The Emergence of Privacy Impact Assessments

David Tancock, Siani Pearson, Andrew Charlesworth

HP Laboratories
HPL-2010-63

Keyword(s):

privacy, privacy impact assessment

Abstract:

This paper considers the emergence of Privacy Impact Assessments (PIAs), and identifies key aspects of their development, concept, practice and policy from their beginnings through to the date of writing (May 2010). A PIA is a systematic process for evaluating the possible effects that a particular activity or proposal may have on an individual's privacy. It should focus on understanding the system, initiative or scheme, identifying, and mitigating adverse privacy impacts, and assisting decision makers in deciding whether or not the project should proceed and if so, in what form. The PIA should be properly distinguished from other business processes such as privacy issue analysis, privacy audits [1] and privacy law compliance checking [2] as these are applied to existing systems to ensure their continuing conformity with internal rules and external requirements.

External Posting Date: May 21, 2010 [Fulltext] Approved for External Publication
Internal Posting Date: May 21, 2010 [Fulltext]

The Emergence of Privacy Impact Assessments

David Tancock[1], Siani Pearson[1] and Andrew Charlesworth[2]

[1] HP Labs, Long Down Avenue, Bristol, UK. BS34 8QZ
[2] Centre for IT and Law, University of Bristol, Queens Road, Bristol, UK. BS8 1RJ
{David.Tancock, Siani.Pearson} @ hp.com; a.j.charlesworth@bris.ac.uk

Keyword(s): Privacy, privacy impact assessment

Abstract. This paper considers the emergence of Privacy Impact Assessments (PIAs), and identifies key aspects of their development, concept, practice and policy from their beginnings through to the date of writing (May 2010). A PIA is a systematic process for evaluating the possible effects that a particular activity or proposal may have on an individual's privacy. It should focus on understanding the system, initiative or scheme, identifying, and mitigating adverse privacy impacts, and assisting decision makers in deciding whether or not the project should proceed and if so, in what form. The PIA should be properly distinguished from other business processes such as privacy issue analysis, privacy audits [1] and privacy law compliance checking [2] as these are applied to existing systems to ensure their continuing conformity with internal rules and external requirements.

Table of Contents

1 Introduction

As of January 2010, the total number of citation counts on *'Google Scholar'* for articles and journals titled *'Privacy Impact Assessment'* appears to be 86, with the highest citation-count for one individual document being 23. This is for an article written by Roger Clarke in 1998, titled *'Privacy Impact Assessments'* [3]. This limited academic interest on PIAs contrasts with the situation in the policy arena, where the topic has attracted notable attention in most of the industrialised countries of the world over the last 12 years. For example, in many jurisdictions such as Canada, Australia, United States (US) and New Zealand (NZ), the practice has been established and documented in the form of PIA guidelines and tools for a good number of years. However, in the United Kingdom (UK) the concept of the PIA may be considered a relatively new process, with the first set of PIA Guidelines being published at the end of 2007 after an international investigation [4]. Therefore, it is important to document the origins and early history of the PIA concept in order to inform the inevitable debates that are likely to be conducted over the coming years.

This report commences with a brief review of the privacy arena in order to provide the context within which PIAs have emerged. The report then identifies key associated notions and terms that pre-dated the concept of PIAs. These ideas are considered because they provide the foundation upon which current PIA processes may be based. The next stage of the report discusses the origins of the term *'PIA'* and furthermore the concept itself is considered. This includes a brief history of PIA development in various jurisdictions. Then an analysis of PIAs is discussed, highlighting the commonalities and differences between the processes and policies. Finally, we discuss the future development of PIAs, focusing on the development of automated decision support systems, and provide conclusions.

2 Privacy

Throughout history, privacy as a concept has been recognised in many diverse regions and cultures of the world. These include writings obtained from ancient Greece, whereby Aristotle wrote about the distinction between the public sphere of political activity and the private sphere associated with family and domestic life [5] and the seminal article written by Warren and Brandeis in 1890, which stated that privacy was the *'right to be left alone'* [6]. However, public interest in privacy has increased in the 20th century, with the proliferation of new technologies, most notably the computer, and has helped to make the concept an important issue of global concern.

For over a century, philosophers, lawyers and political theorists have sought to understand privacy's dimensions from a number of different perspectives and the concept has been deeply contested by both scholars and government agencies. This has resulted in many varied ideas about privacy being published over the years. Indeed, attempts to define a uniformed accepted definition of privacy have been notoriously controversial, and some definitions have been accused of being vague and inconsistent, of being overly inclusive, excessively narrow, or insufficiently distinct from other

value concepts. This is primarily because the concept has many meanings in different contexts, of which some are shown below [7]:

- **Philosophically**: particularly in Europe, people are regarded as being very important for their own sake. The concepts of *'human dignity'* and integrity play a significant role in some countries, as do the notions of individual autonomy and self-determination. In some (though perhaps not all) traditions and jurisdictions, these are the ideas that underpin the notion and significance of human rights.
- **Psychologically**: people need private personal space. This applies in public as well as behind closed doors and drawn curtains. Personal space is the region surrounding a person that he or she regards as psychologically his or hers respectively. Invasion of personal space often leads to discomfort, anger, or anxiety on the part of the victim. Thus, people enjoy having private spaces, and want to keep them, and therefore privacy is the interest that individuals have in sustaining a '*personal* space', free from interference by other people and organisations.
- **Sociologically**: people need to be free to behave and to associate with others, subject to broad social customs, but without the continual threat of being observed.
- **Economically**: people need to be free to innovate. International competition is fierce; all innovators by definition are *'different from the norms of time'* and may perceive themselves to be at risk if they lack private space in which to experiment.
- **Politically**: people need to be free to think, argue and act. However, some types of surveillance, especially in public places or the working environment, may restrict human behaviour and speech.

The following sub-sections consider some broad issues related to privacy, including whether the concept of privacy is a human right in all jurisdictions and whether privacy should take into account the social needs of an individual. In addition, a discussion of the emergence of privacy as a significant policy consideration is included; this can be attributed to the enormous expansion of threats, or claims to privacy.

2.1 Privacy as a Human Right

Privacy's importance is reflected in the fact that fundamental documents that define human rights, such as the *'Universal Declaration of Human Rights'* (UDHR 1948, Article 12), the *'International Covenant on Civil and Political Rights'* (ICCPR 1966, Article 17), and the *'European Convention on Human Rights'* (ECHR 1950, Article 8) all include reference to either privacy or related ideas [8]. Furthermore, the *'European Union (EU) Charter for Fundamental Rights'* (2000), came into full legal force on the 1st of December 2009, when the Treaty of Lisbon was enacted. Article 7 of the Charter corresponds to the meaning and scope of the right guaranteed by Article 8 of the ECHR [9]. However, within these documents there is a considerable degree of inconsistency, as the instruments generally do not define the term *'privacy'* and their scope is usually combined with a range of other freedoms and rights.

For example, in Article 8 (1) and (2) of the ECHR, is a privacy right whereby, individuals have a right to respect to respect for private and family life, home and correspondence, except where the interference is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. In contrast, the US legal system appears more likely to place limits on privacy intrusions by government, via the US constitution than by the privacy sector, against which the US constitution cannot be directly applied [8].

Upon analysis, of the ECHR contracting parties and the US position, we are inclined to suggest that neither the ECHR nor the US constitution in practice treat privacy as a fundamental right. This is because this privacy 'right' can be interfered with on as wide a range of grounds as found in Article 8 (2) of the ECHR. Although, some may argue that Article 3 and possibly Article 4 (1) of the ECHR is actually in practice 'fundamental', in the sense of not being in some way qualified. Furthermore, we suggest that individual privacy rights are more susceptible to interference on 'public interest' grounds. For example, we argue that justifying interception of a person's communication is easier if it is couched in terms of an individual right to private communication versus the public interest in interception (e.g. Article 8 ECHR), rather than a community/social right to private communication versus the public interest in interception (e.g. the privacy penumbra in the US constitution). This may become important in a PIA situation, because the nature of the test employed will affect the balancing exercise(s) that those undertaking a PIA may engage in, and perhaps the outcome of the PIA. Put in a more familiar environment for PIAs, it is easier to justify interference in an individuals privacy interest when arguing their personal data should be merged/matched/shared/mined in the interest of ensuring reduction in benefit fraud, than it is to justify interference in a community/social privacy interest in not having data used in such a way.

Therefore, in this section we will endeavour to discuss the range of possible meanings for privacy, and propose the interpretation that is most appropriate to contemporary needs.

2.2 Social Needs

To try to find a uniform meaning for the term *'privacy'* within the law is a mistake. However, the law does reflect the social and economic needs of individuals; hence, such need could be considered as the appropriate starting-point. Roger Clarke [10] suggests that a reference needs to be made to the emergence of the legal concept of privacy from the late 19th century onwards. Thus, we need to take into account the fact that a considerable amount of change has occurred and continues to occur. Only on that basis can a useful contemporary interpretation of the term *'privacy'* be proposed.

A psychological framework and model for understanding human motivation, management training and personal development was provided by Abraham Maslow during the period 1940-1950. This framework and theory (called *'Maslow's Hierarchy of Needs'* [11]) remains valid today. Indeed, Maslow's ideas surrounding the Hierarchy of Needs - concerning the responsibility of employers to provide a workplace environment that encourages and enables employees to fulfil their own unique potential (self-actualization) - are today more relevant than ever. The framework postulates that individuals' more basic needs have to be largely satisfied before higher-order needs come into play. Thus, if a lower-order need is threatened, the significance of higher-order needs is suspended until the lower-order needs are once again satisfied. The levels of needs are usually represented in the shape of a pyramid, with the largest and lowest levels of needs at the bottom and the highest level of need, such as the need for self-actualisation, at the top. The following list represents the levels attributed to this framework [11]:

- **Level 5:** Self-Actualisation – this is the top level of need and pertains to morality, creativity, spontaneity, problem solving, lack of prejudice, and the acceptance of facts. Furthermore, it promotes the realisation of personal potential, self-fulfilment, and seeking of personal growth and peak experiences.
- **Level 4:** Status (or Self-Esteem) – this includes two levels whereby: the lower level is the need for the respect of others and the need for status, recognition, fame, prestige, and attention; the upper level is the need for self-respect, strength, competence, mastery, self-confidence, independence and freedom.
- **Level 3:** Love or Belonging – this is the middle level and includes needs such as friendship, family and sexual intimacy.

- **Level 2:** Safety – this encompasses basic considerations such as physical security, family security and health, but also broader issues such as security of personal assets and employment.
- **Level 1:** Physiological or Biological – this is the bottom level of the framework and encompasses needs for survival such as water, food, warmth and rest.

The framework describes how people are motivated by needs, whereby most basic needs are inborn, having evolved over thousands of years. Thus, *'Maslow's Hierarchy of Needs'* explains how these needs motivate us all. While Maslow's hierarchy makes sense from an intuitive standpoint, there is little evidence to support its hierarchical aspect. In fact, there is some evidence that contradicts the order of needs specified in the model. For example, some cultures appear to place social needs before any others. Maslow's hierarchy also has difficulty explaining cases such as the *'starving artist'* in which an individual neglects lower needs in pursuit of higher ones. Finally, there is little evidence to suggest that people are motivated to satisfy only one need level at a time, except in situations where there is a conflict between needs. Even though Maslow's hierarchy lacks scientific support, it is quite well known as the first theory of motivation. The framework relates to privacy, because some of the needs and characteristics of self-actualisation include honesty, awareness, freedom, autonomy, trust, privacy, and the individual being comfortable alone. Furthermore, it provides an outline of some important issues that must be addressed if human beings are to achieve the levels of character and competencies necessary to be successful in the information or conceptual age. This indicates that within this framework the interpretation of the need of privacy is about the integrity of the individual and therefore encompasses all aspects of the individual's social needs.

