.gpo.gov/fdsys/pkg/FR-2010-02-03/html/2010-2201.htm

the premises. Practically no comments are advanced or proposed to restrain the reach and aim of the system, or to limit its possible consequences in terms of social effects.

G. BODY SCANNERS

Official name of the document:

The use of body scanners: 10 questions and answers (shorter version of the European Union Agency for Fundamental Rights' opinion in the consultation of the European Commission on "The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection").

Name of the agency responsible for the PIA:

European Union Agency for Fundamental Rights (FRA).

Date of release and (if relevant) frequency of updates/other releases:

Date of release of this document (The use of body scanners: 10 questions and answers): July 2010.
No follow-up releases.
Dates of consultation process: November 2008 – February 2009.

Main steps in the PIA process:

1st step: The European Parliament expressed concern about the lack of legitimacy of the European Commission's proposal to introduce body scanners in EU airports. The Parliament observed that 1. "conditions for taking a decision [had] not yet been met, given that essential information [was] still lacking", 2. "that [the] draft measure could exceed the implementing powers provided for in the basic instrument" and 3. "that that all aviation security measures, including use of body scanners, should respect the principle of proportionality as justified and necessary in a democratic society" and accordingly requested "the FRA, as a matter of urgency, to urgently deliver an opinion on body scanners".[203]
2nd step: The FRA produced and submitted an opinion on the fundamental rights impact of body scanners as a part of the broader public consultation initiated by the European Commission following the Parliament's Resolution.
3rd step: The production and publication of this abridged document on the FRA's website.

Legal or administrative basis for the PIA

- The PIA is not itself a legal document – FRA documents do not have legal force.
- Specific legal basis for the consultation of the Fundamental Rights Agency is provided in the European Parliament's Resolution on the Impact of Aviation Security Measures and Body Scanners on Human Rights, Privacy, Personal Dignity and Data Protection[204] (see main steps of the PIA process, above). The Commission's draft measure was mandated under Article 4(2)(a) of the Regulation On Common Rules in the Field of Civil Aviation and accordingly followed the regulatory procedure with scrutiny. This procedure permitted the European Parliament to object to the adoption of the Commission's proposed measure. It did this with conditions – the consultation of the FRA among them.

[203] European Parliament resolution on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+B6-2008-0562+0+DOC+XML+V0//EN
[204] Ibid.

Name and short description of the smart surveillance technology

The deployment of body scanners in EU airports involves action at both an EU and Member State level and qualifies as a government enterprise.

The assessment repeats the description of security scanner (also known as body scanner) technologies in the Commission Communication "The Use of Security Scanners at EU airports".[205] Body/security scanner is "the generic term used for a technology that is capable of detecting objects carried under clothes. Several forms of radiation differing in wavelength and energy emitted are used in order to identify any object distinct from the human skin. In aviation, Security Scanners could replace walk-through metal detectors (capable of detecting most knives or arms) as means of screening passengers because they are able to identify metallic and non-metallic objects including plastic and liquid explosives."

Names of the main stakeholders involved

For the PIA report: FRA

For the PIA process: FRA

No external stakeholders (e.g., concerned actors: citizens, passengers, private companies providing data, etc.) seem to have been involved in this process. However, the broader consultation of which the FRA opinion was a part included a much broader range of stakeholders.

Main elements of the PIA

This is a fundamental rights impact report and thus goes beyond only assessing privacy impacts. The report has been split into 10 key questions and answers. The question and answer format was designed to "make the paper...a self-standing document".

The report has been split into five parts. Part 1 (Introduction) offers a brief consideration of the technology. Part 2 (Chapters 1-4) considers the legal issues around body scanners, considering how body scanners affect the right to respect for private life, how their use interacts with the right to data protection (including how their use could best respect data protection principles) and how their use must be tightly regulated by law. Part 3 (Chapters 5-7) considers the specific questions associated with body scanner deployment (who should/shouldn't be screened, what level of choice should be offered to those who do not wish to be screened, which information should be given to those to be screened and when). Part 4 (Chapters 8 and 9) considers the proportionality of the use of body scanners in relation to their relative invasiveness (compared to other screening technologies) and their ability to achieve their stated aims in terms of the provision of more security. Finally, Part 5 (Chapter 10) offers a set of conditions to be taken into account to address fundamental rights and privacy concerns.

