Challenges to Managing Privacy Impact Assessment of Personally Identifiable Data

Cyril Onwubiko
Intelligence and Security Assurance, E-Security Group, Research Series Limited, London, UK

ABSTRACT

The challenges organisations face in managing privacy risks are numerous, and inherently diverse. Traditionally, organisations focused on addressing business and security requirements of a project, but most recently, privacy impact assessment has become an essential part of the risk management regime for most projects. Significant efforts are now directed toward providing appropriate guidance on how to conduct privacy impact assessments. Appropriate assessments of privacy invasive technologies, justification for project, collection and handling of personally identifiable data and compliance to privacy legislations possess enormous challenges to carrying out appropriate privacy impact assessments. In this chapter, guidance on how to assess privacy risks of both new and in-service projects is provided. Further, lessons learned from managing privacy risks of new and in-service projects resulting from aggregation, collection, sharing, handling and transportation of personally identifiable information are discussed.

INTRODUCTION

Today's information and communication systems are complex. They span across enterprise boundaries, and use technologies that traverse geographic boundaries, for example, cloud computing. These networks also use a plethora of technologies and software to implement complex business logics, some of which are inherently privacy-invasive, such as location-based technologies, smart cards, radio frequency identification (RFID) tags, and biometrics. While these technologies are exciting to use, they pose significant privacy risks.

Traditionally, risk assessments of projects are carried out primarily on the basis of business and security requirements. Most recently, privacy impact assessment (PIA) has been recommended as an essential project initiation process [1] to assess privacy risks associated with new and existing projects. Privacy impact assessment is used to assess privacy risks that may be associated with a project and to ensure that privacy legislations are not breached, and sensitive personal identifiable data (PID) are not compromised too. Privacy risk assessment is an assessment of risks associated with - failing to comply with state or federal privacy legislation - protecting personal information data of individuals, and satisfying privacy requirements of information systems, that may need to be redesigned or retro-fitted at considerable expense [2]. This means that privacy risk assessment should be carried out on all projects to ensure that:

1) they comply with privacy legislations or regulations;
2) they provide adequate safeguards to manage, handle, share, store or transport sensitive personal data or personally identifiable information (PII), and
3) finally, they comply with project-specific information systems' privacy requirements.

Managing privacy risks can be challenging, not because of the numerous issues of concern, but also because each project is unique and utilizes fundamentally different technologies and mechanisms to deliver its own service. While the steps involved in carrying out privacy impact assessment are the same for any project, but each assessment of privacy for any project is different.

A project in this chapter refers to a system, programme or scheme. A project may involve a collection of systems that are used to deliver service for a specific purpose. For example, a census programme is a project whose aim is to count the number of lawful citizens, by checking and verifying their name, age, address and social or religious inclination, of a particular nation. This project may require the use of information communications technology (ICT) systems, people, electronic and manual processes. Another example, EINSTEIN 2 [3] is a United States project for intrusion detection system that monitors the network gateways of government departments and agencies in the United States for unauthorized traffic. This project invloves the use of ICT systems, people and both electronic and manual processes to monitor and collect traffic information. An in-service (existing) project is a programme of work that is already been delivered and in operational use. A new project is a programme of work that is in the initiation stage of the project lifecycle.

There are a good number of guidelines for conducting privacy impact assessments as demonstrated by [1, 2, 7, 4, 5, 6]; unfortunately, organizations still face difficulty assessing privacy risks associated to new and existing projects. Some of most of the common challenges faced by organization are as follows:

1) How to assess appropriately privacy invasive technologies;
2) Justification for project;
3) Difficulty finding privacy experts within own organization;
4) Lack of prescriptive guideline on how to assess privacy risks associated to a project, and how to determine the level of privacy assessments required for a particular project.

In addition, how to appropriately gather and handle personal information data and compliance to privacy regulations and legislations are other challenges associated to conducting privacy impact assessments.

In this chapter, guidance on how to assess privacy risks of both new and in-service projects is provided. Further, lessons learned from managing privacy risks for new and existing projects resulting from collection, aggregation, sharing, handling and transportation of sensitive personal information are discussed.

PRIVACY IMPACT ASSESSMENT

Privacy impact assessment is an assessment of privacy related risks comprising of four distinct assessments:

1. Assessment of the project's characteristics or features such as technologies or mechanisms deployed or intended of use. This assessment is to check if the technologies or mechanisms would be privacy invasive.
2. Assessment of the project's compliance with privacy regulations, state, federal, national, bilateral or multilateral privacy legislations. This relates to compliance with privacy regulations and legislations, especially those that operate where the project is located or situated. For example, the Data Protection Act 1998 in the UK or the 'the Privacy Act' in the US, or other privacy related pieces of legislations in other parts of the world, such as Canada, Australia and Germany.
3. Assessment of personal information data being processed, or to be processed by the project. For example, is personal information data collected identifiable or not; are they sensitive personal data; are they 'obsolete' personal identifiable data etc.
4. Finally, it is an assessment of the collection, sharing, distribution, storage and transportation of personal information data, and whether the processing of personal information is in line with privacy legislations. It is important to mention that PIA is not only applied to a project, but also applied to a workstream, programme, task, policy, procedure, platform or ICT System.