2.3 The Interpretation of Privacy

Written publications on privacy tend to assume the sole focus of privacy rights is, or should be, based solely on individual privacy interests, rather than community privacy interests. For example, Roger Clarke suggests that after applying the *'Maslow's Hierarchy of Needs'* framework to the concept of privacy the following categories can be valuably distinguished [10]:

- **Privacy of the Person** - sometimes referred to as *'bodily privacy'*. This aspect is concerned with the integrity of the individual's body, and is related to the physiological and safety levels of the framework. At its broadest, it could be interpreted as extending to the protection against freedom from torture and the right to medical treatment, but these are more commonly seen as human rights rather than as aspects of privacy. Positive implications that are more readily associated with privacy include compulsory immunisation to protect individual health and requirements for submission to biometric measurement to protect public safety. Negative implications could be an imposed treatment such as lobotomy and sterilisation, or the compulsory provision of samples of body fluids and body tissue. Another negative implication may be a blood transfusion without consent, although it could be argued that there is a case for this in order to save another individual's life.
- **Privacy of Personal Behaviour** – this could also be called *'media privacy'*. This aspect is related to both the belonging and self-esteem levels of Maslow's framework and perhaps to self-actualisation as well. Positive implications of this aspect that are highlighted usually relate to sensitive matters, such as sexual preferences, habits, political activities and religious practices. Nevertheless, the notions of *'personal private space'* and *'private places'*, such as the home or a public toilet cubicle are vital to all aspects of behaviour. The aspect of *'media privacy'* is also relevant in *'public places'*, where casual observation of the individual is usually conducted by people within the vicinity, which is very different from the negative

implication of systematic observation and the recording of images and sounds by other persons or organisations (e.g. surveillance).

- **Privacy of Personal Communications –** this is sometimes known as *'interception privacy'*. This aspect is also related to both the belonging and self-esteem levels of the framework and perhaps to self-actualisation as well. Individuals desire the freedom to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations. One positive implication arising from this aspect is the use of *'mail covers'*, which is a law enforcement investigative technique used in the US that records the outside cover of sealed or unsealed mail to protect national security to fight crime-related issues. Negative implications include the use of directional microphones and *'bugs'* (with or without recording apparatus, telephonic interception and recording), and third-party access to email-messages.
- **Privacy of Personal Data** – sometimes referred to as *'data privacy'* or *'information privacy'*. This is again related to the upper layers of the framework. Positive implications of this aspect include the notion that personal data should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. However, a negative implication may be that personal data is used by third party organisations without consent from the individual.

The term *'privacy'* is sometimes used in the broad sense outlined in the previous list. However, it is often used to refer to some quite specific need or expectation that is in the public eye at the time. For example, the protection of individuals from the attention of paparazzi, and the use of mobile cameras in changing-rooms, or the conduct of interviews in closed rooms rather than semi-open cubicles. A recent development is that many jurisdictions are installing full body scanners at major airports to protect airline passengers and airplanes from terrorist threats. This proposal is a direct consequence of the attempt by Nigerian *'Umar Farouk Abdulmutallab'*, who is accused of trying to detonate a bomb on a plane bound for the US on 25th December 2009 [12]. However, the Equality and Human Rights Commission (EHRC) has stated that these devices risk breaching an individual's right to privacy under the Human Rights Act as they produce *'naked'* images of passengers that could generate illegal images of children and of celebrities that could be leaked online.

One of the most common narrow usages of the term *'privacy'* is to refer to what is described in the previous list as *'privacy of personal data'*, or sometimes the combination of *'privacy of personal data'* with *'privacy of personal communications'*. Moreover, it appears that in some jurisdictions such as the US and Australia, some statues have equated privacy with the idea of *'data protection'* [10]. Therefore, in some jurisdictions, statues have been described as *'data protection laws'*, while others have been entitled *'privacy laws'*. The reasons for this reduction in the scope applied to the idea arose because one or two aspects of privacy (i.e. privacy of personal data and privacy of personal communications) achieved some dominance over the other aspects considered above, which will be discussed in the next subsection of this paper. However, once again we are inclined to suggest that neither privacy laws nor data protection laws in practice treat privacy as a fundamental right.

There is also a tendency not to engage with issues surrounding the context of privacy claims [13], which is briefly touched upon in this section under 'Privacy of Personal Behaviour'. Using a previous example (i.e. section 2.1), justifying interception of a person's communications is easier if the person seeking to intercept can focus solely on the immediate context of interception (i.e. the person whose communication we are intercepting is a terrorist), rather than the broader social context (i.e. this interception will have an effect on other people who use the phone we are intercepting, or allowing this interception will weaken the general prohibition of interception of communications). Alternatively, justifying interference in an individuals privacy interest when arguing their personal

data should be merged/matched/shared/mined in the interest of ensuring reduction in benefit fraud is easier if government can focus solely on the immediate context (i.e. we already hold this persons data, there is a risk of benefit fraud, the individual risk is low), rather than the broader social context (i.e. this will create honey pots for hackers, there will be greater data security risks etc).
Furthermore, we argue that in some jurisdictions, especially in Europe and the US, privacy and Data Protection may be considered as an economic value. This is because, the driving factor behind the 1995 EU Directive on Data Protection (95/46/EC), itself is economic rather than human rights-based (i.e. the need to prevent barriers to free movement of services/information within the EU market caused by conflicting national Data Protection regimes). Moreover, Member States still vary considerably in their attitude towards the human rights element of Data Protection. In the US, their economic-technological approach have to date resulted in frequent legislation at both federal and state levels regarding specific issues (e.g. US Video Privacy Protection Act (VPPA) 1988). However, at the time of writing this paper, the US have avoided passing comprehensive laws on privacy within the private sector.

Phillip Leith [14], suggests that privacy rights are growing apace, as can be seen from a continuing stream of judgments from UK and European courts, and the rise of special interest privacy groups and other institutions tasked to protect privacy. Privacy has as its proponents suggest at last arrived as a fully fledged legal right. However, despite these advancements, Leith suggests that privacy is becoming less prevalent in society; primarily because of technological and cultural changes, but also because the technical legal implementation of privacy is highly problematic. Therefore, we argue that this seeming paradox should be more critically examined by socio-legal researchers who, to date, have done little to test the assertions and assumptions of the privacy lobby and there is a need for more investigation of the basis and assumptions behind Data Protection and privacy law.

2.4 Privacy and PIAs

The emergence of privacy as a significant policy consideration can be attributed to the enormous expansion of threats or claims to it. Roger Clarke states that [3]:

> "The threats have arisen from a combination of the increased scale of social and economic institutions, the increasingly professional and mechanistic forms of management in both the private and public sectors, increasing information-dependence to cope with the reduction in face-to-face contact, and advances in information technology, all feeding off one another."

These contributing factors have influenced a proliferation of policy instruments for privacy, including privacy seals, standards and codes of practice. Moreover, as both private and public sector organisations moved towards conducting risk assessments, there was a general recognition that progressive tools were required to anticipate and mitigate privacy issues and problems.

This conception resulted in many types of *'privacy tool kits'*, some of which were designed to assist in developing procedures and practices for *'Records and Information Management'* (RIM) while others were different privacy-enhancing techniques or self-regulatory approaches. Generally, these tools were originally developed to encourage private organisations to comply with data protection norms. However, these tools also had some relevance to government agencies, particularly those involved with electronic service delivery and e-government applications, and it was within this context concerning the overall search for different innovative ways to encourage organisations to pursue responsible privacy practices and policies that the general idea of the PIA arose [4]. Therefore, we will consider the ideas and terms that pre-dated PIAs further in the following section.

3 The History of Terms

This section takes a chronological approach regarding the related ideas and terms that gave some impetus to the concept of a PIA. In this respect, Roger Clarke [1] identifies three intellectual threads that appear to give rise to the concept and term *'PIA'*. The three threads suggested by Clarke are the *'technology assessment'*, the *'impact statement'* and the *'impact assessment'*, which will be considered in turn.

3.1 Technology Assessment

In the early 1970s a Technology Assessment (TA) was developed by the *'Office of Technology Assessment'* (OTA) of the US Congress; this was practised during the period 1972-1995. Today, the practice of using a TA is covered by the *'European Parliamentary Technology Assessment'* (EPTA) network [15]. A TA is a concept that embraces different forms of policy analysis: the relationship between science and technology on one hand, and policy, society and the individual on the other.

The aims and objectives of a TA are to evaluate the social and environmental costs, the probable detrimental effects and the possible benefits of technological change. The TA process typically includes policy analysis approaches (e.g. foresight, economic analysis, systems analysis, and strategic analysis) and it discusses many important issues including the energy situation, the potential issues of *'nano'* technology in health care and privacy issues related to e-government.

3.2 Impact Statement

During the early 1970s the US introduced the earliest application of an *'impact statement'* in the form of an *'Environmental Impact Statement'* (EIS), which originated from the green movement of the 1960s [16]. An EIS originally came under a law called the *'National Environmental Policy Act'* (NEPA) of 1970. The Act stipulated that a document be produced by federal government agencies to address actions, which significantly affected the quality of the human environment. It appears that an EIS was used as a tool for decision making; it describes the positive and negative environmental effects of a proposed agency action and cites alternative actions. Since 1970 it has been adopted in a number of jurisdictions. For example, in the UK an EIS was used for certain major projects by *British Petroleum'* and *'British Gas'* in relation to projects in the North Sea. However, the procedure was not formally introduced into the planning system.

Today, many criticisms levelled against EISs are based on the early adoption experience within the US, where it was seen to be a slow and costly procedure that usually involved considerable delays caused by lengthy court battles [17]. Moreover, throughout the years, cynicism about the EIS notion arose amongst people affected by major projects; this was primary since the law only required that an EIS be prepared by federal government agencies. Often, the agencies responsible for preparing an EIS do not compile the document directly, but outsource this work to private-sector consulting firms with expertise in the proposed action and in its anticipated effects on the environment. Because of the intense level of detail required in analysing the alternatives presented in an EIS, such documents may take years or even decades to compile, and often are comprised of multiple volumes that can be thousands to tens of thousands of pages in length. This left a multitude of loopholes open using which projects could gain approval despite having excessive negative impacts on the environment, with these problems being glossed over.

3.3 Impact Assessment

During the mid 1980s a more substantial notion was developed, called an '*impact assessment'*. An impact assessment identifies the future consequences of a current or proposed action [18]. In the

form of an *'Environmental Impact Assessment'* (EIA), the assessment ensures that decision-makers consider environmental impacts to decide whether or not to proceed with the project. An EIA identifies environmental impacts early in a project and allows the use of different principles to prevent, limit, or require strict liability or insurance coverage of a project, based on its likely harms. Today, many jurisdictions provide different guidelines on an EIA and an important note is that the EIS has become the document that is produced at the end of an EIA, rather than the end itself.

In the 40 years since its inception, the EIA has become a widely accepted tool in environmental management. As such, the EIA has been adopted in many jurisdictions with different degrees of enthusiasm, where it has evolved to varying levels of sophistication [19]. The *'International Association for Impact Assessments'* (IAIA) also provides guidance on *'Social Impact Assessments'* (SIA) but privacy is not a focal point of the movement and it appears that the IAIA does not recognise the PIA as a sub domain, nor has mentioned PIAs in any of their journals (which are published every three months).

Although privacy is not an environmental factor in an EIS, an EIA or a SIA, their methodologies are very similar to the processes used in a PIA. For example, an EIA process follows a methodology with feedback loops including public involvement and consists of project identification, screening, scoping, impact analysis, mitigation, environmental statement, review, decision-making, and follow up.