[205] European Commission Communication to the European Parliament and the Council of 15 June 2010 on the Use of Security Scanners at EU airports [COM(2010) 311 final.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0311:EN:NOT

Main criteria used for the privacy impact assessment

The main criteria are not made explicit.

The main legal criteria considered are the rights set out in the European Convention of Human Rights, the Charter of Fundamental Rights of the European Union and the International Covenant of Civil and Political Rights (particularly the right to respect for privacy – Articles 8, 7 and 17 respectively – and the right to data protection – Article 8 of the Charter).

Availability of the PIA report

This document is available freely online from the FRA website.[206]

The original consultation document is not available from the FRA or from the European Commission.

Further uses of the PIA

There are no official comments on the final version of the assessment.

It is not certain what role the assessment played in the ensuing policy process.
This assessment is not a binding document. However, as an opinion from the European Union agency devoted to fundamental rights, it has a certain authoritative status.

General remarks:

Although the logic in considering the privacy and data protection impact is reminiscent of a PIA, this document is a fundamental rights assessment within the context of a much broader consultation. Accordingly, it was never intended to function as a PIA in the strict sense. The range of issues raised by body scanners makes clear that a PIA would not adequately address all of the issues.

[206] http://fra.europa.eu/sites/default/files/fra_uploads/959-FRA_Opinions_Bodyscanners.pdf

REFERENCES

Article 29 Data Protection Working Party, "Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications", Working Paper 00327/11/EN, WP 180, Brussels, 2011.

Article 29 Data Protection Working Party, "Opinion 1/2012 on the data protection reform proposals", Working Paper 00530/12/EN, WP 191, Brussels, 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf

Bamberger, Kenneth A., and Deirdre K. Mulligan, "Privacy Decision making in Administrative Agencies", *University of Chicago Law Review*, Vol. 75, No. 1, 2008, pp. 75-107.

Bamberger, Kenneth A., and Mulligan Deirdre K., "PIA Requirements and Privacy Decision-making in US Government Agencies", in David Wright, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, Heidelberg, London, New York, 2012, pp. 225-250.

Bayley, Robin M., and Colin J. Bennett, "Privacy Impact Assessments in Canada", in David Wright, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, Heidelberg, London, New York, 2012, pp. 161-185.

Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge, Mass. and London, 2006.

Bennett, Colin J., "Appendix D: Jurisdictional Report for United States of America", in *Privacy Impact Assessments: International Study of their Application and Effects*, Information Commissioner's Office, Wilmslow, UK, 2007.

Cabinet Office, "Cross Government Actions: Mandatory Minimum Measures", London, 2008. http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf

Cabinet Office, "Data Handling Procedures in Government: Final Report", London, 2008. http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf

Clarke, Roger, "Privacy impact assessment: Its origins and development", *Computer Law & Security Review*, Vol. 25, No. 2, 2009, pp. 123-135.

Clarke, Roger, "An Evaluation of Privacy Impact Assessment Guidance Documents", *International Data Privacy Law*, Vol. 1, No. 2, 2011, pp. 111-120.

Clarke, Roger, "PIAs in Australia: A Work-in-Progress Report", in David Wright, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, Heidelberg, London, New York, 2012, pp. 119-148.

De Hert, Paul, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments", in David Wright, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, Heidelberg, London, New York, 2012, pp. 33-76.

Dempsey, James X., "Statement before the House Committee on the Judiciary Subcommittee on Commercial and Administrative Law", in The Privacy Officer for the Department of Homeland Security (ed.), *Privacy in the Hands of the Government*, London, 2004.

Department for Transport, "Impact Assessment on the Use of Security Scanners at UK Airports: Consultation", London, 2010. https://http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/2424/ia.pdf

Department of Communities and Local Government, "Making Better Use of Energy Performance Certificates and Data: Consultation", London, 2010. http://www.communities.gov.uk/documents/planningandbuilding/pdf/1491281.pdf

DHS (Department of Homeland Security), "Privacy Technology Implementation Guide", Washington, DC, 2007.

http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_ptig.pdf

DHS (Department of Homeland Security), "Privacy Impact Assessment Template", Washington, DC, 2010. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_template.pdf

Edwards, John, "Privacy Impact Assessment in New Zealand - A Practitioner's Perspective", in David Wright, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, Heidelberg, London, New York, 2012, pp. 187-204.