According to NIST's ITL Security Bulletin 2010 [7] Personally Identifiable Information (PII) or Personal Identifiable Data (PID) is any information about an individual that is maintained by an agency, including information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (based on General Accountability Office and Office of Management and Budget definitions). A list of personally identifiable information is provided in Table 1.

Table 1: Personal Identifiers

S/N	Personal Identifiers	S/N	Personal Identifiers
1	Names (firstname, surname or lastname)	12	Biometric identifiers such as fingerprints, voice prints etc
2	Addresses (home, business or both)	13	Bank, Financial or Credit card details
3	Post code or Zip code	14	Mother's maiden name
4	Email address	15	Tax, Benefit or Pension records or Record numbers
5	Telephone numbers (Fax numbers)	16	Employment records
6	Driving license number	17	School attendance or records
7	Date of birth	18	Vehicle identifiers and serial numbers including license plate numbers
8	Social insurance number / National insurance number	19	Web universal resource locators (URLs)
9	Medical record numbers / Health records	20	Internet protocol (IP) address numbers
10	DNA data	21	Full face photographic images and any comparable images
11	Any other materials relating to social services including child protection and housing	22	Any other unique identifying number, characteristic, or code.

Personal identifiers (shown in Table 1) comprise of both personal information that are in the public domain and sensitive personal data that when released is likely to cause harm or distress to the individual. These identifiers are derived from a couple of standards – HIPAA [8] and HMG IA Standard No. 6 [9]

It is pertinent to mention that compliance with privacy legislation is dependent on where the project that is being assessed is located. For example, a project in the UK would have to comply with the UK privacy legislations and the wider European Union privacy legislations, and may comply with other privacy legislations of other countries if the organisation wishes to do so.

There are also bilateral and multilateral privacy legislations, such as the Safe Harbor Act (Directive 95/46/EC), which regulates the processing of personal data within the European Union in addition to Directive 2002/58/EC that protects privacy of electronic communications [10]. Directive 95/46/EC is also available not only to EU member state (nations), but also, available to other countries outside the EU, which the United States (US) signed up to. Organization operating within bilateral or multilateral privacy legislation should comply with those pieces of privacy legislations. This means that a privacy impact assessment of a project operating in bilateral or multilateral privacy legislation must be equally assessed within the confinements of those bilateral or multilateral privacy agreements, and other specific privacy legislation of its own country. For example, privacy legislation compliance for a privacy impact assessment of a project in the UK would involve assessment of the project's compliance to both UK-specific privacy legislations and EU related privacy legislations.

Privacy impact assessment may seem onerous at times due to the numerous steps involved when carrying out PIA. Depending on the nature of the project, extensive privacy impact assessment maybe required. The UK Information Commissioner's Office (ICO) through its Privacy Impact Assessment Handbook [1] provides useful guidelines. The handbook offers a general purpose framework for carrying out privacy impact assessment.

Our contribution in this chapter is rather unique and much more focused on providing a practical approach to conducting privacy impact assessment that is general-purpose and prescriptive. The usefulness of our contribution can be seen in both the guidelines provided with respect to our Privacy Impact Suitability Assessment (PISA) Framework (see Figure 1) and Privacy Screening Framework (see Table 4).

In the private sector, for example, privacy impact assessments of projects are not as mandated as it is in the public or government sector. While, PIA may be conducted for certain projects based on best endeavours in the private sector, it is mandatory for all government and public sector projects as an essential risk management activity.

For example, the Department of Homeland Security, National Cyber Security Division of the United States conducted privacy impact assessment of its EINSTEIN 2 Program in 2008 to examine its privacy implications with collecting, analyzing and sharing of Computer Security Information across the Federal Civilian Government [11]. According to the United States Computer Emergency Readiness Team (US-CERT), the Department of Homeland Security (DHS) must provide this publicly available PIA prior to initiating a new collection of information that uses information technology to collect, maintain or disseminate information that is in an identifiable form or collects identifiable information through the use of information technology as mandated by the US, E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. § 3501, note), Section 208. Similarly, in the UK, the Information Commissioners Office (ICO), Cabinet Office has recommended privacy impact assessment for all projects, new and existing, whose functionality may require the collection, sharing or use of personal information. This was driven from the UK Data Handling Review of 2008 [12].

PRIVACY IMPACT SUITABILITY ASSESSMENT (PISA) FRAMEWORK

The privacy impact suitability assessment framework is our proposed framework for assessing a project's suitability for PIA assessment (see Figure 1).