3.4 Privacy Impact Assessment

The earliest reference to the term *'PIA'* mentioned in related journals and articles is in a private communication between Roger Clarke and Lance Hoffman in 2004 [1]. This communication states that Lance Hoffman assisted in the preparation of a Berkley, California ordinance requiring a PIA and that the ordinance is included in Hoffman's work of 1973. The communication also indicates that the term was used in discussions with Karl Reed and others in the context of the *'Australian Computer Society's Economic Legal & Social Implications Committee'* (ELSIC) in the mid-1980s. The earliest references this paper has identified for the term *'PIA'* appears to be the following contributions:

1) An Australian acknowledgement in 1995 [20] by Warwick Smith, a telecommunications industry ombudsman who stated that a PIA had a role to play.
2) The Deputy Privacy Commissioner of NZ, Blair Stewart, who wrote two of the earliest papers on PIAs in 1996 [21], which were published in the Australian journal called the *'Privacy Law & Policy Reporter'*.
3) In 1996 [22] the US *'Internal Revenue Service'* (IRS) recognised the importance of protecting the privacy of taxpayers and employees within their automated systems: the IRS suggested that the vehicle for addressing these issues was a PIA.

In the next section, we will briefly discuss the historical development of PIAs, considering the initiatives and notions that gave rise to the emergence of the concept.

4 The History of the Concept

In this section, the initiatives and notions that gave rise to the emergence of the PIA concept will be highlighted and considered. To pinpoint the precise genesis of a PIA with any accuracy is certainly difficult. Their emergence as a policy innovation certainly needs understanding within the context of larger trends in advanced industrial societies to manage *'risk'* and the assumption that the burden of proof for the harmlessness of a new technology, process, service or product should be placed upon the promoters, rather than society as a whole. Extrapolated to the area of privacy, this approach

means that personal information systems are considered as relatively dangerous until shown to be relatively safe, rather than the other way around [6].

Within the privacy realm, there are a number of early references to the desirability of conducting prospective evaluations of compliance with legal norms. Examples especially include policy documents in the US and Australia: for instance, the US Health, Education and Welfare (HEW) departmental document published in 1973, which addressed specific questions relating to the collection of data [23], or in Australia, the cost-benefit analysis of data matching programmes [24].

The HEW document [23] concluded that each time a new personal data system is proposed or modified, those responsible for the activity should answer the following questions explicitly:

- What purposes will be served by the system and the data to be collected?
- How might the same purposes be accomplished without collecting these data?
- If the system is an administrative personal data system, are the proposed data items limited to those necessary for making required administrative decisions about individuals as individuals?
- Is it necessary to store individually identifiable personal data in computer-accessible form, and, if so, how much?
- Is the length of time proposed for retaining the data in identifiable form warranted by their anticipated uses?

Moreover, in 1977 the US *'Privacy Protection Study Commission'* produced a report, which addressed personal privacy in information systems after the introduction of the 1974 *'Privacy Act'* [25]. The scope of the report was the relationships between individuals and various record-keeping organisations and it examined the balance between the legitimate, and sometimes competing, interests of the individual, the organisation, and society in general. The most significant finding of the Commission's report indicates that the *'Privacy Act'* takes an important step in establishing a framework by which an individual may obtain and question the contents of his/her record. However, the Act does not address the question of who is to decide what and how information should be collected and how it may be used.

Data matching [24] searches and matches specific data relating to a person such as surname, address, and date of birth. The *'Data-Matching Program (Assistance and Tax) Act'* 1990 [26], included a requirement for a data matching program and allowed personal data to be transferred between government agencies such as the Tax agency and the department for Social Security. Overall, it appears that this Act is closely related to the PIA notion in that it included requirements to document several initiatives. For example, the Act required an organisation to document the following: the justification for the program; what methods other than data matching were available; why they were rejected and cost/benefit analysis. Cost-Benefit Analysis (CBA) is a cluster of techniques that evaluate projects based on narrow financial criteria, or on broader financial and non-financial factors, or on a yet broader range of factors in order to reflect perspectives additional to that of the sponsor. CBA was applied to the assessment of computer matching projects in a number of jurisdictions around the mid 1990s, and it appears that in the US there was a proposal for a regulatory scheme for computer matching which had an equivalent method to a PIA [27]. However, these early references probably regarded PIAs as statements prepared as a condition precedent to approval of a project or the debate of legislation and there was no actual use of the term 'PIA'.

We should also remember that the basis for many early European regimes (particularly those in Scandinavia and France) was upon a licensing model, whereby there was no processing of personal data unless the data protection authority gave prior permission and there were instances where the occasional use of pre-decisional assessments occurred in some European countries [28]. Indeed, this process is included within Article 20 of the European Directive (95/46/EC), which mandates the need for *'prior checking'* (see sub-section 5.7) of certain especially sensitive information systems

against applicable standards [29].

It is often an assumption that NZ has been the pioneer in PIA development and guidance due to the influential work of the then Assistant Commissioner Blair Stewart in 1996 [2, 21]. However, we should also consider the fact that guidance material for PIAs produced by the US Office of the Privacy Advocate in the Internal Revenue Service (IRS) dates from the mid-1990s [30].

Therefore, what we can say is that these various trends and influences seem to have converged in the mid-1990s when experts and officials in Canada, NZ, US and Australia began to think seriously about PIAs in a more systematic way as an essential tool for data protection. Moreover, the last 15 years have seen PIAs gradually spread around the policy community, even though policy tools took a while to develop, which was largely due to the following factors [4]:

1. Legislative requirements.
2. Policy guidance by government agencies and recommendations issued by privacy and data protection commissioners in countries such as Canada, New Zealand, Australia, Hong Kong, US and the UK.
3. The recognition by organisations that PIAs could expose and mitigate privacy risks, avoid publicity, save money, build trust and assist with legal compliance.

Upon analysis, it seems that the driving forces underlying the emergence of PIAs can be interpreted as follows. First, the demand for PIAs can be seen as a belated public reaction against the increasing privacy-invasive actions of governments and organisations during the second half of the twentieth century. Thus, increasing numbers of people wanted to know about organisations' activities and wanted to exercise control over their excesses. Furthermore, privacy oversight agencies and privacy advocacy organisations called for the techniques to be applied and then called for action.

Second, the adoption of a PIA can be seen as a natural development of rational management techniques as significant numbers of governmental and corporate schemes suffered low adoption and poor compliance. Thus, organisations came to appreciate that privacy was a strategic variable and therefore factored it into their risk assessment and risk management frameworks.

Third, the development of PIAs occurred in parallel within various jurisdictions. Therefore it is important to discuss the emergence of PIAs within these countries, which is done in the following section.

5 Brief History of PIA Development within Jurisdictions

In this section, we will briefly discuss the historical development of PIAs, considering the significant contributions, initiatives and notions that gave rise to the emergence of the PIA concept in each jurisdiction.

5.1 Three Provinces of Canada

The Privacy Commissioners of Ontario and British Columbia (BC) were some of the early movers in developing PIAs within Canada in the mid 1990s. The two provinces were soon followed by the province of Alberta. Today, most provinces and territories in Canada have become active users of PIAs, in name at least [1].

In the province of Ontario early contributions regarding PIAs were made by the then Privacy Commissioner Tom Wright (1993, 1994, 1995, 1997) [1]. However, the principal driver behind government policy in relation to PIAs was not the privacy oversight body (i.e. Information Privacy Commissioners Office (IPCO)), but a central agency called the *'Management Board Secretariat'* (MBS) [31]. The MBS decided in June 1998 that a completed PIA became a pre-requisite for

approval of *'Information and Information Technology'* (I&IT) project plans submitted for Cabinet approval. The first set of guidelines for the application of PIAs was approved in 1999 by the MBS and was updated in 2001. However, in 2006 the MBS functions to oversee PIAs were absorbed within the *'Ministry of Government Services'* (MGS), who have now become the central agency. The current set of guidelines for PIAs was updated in 2009 by the MGS and is being used to assess privacy implications in I&IT projects that deal with personal information in government departments and agencies [32]. Recent developments have seen the Privacy Commissioner of Ontario express some real concerns about a new government plan to share biometric data (i.e. fingerprints) with Britain, Australia, the US and NZ to combat immigration fraud, and especially at the perceived need for high-value data-sharing by the government's *'Immigration Department'* [33]. At the time of writing, the Commissioner is waiting for a response from the *'Immigration Department'* regarding these concerns.

In BC, early contributions to the emergence of PIAs were made by the then Privacy Commissioner David Flaherty (1994, 1995) [1], and by the late 1990s, PIAs of some kind were well developed within the province's public sector. The impetus for the application of PIAs in this province was provided by a public disturbance over disclosure of the City of Victoria's property value assessments on its main website in 1998 [34]. In 2002, the *'Freedom of Information and Protection of Privacy Act'* was amended such that section 69 (5) required agencies to conduct PIAs for a new enactment, system, project or program and the process has been supported by guidance since as early as 1998. Since 1998, BC has held copies of PIA summaries on its main database, and the current number is approximately 165; however, it appears that the scope is limited to the determination of their compliance with the 2002 amendment of the *'Freedom of Information and Protection of Privacy Act'*. Therefore, we would argue that they are little more than a data protection law compliance check and fall a long way short of being a comprehensive PIA.

In the province of Alberta, section 64 of the *'Health Information Act'*, which was enacted in 1999, imposes on public agencies in the health care sector the requirement to conduct PIAs [10]. The PIA in Alberta is based on the EIA model and its scope is defined in the following statement [35]:

> "PIAs are used in Alberta for proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information that may affect the privacy of the individual who is the subject of the information."

However, PIAs are not mandated elsewhere in the Alberta public sector and a central agency, called *'Services Alberta'*, provides guidelines in relation to their conduct. Moreover, little evidence has emerged from this province that PIAs for institutions outside the health sector have increased on previous years, which may reflect the fact that for PIAs for these organisations the process is not mandatory.

5.2 Federal Canada

The impetus for the introduction of PIAs at a federal level was the debacle surrounding the *'Human Resources Development Canada's (HRDC) Longitudinal Labour Force File (LLF)'* in 2000, which cost the department millions of dollars [36]. The federal government's response to this incident and concerns about the impact and cost of future privacy issues in the provision of government services led to the *'Treasury Board'* of Canada being given the task of creating a PIA policy to ensure that privacy was considered throughout the design or re-design of programs or services [37]. At the federal level, PIAs are not explicitly provided for in either the *'Privacy Act'* of 1983 or the *'Personal Information Protection and Electronic Documents Act'* (PIPEDA) of 2001. However, the federal policy premises that federal government departments and agencies should actively seek to be in compliance with the principles enumerated in the *'Code of Fair Information Practices'* in the federal

'Privacy Act'. Thus, PIAs are seen at a federal level as an effective method of achieving such compliance.

The *'Information and Privacy Policy Office, Chief Information Officer Branch, Treasury Board of Canada Secretariat'* is the central agency that administers and interprets PIA policy and provides advice to institutions, the President of the Treasury Board and the Treasury Board itself. It is tasked with developing and maintaining guidelines to assist organisations in implementing the policy and is responsible for monitoring compliance.