European Commission, "Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification", C (2009) 3200 final, Brussels, 2009. http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

European Commission, "A comprehensive approach on personal data protection in the European Union", COM(2010) 609 final, Brussels, 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF

European Commission, "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offencesor the execution of criminal penalties, and the free movement of such data", COM(2012) 10 final, Brussels, 2012.

European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", COM(2012) 11 final, Brussels, 2012.

Finn, Rachel L., David Wright, and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert, and Yves Poullet (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp. 3-32.

Flaherty, David, "Privacy Impact Assessments: An Essential Tool for Data Protection", *Privacy Law and Policy Reporter*, Vol. 7, No. 5, 2000. http://www.austlii.edu.au/au/journals/PLPR/2000/

GAO (Government Accountability Office), "Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain", Report to te Ranking Minority Member, Subcommittee on Oversight of Government Management, Committee on Homeland Security and Governmental Affairs, U.S. Senate GAO-05-866, Washington, DC, 2005. http://www.gao.gov/new.items/d05866.pdf

GAO (Government Accountability Office), and Linda D. Koontz, "Homeland Security: Continuing Attention to Privacy Concerns is Needed as Programs Are Developed", Testimony before the Subcommitee of Homeland Security, Committee on Appropriations, House of Representatives GAO-07-630T, Washington, DC, 2007. http://www.gao.gov/new.items/d05866.pdf

Gutwirth, Serge, Rocco Bellanova, Michael Friedewald, Dara Hallinan, David Wright, Paul McCarthy, Julien Jeandesboz, Emilio Mordini, Silvia Venier, Marc Langheinrich, and Vlad Coroama, "Smart Surveillance - State of the Art Report", Deliverable 1.1, SAPIENT Project, January 2012.

HIQA (Health Information and Quality Authority), "International Review of Privacy Impact Assessments", Mahon, Cork, Ireland, 2010. http://www.hiqa.ie/publications/international-review-privacy-impact-assessments

HIQA (Health Information and Quality Authority), "Guidance on Privacy Impact Assessment in Health and Social Care", Dublin, 2010.

http://www.hiqa.ie/system/files/HI_Privacy_Impact_Assessment.pdf
ICO (Information Commissioner's Office), "Privacy Impact Assessments: International Study of their Application and Effects", Wilmslow, Cheshire, UK, 2007. http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/privacy_impact_assessment_international_study.011007.pdf
ICO (Information Commissioner's Office), "Privacy impact assessment handbook", UK Information Commissioner's Office, London, 2007.
ICO (Information Commissioner's Office), "Privacy impact assessment handbook. Version 2.0", UK Information Commissioner's Office, London, 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html
Longworth, Elizabeth, "Notes on Privacy Impact Assessmentas", Longworth Associates, Christchurch, NZ, 1996.
Ministry of Justice, "Undertaking Privacy Impact Assessments: The Data Protection Act 1998", London, 2010. http://www.justice.gov.uk/downloads/information-access-rights/data-protection-act/pia-guidance-08-10.pdf
OCIPO (Office of the Chief Information and Privacy Officer), "Privacy Impact Assessment Guide for the Ontario Public Service", Queen's Printer for Ontario, Toronto, 2010.
OIPC (Office of the Information and Privacy Commissioner of Alberta), "Privacy Impact Assessment Requirements", Edmonton, 2009. http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf
OMB (Office of Management and Budget), "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002", Washington, DC, 2003. http://www.whitehouse.gov/omb/memoranda/m03-22.html
OPC (Office of the Privacy Commissioner of Canada), "Assessing the Privacy Impacts of Programs, Plans, and Policies", Audit Report of the Privacy Commissioner of Canada, Ottawa, 2007. http://www.privcom.gc.ca/information/pub/ar-vr/pia_200710_e.pdf
OPC (Office of the Privacy Commissioner), "Privacy Impact Assessment Guide", Sydney, 2010. http://www.privacy.gov.au.
OVPC (Office of the Victorian Privacy Commissioner), "Privacy Impact Assessments: A guide for the Victorian Public Sector (Edition 2)", Melbourne, 2009.
Privacy Commissioner's Office, "Privacy Impact Assessment Handbook", Wellington, New Zealand, 2007.
Privacy Commissioner's Office, "Guidance Note for Departments Seeking Legislative Provision for Information Matching, Appendix B", WELLINGTON, NEW ZEALAND, 2008. http://privacy.org.nz/guidance-note-for-departments-seeking-legislative-provision-for-information-matching/ - appendix
Privacy Commissioner's Office, "Operating programmes", Welington, New Zealand, last updated 30 June 2010. http://privacy.org.nz/operating-programmes/
Rotenberg, Marc, "The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11", Electronic Privacy Information Center, Washington, D.C., 2006. http://ssrn.com/abstract=933690
Stewart, Blair, "Privacy impact assessments", *Privacy Law and Policy Reporter*, Vol. 3, No. 4, 1996. http://www.austlii.edu.au/au/journals/PLPR/1996/39.html
Stewart, Blair, "PIAs – an early warning system", *Privacy Law and Policy Reporter*, Vol. 3, No. 7, 1996. http://www.austlii.edu.au/au/journals/PLPR/1996/65.html
Stewart, Blair, "Privacy Impact Assessment: Some Approaches, Issues and Examples", *Information technology management research*, Vol. 4, No. 3, 2002, pp. 23-38.
Tancock, David, Siani Pearson, and Andrew Charlesworth, "Analysis of Privacy Impact Assessments within Major Jurisdictions", in *Proceedings of the Eighth Annual*