Since 2002 the central agency has published several versions of the guidelines and tools for PIA development and application. The current set of PIA guidelines, which were updated in 2009, require that initiatives comply with privacy requirements and resolve privacy issues that may be of potential public concern and the process is accordingly not limited to compliance with privacy laws. Recent developments concerning PIAs at the federal level has seen the introduction of a tool for a *'Preliminary PIA'* (PPIA) in 2007. This tool, called a *'PPIA Report Template'*, contains the following key elements [38]:

- **Executive Summary**: this may be used as an appropriate way to communicate the results of the PIA with the public
- **Introduction**: this includes the reason(s) for conducting a PPIA rather than a PIA on the project; it clarifies objectives and provides a statement of work to be performed and any assumptions affecting the scope of work
- **Project Background**: this describes the project, including objectives, clients, governance structure, business case and deliverables, and lists each stakeholder's role and responsibilities
- **Legislative and Policy Authorities for the Project**: this section enables the user to list the relevant Acts, policies or regulations with section references and the reason(s) for citation, including the *'Privacy Act'*, *'PIPEDA'*, *'Privacy and Data Protection Policy'* and the *'Integrated Risk Management Framework'*.
- **Description of Personal Information**: this section lists each data cluster of personal information and the data elements contained within the cluster. For example, name, address telephone number and date of birth. It also provides an overall narrative description of the data flow for the collection, use and disclosure of personal information clusters as it relates to stakeholders
- **Potential Privacy Risks**: this describes each potential privacy risk and possible options for mitigating the risk
- **Overview of Security Requirements**: this describes security requirements and plans for the 'Threat and Risk Assessment' (TRA)
- **PIA Plan**: this section describes: the PIA activities and planned timelines; any assumptions about the scope of the PIA; any consultation planned with the public or with the 'Office of the Privacy Commissioner' (OPCC); any resource requirements for conducting a PIA

Furthermore, in October 2007 the OPCC conducted an audit report on the privacy impacts of programs, plans and policies [39]. In this report, the OPCC has made multiple recommendations for improvements concerning not only PIAs, but also a range of privacy issues.

In October 2009 the OPCC responded to a PIA report completed by the *'Canadian Air Transport Authority'* (CATSA) in anticipation of the deployment of *'Millimetre Wave'* (MMW) screening technology at selected major airports throughout the country. In this letter, the Commissioner made several recommendations to CATSA and is currently waiting for a formal response from them concerning those recommendations [40].

5.3 New Zealand

Throughout the years, significant published works by Blair Stewart have contributed to the emergence of PIAs in most jurisdictions. These include some of the earliest papers on PIAs in 1996 [2, 21], and later papers in 1999, 2001 and 2002 respectively [41, 42, 43]. Moreover, Blair Stewart was one of the first to define a PIA and distinguish it from a privacy compliance audit and legal opinion in a speech in Hong Kong in 2001 [42], when he stated that a PIA was *'an assessment of any actual or potential effects that a proposal may have on privacy and the ways in which any adverse effects can be mitigated'*.

The impetus for the application of PIAs within NZ arose due to tensions between the then Privacy Commissioner, Bruce Slane, and the *'Department of Transport'* in relation to a project to establish a new national driver licensing scheme and card. The outcome of this dispute not only led to a government cabinet instruction being issued requiring the department to perform a PIA (because it was recognised at the time that the scheme would have substantial privacy impacts [6]) but also the Commissioner adopting a policy of encouraging PIAs in particular circumstances. In January 1999 the Privacy Commissioner published a *'Guidance Note in Information Matching Privacy Impact Assessments'* (IMPIA) [44]. The scope of this guidance is restricted to matching programmes, which are the subject of specific requirements under the 1993 *'Privacy Act'* and the current version of the guidance document is dated 2006. However, since 1996, there has been a statutory requirement for each of the approved matching programs to undertake an IMPIA and currently 46 approved matching programs have been the subject of this process.

A set of guidelines for conducting PIAs was published in 2002 [45] and it acknowledges the authorship of Blair Stewart, David Flaherty and Nigel Waters, as well as the parallel work done on PIAs in Alberta, Ontario and BC and also interactions with Hong Kong. The current set of guidelines (dating from June 2007) provide detailed practical guidance on how to prepare a PIA report. However, the materials that describe the PIA processes are very similar to those in the original set of 2002. Therefore, we suggest that no significant progress in the development of PIAs has taken place in NZ since the international report in 2002 [4].

5.4 Federal Government of the United States of America

Within the US a complex body of law (i.e. constitutional, tort and statutory) governs the collection, processing and disclosure of personal information at a federal and state level. Furthermore, there are several federal provisions enacted for certain sectors such as the *Health Insurance Portability and Accountability Act'* (HIPPA, 1996), which protects the privacy of individuals within personal health information [8].

Three legislative provisions are especially relevant for the conduct of PIAs within the federal government [46]. The first provision is the *'Administrative Procedure Act of 1946'* (APA), which governs the general method by which federal agencies may propose and establish regulations; this Act requires agencies to keep the public informed of their organisation, procedures and rules. The second legislation is the *'Privacy Act of 1974'*, which establishes the statutory *'fair information principles'* for federal agencies and obliges the publication of Systems *of Record Notice'* (SORN) when most new personal information systems are established. Thus, all federal agencies are required to publish the records of each system (i.e. new or modified) in the *'Federal Register*'. However, there are some exemptions for systems established for national security reasons.

The third legislation regarded as the main impetus for PIAs in the US is the *'Electronic Government Act of 2002'* [46], which states that each federal agency shall undertake a PIA before:

I. Developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form

II. Initiating a new collection of information

Agencies are to ensure review by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and if practicable, after completion of the review under clause (ii) of the *'Electronic Government Act'*, make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means. However, this requirement may be waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment. This legislation was designed to supplement the broader requirements within the *'Privacy Act'*.

The history of PIAs within the US dates to the mid 1990s when the *'Inland Revenue Service'* (IRS) began to require PIAs for large projects and indeed issued a set of PIA guidelines in 1996. The IRS conducts PIAs on information systems that collect personally identifiable information and the current version of the IRS guidelines is dated 2000. However, the language used is difficult to read and expansive, but the actual activity that they require appears limited as the document refers not to the *'conduct'* of a PIA but to its *'completion'*, indicating that it is perceived as a product rather than as an important process that could influence privacy design. Upon analysis, it appears that this document may be driven from the provisions of some US statues and not from an assessment, analysis or examination of a proposed system, initiative or scheme or its possible privacy impacts [30]. Furthermore, the *'Department of Homeland Security'* (DHS) Privacy Officer has authority under section 2.22 of the *'Homeland Security Act of 2002'* to require PIAs and a *'Privacy Threshold Analysis'* (PTA) instrument is used to determine whether a PIA is required.

A vast number of PIAs is being completed each year in the US, and this may be because there is a legislative mandate for government agencies to do so. However, government agencies may have subverted the term *'PIA'* to refer to a mere legal compliance study and US private sector philosophies tend to reject the notion that public policy and consumers might have a role to play in the design of business systems, with international significance because US corporations have such a substantial impact throughout the world.

5.5 Private Sectors in the United States of America

Within the private sector of the US, there is still very little evidence of PIAs at state level. Even in California the only signs of progress have been a 2006-07 legislative debate over a Bill that mentioned PIAs, and a declaration by the State's *'Office of Privacy Protection'* that it is developing a method and tools for agencies to use. However, at the time of writing there is no evidence of either PIA policy or PIA tools published by the State Office.

5.6 Australia

An early form of PIA was developed in Australia in 1990. This early form was called a *'program protocol'* that was imposed on a particular family of data matching programs by section 12 of the *'Data-Matching Program (Assistance and Tax) Act'* [1]. In 1992, non-binding guidelines for application to other data matching programs were published and both sets of guidelines were prepared by Nigel Waters, Deputy to the then Privacy Commissioner, Kevin O'Connor.

The earliest mention of the term *'PIA'* found in Australian sources appears to be a 1995 acknowledgement by the *'Telecommunications Industry Ombudsman'*, which stated that PIAs had a role to play [20]. The impetus for PIAs in Australia was provided by Blair Stewart's publications and David Flaherty's work in BC and soon afterwards, descriptions of the PIA process in lesser and greater detail were published by Roger Clarke in 1998 [1].

In December 2001 the then Privacy Commissioner, Malcolm Crompton, issued *''Guidelines for Agencies using PKI to communicate or transact with individuals'*, which resulted in a draft set of

generic guidelines, which was released for public consultation in 2004, and published in the final form by Crompton's successor two years later in 2006. In addition, the *'State of Victoria'* issued a set of guidelines on the PIA in 2004 [47], and another major State (e.g. New South Wales) was very supportive of PIAs at the time, but has since lacked the resources and government commitment to pursue the matter.

It is evident that many mainstream agencies and authorities such as Health and Statistics in Australia have conducted separate PIAs even though they are not compelled to do so by legislation or policy mandates, but through persuasion from the Privacy Commissioners. In 2009, the Victorian Commissioner published a set of guidelines on PIAs, which appear to be very similar to the original set produced in 2004: both could be regarded as a straightforward implementation of the fair information principles with Canadian influences.

5.7 Europe

Article 20 of the 1995 EU Directive (95/46/EU), headed *'Prior Checking'* [29], states that:

> "Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof."

The requirement appears to have been implemented in the laws of some 20 of the EU nations, but the form in which it is expressed is highly varied and the coverage is very patchy. Moreover, the actual extent to which the various laws are respected is far from clear.

As of May 2010, searches within *'Google Scholar'* with the title *'PIAs in Member States of the European Union'* (EU), have generated virtually no material. The exceptions to these were four jurisdictions:

1. United Kingdom – this will be discussed in the next sub-section.
2. Finland – who have discussed the possibility of using PIAs [1], based on the models found in Canada, Australia and New Zealand. However, no collaborating evidence or material related to PIAs within Finland has been found at the time of writing.
3. The Netherlands – who have mentioned the term within government documents for a very long time [1], but so far, nothing has come of it.
4. Ireland – where the Data Protection Commissioner recommends that documented PIAs be carried out in relation to any proposal to apply biometrics in the workplace or school [48].

5.8 United Kingdom

Within the UK, the concept of the PIA may be considered a recent development. In November 2007, following an international survey leading to the publication of a report [4], the Information Commissioners Office (ICO) launched its own PIA process. This took the form of a Handbook to help organisations assess the impact of their operations on personal privacy. At the same time, the loss of personal data relating to child benefit records by HM Revenue and Customs resulted in a Cabinet Office review. The ensuring report, *'Data Handling Procedures in Government'*, published in June 2008, mandated the use of PIAs in central government departments and called for PIAs to be built into the government's reviews of information and technology projects [49].

The Handbook was updated in 2009 [50] and has become a significant part of the privacy *'toolkit'*. Initial indications are that it is gaining traction in influencing public policy. In January 2010, the Cabinet Office published a report, whereby it states the *'Data Handling Review'* (DHR) obliges government departments to carry out PIAs on new projects or programmes involving

significant amounts of personal data [51]. In Annex A (4) (e.g. Process Measures to Manage Information Risk) of the report, it states that PIAs in the UK are now established, and ongoing, as shown below:

> "Annex A: (4). Conduct Privacy Impact Assessments (PIA): Established and Ongoing - All new ICT projects that include personal data must now complete a PIA; guidance on the process is provided on the Information Commissioner's website. The PIA is also being applied to the development of new policies that encompass the handling of personal information."

The report, also suggests that the ICO has done significant work in promoting the use of PIAs across government through the provision of guidance and workshops. If PIAs are used, for any proposal that involves the processing of personal data privacy must be considered early in the planning process, allowing any adverse impacts to be reduced or avoided altogether. 270 such assessments are now complete or underway across government and departments are making sure that these processes are part of all procurements of IT systems or projects involving large amounts of personal data.

Warren et al concluded in their 2009 Report [52], that there were some difficulties experienced by organisations in the UK when they considered conducting PIAs:

- **Internal Stakeholder Resistance**: project managers often perceived PIAs to be a burden; public relations managers were wary of engagement with external stakeholders, or publication of the process; and security officers sometimes considered PIAs to be a threat to their expertise, and consequently their position in the organisation.
- **External Stakeholder Resistance**: external stakeholders (e.g. independent experts, regulators, civil society groups, professional bodies and charities) can often be reluctant to engage with an organisation conducting a PIA. This is either through lack of interest, lack of trust, or lack of resources.

The report [52] also noted that the ICO itself did not have the resources to validate PIAs and that civil society groups, in particular, were often too time-pressured – and lacked the resources - to contribute to the process. Therefore, it may be necessary for organisations conducting a PIA, to host working lunches or visit external stakeholders, rather than expecting them to read lengthy documents or visit other organisations.

One of the first Government Departments to undertake a PIA in the UK was the '*National Policing Improvement Agency'* (NPIA), relating to how they managed and shared information between authorities. This primarily involved the *'Police National Database'* (PND) [53]; it appears that the PND is not a new operational database, but an existing one, which creates new information by discovering links between existing information on a number of police authorities. The following list shows some of the reasons why a PIA was carried out by the NPIA, in relation to the PND:

1. Identify and manage the risks that privacy issues represent to realising the intended benefits of PND
2. Generate information to aid decision making and support good governance and business practice around information processing
3. Identify any necessary privacy features so these can be designed in at an early stage rather than be subject to costly retro-fitting at a later stage
4. Allow privacy considerations to be built into the design from the outset to provide a foundation for a flexible and adaptable system, reducing the cost of future changes and ensuring a longer service life

5. Promote public confidence to maximise the information that people are prepared to disclose to the police and reduce the risks of privacy-related incidents that could undermine public confidence and cause embarrassment to the Police Service, the NPIA or the Government.

An initial screening was done to decide whether a full scale PIA or small scale PIA was necessary and involved a considerable number of questions, which are included in the appendices of the (NPIA) report. It seems significant that most questions were answered *'YES'* or affirmative in the screening process and the results were then initially discussed with the ICO. This discussion resulted in a full scale PIA being carried out and the results obtained from the PIA proposed a number of features and processes for the PND, which included the following criteria [53]:

- Protection to ensure that the system is only accessible by authorised, trained users
- Users will only be able to access the sorts of information and facilities that they need to do their job
- All use of the system will be logged and subject to audit
- PND capabilities will be designed with consideration of privacy requirements
- Rules for the use of the system, and of any information obtained from it, will be set. These will include that the system and data must only be used for policing purposes.

Another Government Department to publish a PIA report is the *'UK Border Agency'* [54] on 21st August 2009. Its uniqueness is that the report is on the international exchange of information between certain countries where many of the privacy issues and risks manifest themselves in different ways than they do in new projects or initiatives. In deciding whether to conduct a PIA and what type of PIA to conduct, they considered carefully the scope of international protocols and their potential risks, which are outlined in the following list:

- The project does not involve the introduction of new legislation, or present a new policy area. Concepts and practices of data sharing based on fingerprint checks for immigration functions are already well advanced in other contexts, for example, across Europe through the Eurodac system. However, whilst this project largely builds on such initiatives, it does contain new features, whose privacy impacts need to be understood and any adverse impacts minimised.
- The project does not involve collecting or storing new data from individuals, but it does involve new arrangements for exchanging personal data (including some sensitive personal data) with authorities of different countries. The ability of Her Majesty's Government to control the use of that data may therefore be diminished.
- The data will be used for limited purposes that are already well established, namely immigration and nationality purposes, which are generally the same as or similar to the purposes for which the data was originally collected. Nevertheless, these purposes involve inherent sensitivities.
- The project involves data sharing on a case-by-case basis, based on fingerprint matching, rather than bulk data exchange.
- The other countries with which data will be shared are outside the EU and therefore not bound by European Data Protection legislation. It is important to find other ways to ensure that the rights and freedoms of data subjects are respected.
- Each of the countries participating in the project has committed to developing clear arrangements for how it will operate and how privacy risks will be minimised, with the guidance of privacy experts in each country. Having such arrangements in place should be a major factor in mitigating the privacy risks, and the PIA process should help make sure they do so.

The Border Agency decided to follow a small-scale PIA process because the project had privacy issues associated with it, but not the large inherent risks that would warrant a full scale PIA. For example, those typically associated with new policy areas, major new databases, or using data collected in connection with one purpose for very different purposes. Nevertheless, the Border Agency found that a substantial range of issues emerged, and expanded their approach to ensure that those issues were all addressed appropriately.

5.9 Hong Kong

PIAs were discussed at length in Hong Kong at an international computer conference in September 2008, where the guest speaker was the current Commissioner Mr Robert Woo who said on the subject of PIAs [55]:

> "Prevention is always better than cure is an axiom that also applies to the protection of personal data. Hence, where a new project or undertaking is to be launched involving the collection and holding via electronic means of a large number of personal data or personal data of a sensitive nature. The data user is advised to undertake a privacy impact assessment. An example that should be followed is the Smart ID card of 2003 where the Immigration department undertook no less than 4 PIAs before actually going ahead with the project."

Currently the Commissioner is undertaking a major review of the 13-year-old Ordinance and has made several important proposals. However, so far, he has not mentioned PIAs, but it is reasonable to expect that some provisions will be made relating to PIAs in the future.

The analysis of the history of PIAs within the jurisdictions shows that there are some commonalities and differences between the processes, policies and application of PIAs. Therefore, it is important to reflect this in the following section.

6 Analysis of Commonalities and Differences between PIAs

In this section, we seek to focus on the commonalities and differences between PIAs throughout the major jurisdictions that currently conduct them.

6.1 Common Characteristics of PIAs

Over the years, there have been many different arguments advanced in favour of PIAs. Descriptions of the benefits of conducting PIAs are common features of the guidance material provided by various regulators around the world. The following list shows some examples of the common elements attributed to PIAs.

- **Meeting and Exceeding Legal Requirements:** Data protection legislation only addresses certain aspects regarding privacy: there are other types of legislation that have an impact on privacy and either empower or prohibit certain acts that may intrude upon the privacy of the individual. In this respect, a PIA should accept their values and check that they have all been complied with as an integral part of the risk management assessment.
- **Needing to be Prospective:** PIAs are most useful for new programmes, services or technologies. They should occur in advance of the application or introduction to spot and raise privacy issues at an early stage of the planning process. They must therefore have the potential to identify, avoid, mitigate, stop, or suggest alternative solutions to privacy risks, as well as the ability to modify plans accordingly.

- **Avoiding Unnecessary Costs:** By performing a PIA early in a project, an organisation avoids problems at a later stage, when the costs of making significant changes will be much greater. Also, building privacy sensitivity into the design early provides a foundation for a flexible and adaptable system thereby reducing costs and ensuring a longer life for the application.
- **Eliminating Inadequate Solutions:** Privacy impacts discovered at a later stage are often not as effective at addressing and managing those designed into the project from the start. Therefore, designing in privacy solutions can make the project more resistant to failures and much better equipped to recover if failure does occur.
- **Avoiding Loss of Trust and Reputation:** A PIA is a means of ensuring that systems that contain privacy flaws are not implemented, and hence avoid attracting the attention of competitors or the media and avoid giving rise to concerns among customers. In this context, a PIA will help to maintain or enhance an organisation's reputation. Thus, by addressing the identified privacy issues early, a PIA can mitigate not only the risks of low adoption rates regarding the perceived harm to privacy or the protection of personal information, but can also mitigate the risk of retrospective imposition of regulatory conditions as a response to public concerns about the project. Furthermore, a PIA can provide an organisation with a commitment from stakeholders to support the project from an early stage, thereby avoiding opposition from stakeholders at a late stage in the process when it is more expensive to enact change.
- **Informing Decision Makers:** A PIA helps decision-makers to decide whether the project should continue, and in what form.
- **Informing Stakeholders:** A PIA should enable stakeholders to achieve an understanding of the project early and assess it from their own perspective. Therefore, an organisation should make the aims of the project better understood and provide stakeholders with the opportunity to have their perspectives reflected in the design of the project, thereby pre-empting any possible misinformation campaigns by opponents of the project.

In summary, it appears that PIAs are more beneficial to organisations than to individuals, although PIAs do help organisations to benefit society generally and to protect individual privacy. Privacy rights are protected and advanced by convincing agencies and businesses to carry out a PIA for the following reasons: to demonstrate legal compliance, to allow organisations to develop better policy, to save money, to develop a culture of privacy protection, to prevent adverse publicity, and to mitigate risks in advance or resource allocation. However, there are some variations in the implementation of PIAs within the different jurisdictions under study. In the next section, we consider these aspects.

6.2 Variations of PIAs Processes

Our analysis of the various guidance materials indicates that PIAs vary across jurisdictions sometimes substantially and that there are many interrelated dimensions. The following sub-sections describe the major dimensions that we have identified.

6.21 Defining PIAs

Since the early 1970s when the term was first used [1], the meaning ascribed to the term *'PIA'* by privacy oversight offices (e.g. UK Information Commissioners Office (ICO)) and by central agencies (e.g. Treasury Board Secretariat (TBS) of Canada) has varied over time and across most

jurisdictions. Some examples of representative definitions and descriptions for PIAs found in law, policy and guidance material across the various jurisdictions studied are illustrated in figure 1.

JURISDICTION	DEFINITION
United Kingdom	"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." [50]
New Zealand	"A PIA is "a systematic process for evaluating a proposal in terms of its impact upon privacy" [45].
Canada	"PIAs are used to identify the potential privacy risks of new or redesigned federal government programs or services." [38]
Australia	"A PIA is an "assessment of actual or potential effects on privacy, and how they can be mitigated." [56]
United States of America	"A PIA is an analysis of how information in identifiable form is collected, stored, protected, shared and managed...[to] ensure that system owners and developers have consciously incorporated privacy protection throughout the entire life cycle of a system." [57]
Canadian Province of Alberta	"A privacy impact assessment (PIA) is a process that assists public bodies in reviewing the impact that a new program, administrative process or practice, information system or legislation may have on individual privacy." [35]

Fig. 1. Definitions for PIAs

The different definitions provided by the guidance material for PIAs may be synthesised and interpreted to give the following broad definition:

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

A PIA is partly a predictive exercise, looking to prevent or minimise adverse effects on privacy. Typically, PIAs are a series of steps, posing and answering questions and considering options, as

discussed further in the next section of this paper. However, a PIA is different from other business processes, such as privacy issue analysis, privacy audits, or privacy law compliance checking. This is because these processes apply to existing projects, to ensure their continuing conformity with internal rules and external requirements [2].

6.22 The Level of Prescription

The requirements for conducting PIAs within different jurisdictions are by *legislation* (e.g. required by law), prescribed by binding *policy*, or *recommended* by those with no legal authority (e.g. Privacy Commissioners) and the landscape can be very complex, as illustrated in Figure 2.