International Conference on Privacy, Security and Trust, Ottawa, 17-19 August 2010, IEEE Press, 2010, pp. 118-125.

TBS (Treasury Board of Canada Secretariat), "Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks", Ottawa, 2002. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp

TBS (Treasury Board of Canada Secretariat), "Policy on Privacy Protection", 1 April 2008. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510&section=text.

TBS (Treasury Board of Canada Secretariat), "Directive on Privacy Impact Assessment", 1 April 2010. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450&section=text.

Teufel III, Hugo, "Privacy Policy and Guidance Memorandum", Memorandum #2008-02, Department of Homeland Security, Washington, DC, 2008. http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf

Warren, Adam, and Andrew Charlesworth, "Privacy Impact Assessment in the UK", in David Wright, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, Heidelberg, London, New York, 2012, pp. 205-224.

Waters, Nigel, "Privacy Impact Assessment – Traps for the Unwary", *Privacy Law & Policy Reporter*, Vol. 7, No. 9, 2001. http://www.austlii.edu.au/au/journals/PLPR/2001/10.Html

Waters, Nigel, "'Surveillance-Off': Beyond Privacy Impact Assessment – Design Principles to Minimize Privacy Intrusion", Paper presented at: 16th Annual Privacy Laws and Business International Conference: Transforming Risk Assessment into Everyday Compliance with Data Protection Law, St John's College, Cambridge, England, 7–9 July, 2003.

Wright, David, "Should privacy impact assessments be mandatory?", *Communications of the ACM*, Vol. 54, No. 8, 2011, pp. 121-131.

Wright, David, Raphaël Gellert, Serge Gutwirth, and Michael Friedewald, "Precaution and privacy impact assessment as modes towards risk governance", in René von Schomberg (ed.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, Publications Office of the European Union, Luxembourg, 2011, pp. 83-97. http://ec.europa.eu/research/science-society/document_library/pdf_06/mep-rapport-2011_en.pdf

Wright, David, and Kush Wadhwa, "A step-by-step guide to privacy impact assessment", Paper presented at: Second PIAF workshop, 24 April 2012, Sopot, Poland, 2012. http://www.piafproject.eu/Events.html

Wright, David, and Kush Wadhwa, "Introducing a privacy impact assessment policy in the EU Member States", *International Data Privacy Law*, Vol. 3, No. 1, 2013. http://idpl.oxfordjournals.org/

Co-ordinator:
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48 | 76139 Karlsruhe | Germany
Phone: +49 721 6809-146 | Fax +49 721 6809-315
michael.friedewald@isi.fraunhofer.de