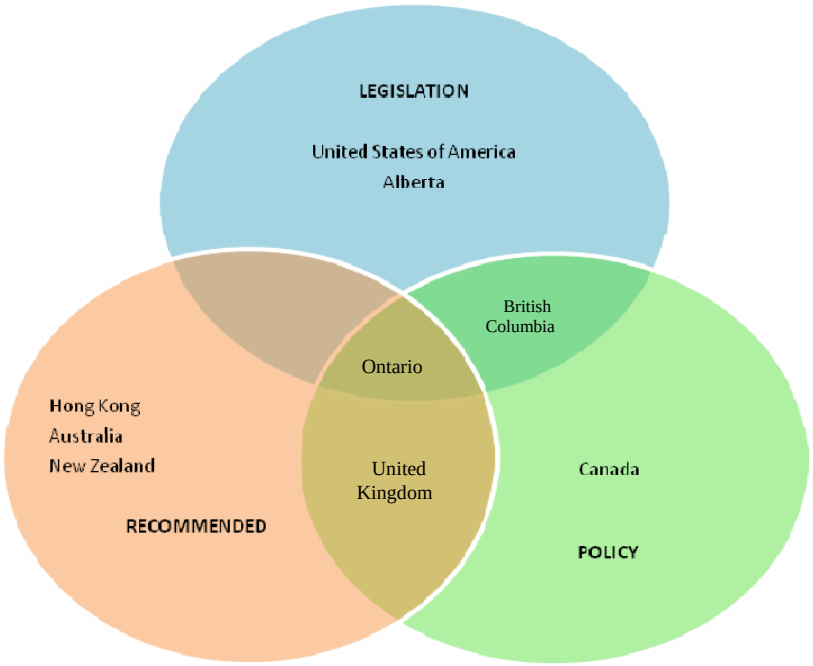

Fig. 2. Prescription Levels for PIAs within jurisdictions

In some jurisdictions, the requirement to undertake a PIA is enshrined in law. These jurisdictions include the US, the Canadian provinces of BC, Alberta and Ontario (e.g. health organisations, where the health information statutes have mandatory PIA (or PIA-like) provisions). Where PIAs are mandated, their nature is dictated by the language of the statute [4]. For example, the US federal *'E-Government Act'* (2002), which requires agencies to conduct a PIA before developing or procuring IT systems or projects that collect, maintain or disseminate information in an identifiable form.

Experience in the US suggests that the legislative mandate produces a large number of PIAs each year, because it is a necessary condition for receiving budget approvals especially for IT procurement projects. Although PIAs in the US ensure that there is some level of analysis of privacy risk within federal agencies, their effectiveness varies depending on whether there is in-house privacy expertise and whether there are some delays in completing PIAs, especially when there are insufficient staff resources. Moreover, requiring a PIA to 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 seems that more often than not that they are compliance checks completed without a broader analysis of privacy risks.

In BC, the legislative mandate ensures a consideration of privacy issues within ministries that might not happen otherwise and the greatest benefits are achieved when the PIA is conducted early enough in the process. There are also benefits with having central agency experts review the PIAs, which is required by policy. On the other hand, there is the perception that the PIA process is a net drain on resources of little benefit for the creator or the regulator, despite many instances of the PIA resulting in positive changes to initiatives [58].

Although, there are no broad legislative mandates requiring PIAs in both Australia and NZ, there are narrow legislative requirements requiring PIAs for Information Matching in NZ and Data Matching programmes in Australia and the Office of the Victorian Privacy Commissioner has drawn attention to the risks inherent in legislatively mandated PIAs [47].

Upon analysis, legislative mandates for PIAs require a lot of work in their completion, which is work that typically can only be achieved through checklists whereby the organisation focus is on compliance rather than adopting a strategic approach and such forms do not require practitioners to ask the big policy questions, although accompanying guidance might suggest it. Moreover, it is common for organisations to be required to consider whether a PIA is needed, hence, in some jurisdictions, PIAs are regarded as an instrument of policy.

PIAs are considered *'mandated by policy'* where the policy is promulgated by a regulator with the authority to issue binding direction. The regulator can be a central agency charged with that authority under privacy legislation or an organisation with authority over administration and financial management or information technology under other legislation. For example, at the Canadian national government level, the Treasury Board policy requires departments and agencies to conduct of PIAs for proposals for all new programmes and services that raise privacy issues [38]. The policy applies to all government institutions listed in the Schedule to the *'Privacy Act'*, except the Bank of Canada. These include Departments and Ministries of State, as well as a range of government related institutions including the majority of the Crown Corporations (e.g. Canada Lands Company Limited, Canada Post Corporation, Telefilm Canada), federal agencies (e.g. Canadian Transportation Agency, Canada Revenue Agency) and other bodies funded by, or with boards wholly or partially appointed by, government (e.g. Canadian Wheat Board).

In the UK, the policy regarding government departments conducting PIAs, has been recently provided by the *'DHR'* report of January 2010, whereby the report obliges PIAs to be conducted on new projects or programmes involving significant amounts of personal data [51].

PIAs are only recommended if the organisation advocating their conduct does not have the authority to issue binding direction to the target organisations or if the wording is such that the conduct of a PIA is optional. In this respect, central agencies such as the Treasury Board of Canada usually have the authority to issue binding policy, but commonly, oversight bodies such as Privacy or Information Commissioners within jurisdictions such as NZ and Australia are only able to exhort or recommend that organisations conduct PIAs [4]. For example, the Privacy Commissioner of Hong Kong has had a history of suggesting that PIAs be undertaken for specific initiatives and has produced guidance that describes circumstances in which the Office recommends the completion of PIAs [55].

Analysis of the prescription levels suggests that in some cases, such as the Canadian province of Ontario, all three levels of prescription (as illustrated in Figure 2) exist with regard to different types of organisations or initiatives for conducting PIAs [58]. For example, the *'Personal Health Information Protection Act'* requires health information providers to perform PIAs and the policy suggests that organisations are required to conduct PIAs at the detailed design phase or when requesting funding approval for product acquisition or system development work. Furthermore, in August 2009 the Ontario's Privacy Commissioner expressed concerns about a new government plan to share biometric data (i.e. fingerprints) with Britain, Australia, US and New Zealand to combat immigration fraud and made several recommendations to the Immigration department regarding its PIA [33]. Thus, Ontario is at the intersection of all three prescription levels shown in Figure 2.

Similarly, there are some other cases at the intersection of different levels of prescription, such as the UK, which comes both under the 'recommended' and the 'policy' spheres shown in Figure 2. In the UK, a Cabinet Office report in 2010 [51], suggested that the Information Commissioners Office (ICO) had done significant work in promoting the use of PIAs across government through the provision of guidance and workshops and that currently 270 such assessments are now complete or underway across government departments or agencies. However, the report also obliges government departments to carry out PIAs on new projects or programmes involving significant amounts of personal data as part of its policy on PIAs.

Our analysis also identifies that organisations conduct PIAs in the absence of any level of prescription (e.g. self-regulation), but is based on their perception of the benefits. These motivations are typically more common in private sector organisations concerned about reputation.

6.23 Application of PIAs in the Private or Public Sector

In each of the jurisdictions under study, there is a longer history of regulation within organisations in the public sector than in the private sector. For example, in Canada, NZ, Australia and the US, public sector privacy legislation has generally predated that for the private sector. Therefore, most PIA requirements apply to public sector organisations such as government ministries or departments and types of public bodies or agencies. However, it is increasingly difficult to determine the limits of the public sector PIAs under current conditions. This is because many public agencies that are outside government ministries now have extensive experience with PIAs. This includes organisations in the health sector, higher education, and statistical agencies.

Although there is evidence that PIAs are conducted within the private sector (e.g. self-regulation), we do not know the extent of this in the absence of a mandate. Furthermore, private sector organisations have been mentioned by oversight bodies (e.g. Privacy Commissioners) and central agencies (e.g. Treasury Board of Canada) for conducting PIAs in high-risk situations or initiatives [4]. For example, PIAs are more likely to be carried out where: companies have high-profile privacy expertise in the form of Chief Privacy Officers; government schemes such as road pricing are being delivered; organizations have been the subject of public embarrassment, for example as a result of high-profile data breaches.

6.24 Conditions and Circumstances for Conduct of PIAs

Some jurisdictions have developed screening tools to help organisations determine if they should conduct a PIA or not for any given initiative, or to help them identify privacy issues that may require further analysis. Commonly, a screening exercise is conducted initially to determine if a PIA should be completed according to the rules or recommendations in the jurisdiction. This can be as simple as determining whether personal information is involved, or take the form of a structured instrument that poses a series of questions, as in NZ [25] and the UK [50]. In the US, the screening process is a form called a Privacy Threshold Analysis [57]. Those completing the form provide a variety of information about the system, answering specific questions tailored to their operational context, and the Privacy Office makes an assessment that determines whether or not a PIA is required [57]. In Canada, a Preliminary PIA (PPIA) is similar to a screening tool [38].

6.25 The Scale of the PIA Process

Generally, there are two different types of PIAs conducted in all jurisdictions, although the names and the processes vary. For example, names attributed to a short form of PIA are 'small-scale' (e.g.

UK), 'PPIA' (e.g. Canada) and 'Privacy Scan' or 'Privacy Impact Statement' in other jurisdictions. The short form of PIA is similar to a full-scale PIA, but is less formalised and requires less exhaustive information gathering and analysis, usually focusing on specific aspects of a project [50].

A full-scale PIA conducts a more in-depth internal assessment of privacy risks and liabilities. It analyses privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid such concerns. The process guidelines for a full-scale PIA tend to be more comprehensive and suggest the various stages of the process. For example in Australia, the process for conducting a PIA consists of five stages [56]:

- **Project Description**: this broadly describes the project, including the aims and whether any personal information will be handled.
- **Mapping the Information Flows**: this describes and maps the flows of personal information in projects.
- **Privacy Impact Analysis**: this identifies and analyses how the project impacts upon privacy.
- **Privacy Management**: this considers alternative options, particularly those which will improve privacy outcomes whilst still achieving the project's goal.
- **Recommendations**: this produces a final PIA report, which includes the above information and recommendations.

In the Canadian province of Ontario, the PIA process consists of three stages which are similar to those of Australia [59], as illustrated in Figure 3.

Conceptual Analysis	Data Flow Analysis	Follow-up Analysis
Prepare a plain language description of the scope and business rationale of proposed initiative Identify in a preliminary way potential privacy issues and risks, and key stakeholders Provide a detailed description of essential aspects of the proposal, including a policy analysis of major issues Document the major flows of personal information Compile an environment issues scan to review how other jurisdictions handled a similar initiative Identify stakeholder issues and concerns Assessment of public reaction	Analyse data flows through business process diagrams, and identify specific personal data elements or clusters of data Assess proposal's compliance with FOI and privacy legislation, relevant programme statutes, and broader conformity with general privacy principles Analyse risk based on the privacy analysis of the initiative, and identify possible solutions Review design options, and identify outstanding privacy issues/concerns that have not been addressed Prepare response for unresolved privacy issues	Review and analyse physical hardware and system design of proposed initiative to ensure compliance with privacy design requirements Provide a final review of the proposed initiative Conduct a privacy and risk analysis of any *new changes* to the proposed initiative relating to hardware and software design to ensure compliance with FOI and privacy legislation, relevant programme statutes, and broader conformity with general privacy principles Prepare a communications plan

Fig. 3. Ontario PIA Process

In the UK, the processes involved in conducting a PIA are again similar to PIAs conducted in other jurisdictions and consist of the following [50]:

- **Initial Assessment**: this examines the project at an early stage, identifies stakeholders, assesses privacy risks and decides whether a PIA is necessary or not and if so, what level of PIA is required.
- **Small-Scale PIA**: this is less formalised and requires less exhaustive information gathering and analysis and usually focuses on specific aspects of a project.
- **Full-Scale PIA**: this consists of five phases that are usually conducted in sequence and include the following:
    - **Preliminary:** establishes and ensures a firm basis for the PIA, so that it can be conducted effectively and efficiently.
    - **Preparation:** makes the arrangements needed to enable the following phase (i.e. consultation and analysis) to run smoothly.
    - **Consultation and Analysis:** identifies problems early on, discovers effective solutions, and ensures that the design is adapted to include those solutions.
    - **Documentation:** documents the PIA process and the outcomes and delivers a PIA report.
    - **Review and Audit:** ensures that the undertakings arising from the consultation and analysis phase are actually within the running system or implemented project.
- **Privacy Law Compliance Check:** this check examines compliance with statutory powers, duties and prohibitions in relation to the use and disclosure of personal information
- **Data Protection Compliance Check**: this checks for compliance with the Data Protection Act of 1998. An organisation usually conducts this check when the project is more fully formed.

6.26 Who Conducts PIAs

PIAs are usually completed by a senior analyst or a manager with ongoing programme administration responsibilities. The various guidance material suggests a team or committee approach and stipulates what types of expertise should be drawn in to the PIA. This can include, with varying degrees of participation, the following personnel [50]:

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

In Hong Kong, the guidance material suggests that there are distinct advantages in outsourcing a PIA, which lends impartiality to the process [55].

6.27 Comparison of PIAs with Other Business Processes

A PIA is different and distinguished from other business processes, such as privacy audits, or privacy law compliance checking [4]. A privacy audit is valuable in that it confirms that privacy

undertakings or privacy law is being complied with, or highlights problems that need to be addressed. To the extent that it uncovers problems, however, they are likely to be expensive to address and may disturb the conduct of the organisations business. A privacy compliance check focuses on laws which affect privacy, such as the *'Data Protection Act'* (1998) and the *'Privacy and Electronic Communications Regulations'* (2003) amongst others and ensures that the project is legally compliant. Although these processes are part of the PIA process in some jurisdictions, Warren et al (2009) [52], suggests that privacy audits and compliance checks are conducted at the end of the project as an entirely separate activity to the PIA itself. This is because these processes apply to existing projects in order to ensure their continuing conformity with internal rules and external requirements.

6.28 End Results of an Effective PIA

Ideally, the results of an effective PIA should include the identification of the project's privacy impacts, and the appreciation of those impacts from the perspectives of all stakeholders. The result should also provide an understanding of the acceptability of the project and its features by the organisation and people that will be affected by it. It should produce an identification and assessment of less privacy-invasive alternatives, and identify the ways to avoid the negative impacts on privacy and show other ways to lessen those negative impacts. Where negative impacts on privacy are unavoidable, the PIA should provide justification and clarification for them in relation to the business needs. Important deliverables of the results include documentation (e.g. PIA Report) and publication (e.g. Internet Website) of the outcomes. In practice, the end results of a PIA may not meet all of these goals.

The analysis of PIAs within the jurisdictions studied has shown that there are some commonalities and differences between the processes, policies and application of PIAs contained within the various guidance materials. However, throughout the various guidance materials available there is no suggestion of how the future development of PIAs should proceed; therefore in the next section we will discuss the future development of PIAs.

7 Future PIAs

In this section, we consider how PIAs may change over time, focusing on the usage of automated decision support systems and the increase of cross border (jurisdictional) PIAs. This is a brief summary as we will be providing a more detailed analysis of these aspects in a separate report.

7.1 Automated Decision Support Systems

Usage of automated systems to support PIAs is a very new field and there are not many such systems available. A few initial tools in the PIA space have been available, largely being the screening tools already considered in section 6.24. These were in the main based on a simple 'decision tree'-type approach. However, very recently there has been a step change in approach: one research area that is making significant advances is the support of PIAs using automated Decision Support Systems (DSS) (such as privacy expert systems). Typically, a DSS has a knowledgebase (KB) that needs to be created and updated periodically by experts on an ongoing basis and a rules engine for which rules are defined that automatically generate an output report based upon user input. Within this context, we will discuss briefly two DSSs that are at the cutting edge of research.

PRAIS is a research project that has developed a prototype DSS tool for context-sensitive privacy-aware information sharing in children's social care [60]. The DSS is based on the architecture developed for the Identity Governance Framework (IGF) [61]. Information sharing is based on a pull model: this means that the recipients are alerted that information is being made

available to them, after which it is retrieved from the source. At first, this may seem counterintuitive but the IGF architecture supports this design choice because it allows the owner of the information to retain liability for the data and to audit each use. However, the scope of PRAIS is very narrow as it is not intended that the DSS will ever make decisions on behalf of properly trained personnel but instead will assist social care practitioners in making privacy-aware decisions where required.

Hewlett Packard's Privacy Advisor (HPPA) is an expert system that captures data about business processes to determine their privacy compliance [62, 63]. The tool helps organisations to ensure privacy concerns are met and supports enterprise accountability, supplying employees with sufficient information and guidance to ensure that they design and conduct their projects in compliance with organisational privacy policies. HPPA uses a rules engine for which rules are defined that are used both to generate questions that are customised to the employee's specific situation and also to codify HP's privacy rulebook and other information sources. Based on the employee's response to these questions, it automatically generates an output report that includes an analysis of possible privacy risks and a checklist of actions that the employee should take in order to mitigate these risks. This tool is being rolled out to employees within HP throughout 2010.

7.2 Cross Border PIAs

Compliance with national and regional privacy legislation, policy and regulations is complex and evolving. Every problem is therefore, compounded exponentially on a local level when private information is collected, used or shared across jurisdictions. For example, when a Canadian uses a credit card with a US travel agent to book a cruise from the UK to Australia on a NZ ship, the distribution of private information goes to multiple jurisdictions over systems that may reside in even more countries. What data are private, who has those data and what laws and regulations may apply are by no means clear. Privacy risks may flow from any of a number of sources, including system characteristics, technical architecture and program design.

The purpose of a 'cross-border PIA' is to identify, review and adequately address privacy issues and to provide documented assurance. A critical part of this is the analysis of the data flows of personally identifiable information associated with cross-border operations and systems. This can be done at a number of levels. On one level, transborder data flow legislation can be encoded and incorporated into decision-making about whether certain actions are compliant with legal or corporate policy, for example as was done with [62, 63]. Alternatively, this analysis could be carried out in a data-centric way, such that the cross-border PIA would identify and track all personally identifiable information from the point of collection, through all use and distribution, to the point where the information is destroyed. The wide variety of operations, systems and jurisdictions that may be involved precludes any detailed discussion here, but it is important to understand that the identification and documentation of data flows must be done prior to conducting a PIA. This will require documentation of the flow of personally identifiable information throughout the business process, which will require separate consideration of business process diagram documents and data flow tables [64]. Moreover, a cross-border PIA requires teams from each jurisdiction and access provided to external expertise when necessary. In its fullest form, that can be a very complicated undertaking, and hence is only likely to take place for business processes where there is high privacy risk and strong regulatory pressure for such a PIA.

8 Conclusions

This paper has carried out an assessment of the different types of PIAs that have been carried out around the world. We have found that a PIA is a process to help determine whether technologies,

information systems and proposed programs or policies meet privacy requirements. It measures both technical compliance with privacy legislation and the broader privacy implications of a given proposal, project or product. Moreover, it is a tool to generate and communicate confidence that organisational privacy objectives have been defined and addressed and the use of a PIA can promote a more fully informed policy decision-making process for operations and system design choices.

Although there are many differences between PIAs within jurisdictions, we found that a common basis for them can be described and in the coming years it is anticipated that a variety of systems will be developed to help organisations conduct and support PIAs, particularly in the refinement of this approach including greater usage of automated technologies.

Our analysis of PIAs suggests that increases in specific trends are likely to happen within jurisdictions in the future including: the enactment of specific legislation or policies that mandate the use of PIAs for projects that contain significant amounts of personal data; an increase in the number of PIAs being conducted especially in relation to new and emerging technologies (such as cloud computing services, social networking technologies, federated identity management solutions, products using Radio Frequency Identifiers (RFID), etc.). It is also anticipated that private organisations will conduct PIAs more often due to increasing regulatory pressure and to protect their reputations and that cross-border PIAs will be further developed.

Time will tell if PIAs achieve their aims of identifying and resolving privacy issues and risks. However, without PIAs it will be difficult for organisations to achieve an appropriate balance between conflicting privacy issues and interests, and in particular to avoid subsequent serious harm (especially resulting from distrust from the public, consumers or government agencies) and balance this against the return of investment spent on business technologies.

9 References

[1] R. Clarke. (2009, April). “Privacy impact assessment: its origin and development.” *Computer Law & Security Review.* [Online] 25 (2), pp. 123-135. Available: http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VB3-4W04B2D-4&_user=121739&_coverDate=12%2F31%2F2009&_rdoc=1&_fmt=high&_orig=search&_sort=d&_docanchor=&view=c&_searchStrId=1187574478&_rerunOrigin=scholar.google&_acct=C000010018&_version=1&_urlVersion=0&_userid=121739&md5=95d751f134a0fcd2c1c94abbfff93f0b, [Oct. 4, 2009].

[2] B. Stewart. (1996, July). “Privacy Impact Assessments.” *Privacy Law & Policy Reporter.* [Online] 3(7), pp 61-64. Available: http://www.austii.edu/au/journals/PLPR/39.html, [Oct. 26, 2009].

[3] R. Clarke. “Privacy Impact Assessments.” Internet: http://www.rogerclarke.com/DV/PIA.html, May. 26, 2003 [Oct. 28, 2009].

[4] C. Bennett. R. Bayley. A. Charlesworth. R. Clarke. “Privacy Impact Assessments: International study of their application and effects.” Internet: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/privacy_impact_assessment_international_study.011007.pdf#13, Oct. 2007 [Oct. 27, 2009].

[5] J. DeCew. “Privacy.” Internet: http://plato.stanford.edu/enties/privacy/, Sept. 18, 2006 [Nov. 26, 2009].

[6] C. Bennett. C. Raab. *"The governance of privacy: policy instruments in global perspective."* Cambridge, MA: Massachusetts Institute of Technology, 2006, pp 3-22.

[7] D. Solove. *"Understanding Privacy."* Cambridge Massachusetts: Harvard University Press, 2008, pp 1-18.

[8] I. Lloyd. *"Information technology law."* Oxford: Oxford University Press, 2008, pp 119-150.

[9] Europa. “The European Parliament and the Treaty of Lisbon.” Internet: http://europa.eu/lisbon_treaty/index_en.htm, Dec 3, 2009 [Dec. 5, 2009].

[10] R. Clarke. “What is Privacy?” Internet: http://www.rogerclarke.com/DV/Privacy.html, Aug. 7, 2006 [Nov. 22, 2009].
[11] W. Huitt. “Maslow’s Hierarchy of Needs.” Internet: http://www.edpsycinteractive.org/topics/regsys/maslow.html, July 2007 [Nov. 21, 2009].
[12] BBC News. “Body scanners risk right to privacy, says UK watchdog.” Internet: http://news.bbc.co.uk/1/hi/uk/8464266.stm, Jan. 17, 2010 [Jan. 18, 2010].
[13] H. Nissenbaum. *"Privacy in Context: Technology, Policy, and the Integrity of Social Life."* Stanford California. Stanford University Press, 2009, pp 1-20.
[14] P. Leith. (November, 2009) "The Socio-Legal Context of Privacy." *International Journal of Law in Context.* [Online] 2 (2), pp 105-136. Available: http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=547660, [Apr. 24, 2010].
[15] European Parliamentary Technology Assessment. (2009, March) *“What is a Technology Assessment.”* [Online]. http://www.eptanetwork.org/EPTA/what.php, [Nov. 30, 2009].
[16] M. Barrett. (2003, June). “Environmental impact statement.” *Omega.* [Online]. 7 (5), pp. 431-439. Available: http://www.sciencedirect.com/science/article/B6VC4-48TTM96-5J/2/773df09b6a1d2455faeca8d67d622776, [Nov. 28, 2009].
[17] Justia. “Robertson v. Methow Valley Citizens, 490 U.S. 332 (1989).” Internet: http://supreme.justia.com/us/490/332/case.html, June. 06, 2009 [Nov. 30, 2009].
[18] International Association for Impact Assessment. . “Principles of Environmental Impact Assessment Best Practice.” Internet: http://www.iaia.org/publicdocuments/specialpublications/Principles%20of%20IA_web.pdf, Jan. 1999 [Dec. 1, 2009].
[19] G. Beanlands. *“Environmental Impact Assessment: Theory and Practice”*, 5th ed, P.Wathern Ed, Great Britain, Routledge, 2004, pp 31-85.
[20] T. Dixon. (1997, January). “Communication Law Centre wants IPPs revised in line with Australian Privacy Charter.” *Privacy Law & Policy Reporter.* [Online]. 3(9), reference 5. Available: http://www.austlii.edu.au/au/journals/PLPR/1997/4.html, [Dec. 16, 2009].
[21] B. Stewart. (1996, June). “PIAs – an early warning system.” *Privacy Law & Policy Reporter.* [Online]. 3 (7), pp. 45-49 Available: http://www.austlii.edu.au/au/journals/PLPR/1996/65.html, [Oct. 26, 2009].
[22] Consulting House. “IRS Privacy Impact Assessment: Version 1.3.” Internet: http://www.consultinghouse.net/attach/tbbbsd010%5Cyjh90_2004316171239.pdf, Dec. 16, 1996 [Oct. 25, 2009].
[23] HEW. “Records, Computers and the Rights of Citizens.” Internet: http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm, July. 1973 [Oct. 31,2009].
[24] R. Clarke. “A History of Privacy impact Assessments.” Internet: http://www.rogerclarke.com/DV/PIAHist.html, February, 2004. [Oct. 28, 2009].
[25] D. Linowes. “Personal Privacy in an Information Society.” Internet http://aspe.hhs.gov/datacncl/1977privacy/preface.htm, July 1997 [Oct. 30, 2009].
[26] Commonwealth Consolidated Acts. “Data-Matching Program (Assistance and Tax) Act.” Internet: http://www.austlii.edu.au/au/legis/cth/consol_act/dpata1990349/index.html, 2000 [Nov. 17, 2009].
[27] R. Clarke. “A Normative Regulatory Framework For Computer Matching.” Internet: http://www.rogerclarke.com/DV/MatchFrame.html, Feb. 3, 1994 [Nov. 17, 2009].
[28] D. H. Flaherty. *“Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States.”* Chapel Hill; London: University of North Carolina Press, 1989.

[29] A. Charlesworth. (2007, Oct). "Broad Jurisdictional Report for the European Union." *Privacy Impact Assessments: International study of their application and effects.* [Online]. Appendix H, pp. 3-4. Available: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/privacy_impact_assessment_international_study.011007.pdf#13, [Oct. 27, 2009].
[30] Inland Revenue Service. "Privacy Impact Assessments." Internet: http://www.irs.gov/privacy/article/0,,id=122989,00.html, Jan. 28, 2010 [Jan. 29, 2010].
[31] The Office of the Chief Information and Privacy Officer. "Privacy Impact Assessment Guidelines: Part Five – Linkage to government management processes." Internet: http://www.accessandprivacy.gov.on.ca/english/pia/pia5.html, Aug. 12, 2009 [Nov. 22, 2009].
[32] The Office of the Chief Information and Privacy Officer. " Privacy Impact Assessment Guidelines: Part One – Privacy Impact Assessments: An Overview." Internet: http://www.accessandprivacy.gov.on.ca/english/pia/pia1.html, Aug. 12, 2009 [Nov. 22, 2009].
[33] M. Blanchfield. "Canada Plans to Share Fingerprint database with UK; Australia." Internet: http://www.windsorstar.com/Canada+plans+share+fingerprint+database+with+Australia/1917825/story.html, Aug. 21, 2009 [Oct. 29, 2009].
[34] D. H. Flaherty. "An investigation concerning the disclosure of personal information through public property registries." Internet: http://www.oipcbc.org/investigations/reports/invrpt11.html, Mar. 31, 1998 [Nov. 22, 2009].
[35] Services Alberta. "Privacy Compliance: Privacy Impact Assessments." Internet: http://foip.gov.ab.ca/resources/guidelinespractices/chapter9.cfm#9.3, Sept. 25, 2005 [Oct. 31, 2009].
[36] S. Bloomfield. "The Role of the Privacy Impact Assessment: Managing Government Information 2nd Annual Forum." Internet: http://www.priv.gc.ca/speech/2004/sp-d_040310_e.cfm, Mar. 10, 2004 [Dec. 10, 2009].
[37] Treasury Board of Canada Secretariat. "Privacy Impact Assessment Policy. " Internet: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450&section=text, May. 2, 2000 [Nov. 15, 2009].
[38] Treasury Board of Canada Secretariat. "Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks." Internet: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp, Sept. 11, 2009 [Nov. 19, 2009].
[39] The Office of the Privacy Commissioner of Canada. "Assessing the Privacy Impacts of Programs, Plans, and Policies." Internet: http://www.priv.gc.ca/information/pub/ar-vr/pia_200710_e.cfm, October 2007 [Nov. 17, 2009].
[40] The Office of the Privacy Commissioner of Canada. "OPCC letter in response to the Privacy Impact Assessment (PIA) completed by the Canadian Air Transport Security Authority (CATSA) in anticipation of the deployment of millimeter wave (MMW) screening technology at selected Canadian airports." Internet: http://www.priv.gc.ca/pia-efvp/let_20100108_e.cfm, Oct. 29, 2009 [Nov. 25, 2009].
[41] B. Stewart. (1999, June). "Privacy impact assessment towards a better informed process for evaluating privacy issues arising from new technologies." *Privacy Law & Policy Reporter.* [Online]. PLPR 8 Available: http://www.austlii.edu.au/au/journals/PLPR/1999/8.html, [Nov. 26, 2009].
[42] B. Stewart. "PIA: Some approaches, issues, and examples." Internet: http://www.pco.org.hk/misc/stewart_color.ppt, March 2001 [Nov. 25, 2009].
[43] B. Stewart. "Privacy impact assessment roundup." *Privacy Law & Policy Reporter.* [Online].PLPR 41 . Available: http://www.austlii.edu.au/au/journals/PLPR/2002/41.html, 2002 [Nov. 19, 2009].
[44] Privacy Commissioner of New Zealand. "Data Matching: Overview." Internet: http://www.privacy.org.nz/overview-2/, Sept. 2009 [Oct. 25, 2009].

[45] The Office of the Privacy Commissioner of New Zealand. “Privacy Impact Assessment Handbook.” Internet: http://www.privacy.org.nz/library/privacy-impact-assessment-handbook, July. 2004 [Oct. 30, 2009].
[46] C. Bennett. (2007, Oct). “Jurisdictional Report for the United States of America.” *Privacy Impact Assessments: International study of their application and effects.* [Online]. Appendix D, pp. 3-4. Available; http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_appd_us_2910071.pdf, [Oct. 28, 2009].
[47] The Office of the Victorian Privacy Commissioner. “Privacy Impact Assessments: A guide for the Victorian Public Sector.” Internet: http://www.privacy.vic.gov.au/privacy/web.nsf/download/B595F5F2FDFD2135CA2575AC0012BC0E/$FILE/OVPC%20Privacy%20Impact%20Assessment%20Guide%20Edition%202%20May%202009.pdf, Apr. 27, 2009 [Oct. 30, 2009].
[48] Data Protection Commissioner of Ireland. “Biometrics in the workplace.” Internet: http://www.dataprotection.ie/docs/Biometrics_in_the_workplace./244.htm, November 2009 [Nov. 24, 2009].
[49] House of Commons Hansard Written Answers. “Privacy: Impact Assessments.” Internet: http://www.parliament.the-stationery-office.co.uk/pa/cm200809/cmhansrd/cm090424/text/90424w0017.htm, June. 15, 2009 [Oct. 29, 2009].
[50] Information Commissioners Office. “Privacy Impact Assessment Handbook.” Internet: http://www.ico.gov.uk/handbook/, June. 2009 [Oct. 29, 2009].
[51] Cabinet Office. “Protection Information in Government.” Internet: http://www.cabinetoffice.gov.uk/media/328380/protecting-information.pdf, Jan. 10,2010 [Feb. 25, 2010].
[52] A. Warren. R. Bayley. A. Charlesworth. C. Bennett. R. Clarke. C. Oppenheim. (2008, March). “Privacy Impact Assessments: International experience as a basis for UK guidance.” *Computer Law and Security Report.* [Online]. 24 (3), pp. 233-242. Available: http://hdl.handle.net/2134/4481, [Nov. 3, 2009].
[53] National Policing Improvement Agency. “Police National Database – Privacy Impact Assessment Report.” Internet: http://www.npia.police.uk/en/docs/IMPACT_PND_Privacy_Impact_Assessment.pdf, April. 2008 [Oct. 29, 2009].
[54] UK Border Agency. “Report of a Privacy Impact Assessment conducted by the UK Border Agency in relation to the High Value Data Sharing Protocol amongst the immigration authorities of the Five Country Conference.” Internet: http://www.bia.homeoffice.goc.uk/sitecontent/documents/managingourborders/strengthening/pia-data-sharing-fcc.pdf, Aug. 21, 2009 [Oct. 29, 2009].
[55] R. Woo. “Impact of Technology on Data Privacy.” Internet: http://www.pcpd.org.hk/english/files/infocentre/speech_20080926.pdf, Sept. 26, 2008 [Oct. 30, 2009].
[56] Australian Government: Office of the Privacy Commissioner. “Privacy Impact Assessment Guide.” Internet: http://www.privacy.gov.au/materials/types/download/9349/6590, August 2006 [Oct. 30, 2009].
[57] United States of America Department of Homeland Security. “Privacy Impact Assessments: Official Guidance.” Internet: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf, May 2007 [Nov. 6, 2009].
[58] A. Charlesworth. (2007, Oct). “Jurisdictional Report for Canada.” *Privacy Impact Assessments: International study of their application and effects.* [Online]. Appendix C, pp.5-

6. Available http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_appc_can_2910071.pdf, [Oct. 30, 2009].

[59] Information and Privacy Office of Ontario. "Privacy Impact Assessment: A Users Guide." Internet: http://accessandprivacy.gov.on.ca/english/pia1.pdf, June 2001 [Nov. 25, 2009].

[60] R. Harbird. . M. Ahmed. A. Finkelstein. E. McKinney. A. Burroughs. "Privacy Impact Assessment with PRAIS." Internet: http://www.cs.ucl.ac.uk/staff/A.Finkelstein/papers/hotpets.pdf, February 2007 [Nov. 15, 2009].

[61] Liberty Alliance Project. "ID governance – identify privacy and access policy, marketing requirements document." Internet: http://www.projectliberty.org/, 2007 [Nov. 16, 2009].

[62] S. Pearson. T. Sander. R. Sharma. "Privacy Management for Global Organisations." *Data Privacy Management and Autonomous Spontaneous Security*. LNCS 5939, pp. 9-17. Available: http://www.springerlink.com/content/a13142g81255p453/fulltext.pdf?page=1, March 2010 [March. 28, 2010].

[63] S. Pearson. P. Rao. T. Sander. A. Parry. A. Paull. S. Patruni. V. Dandamudi-Ratnakar. P. Sharma. "Scalable, Accountable Privacy Management for Large Organizations." *INSPEC 2009: 2nd International Workshop on Security and Privacy Distributed Computing, Enterprise Distributed Object Conference Workshops (EDOCW 2009), IEEE*. pp, 168-175, September 2009 [Nov. 7, 2009].

[64] T. Karol. (June, 2001). "Cross-Border Privacy Impact Assessments: An Introduction." ." *Information Systems Control Journal*. [Online]. Volume 3. Available: http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17226&TEMPLATE=/ContentManagement/ContentDisplay.cfm, [Nov. 6, 2009].