The PISA framework is a seven (7) step privacy assessment model, which aims to evaluate if a project is required to undergo PIA or not; and to determine the level of PIA required, where applicable. The first step (indicated by the small circle on each object) is the start of the PIA assessment. The second step is the scene setting assessment (a.k.a. stage 1 PIA). At this stage, the project is initially assessed as to whether personal information data will be processed by the project. For existing projects, the scene setting assessment will check if information being processed by the project involves personal information data. The third step is when a decision is reached whether the project should or should not undergo a stage 2 PIA assessment. If the outcome shows that personal information data is not being or will not be processed, then PIA is completed (step 7) and that concludes privacy impact assessment for that project. If otherwise, then the fourth step begins. The fourth step is the stage 2 PIA.

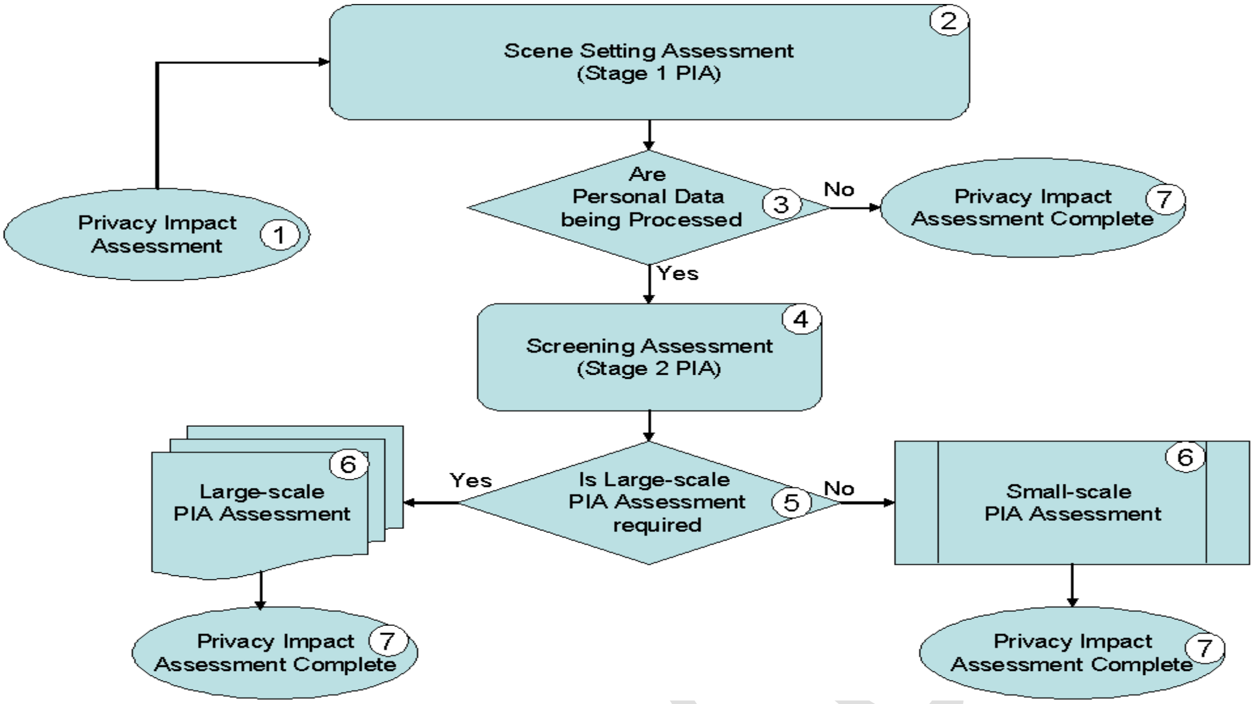

Figure 1: PISA Framework – Privacy Impact Suitability Assessment Framework

The second stage PIA (Stage 2 PIA) starts with the screening exercise when privacy risks of the project are assessed in much more detail than stage 1. This involves assessing the project's characteristics, such as technologies or mechanisms that will be deployed in the project, for example, checking if such technologies are privacy invasive. It also assesses the type of personal data that will be collected, and to ensure the people providing these data are aware and willing. In addition, it assesses if there is good justification for the project. The fifth step is when a decision is reached as to whether small-scale PIA or large-scale PIA is pertinent for the project. The sixth step involves carrying out large-scale or small-scale PIA, and finally, the seventh step completes the assessment. Since every project should be assessed of privacy risk, we thought the framework is a foundational contribution, which assist privacy experts and organization conduct, in a practical way, a privacy assessment of their projects.

Scene Setting Assessment (Stage 1 PIA)

The scene setting assessment (SSA) is the first stage PIA of a project. It is aimed to ascertain if the project will process personal information data, or already processes personal information data. This is applicable to existing project (see Figure 1). To conduct a scene setting PIA assessment of a project, we have designed ten (10) fundamental scene setting questions to help with the assessment in order to deduce the suitability or appropriateness of privacy impact assessment of the project, as shown in Table 2.

Table 2: Privacy Impact Assessment Questions

S/N	Questions
1	Would the workstream, project or ICT system consume, process, transport or store personal information data?
2	What personal information will be processed (collect, share, transport or store) by the project?
3	Why is personal information being collected by the project?

4	What is the intended use of personal information being collected?
5	How would these information be processed, this includes sharing, transporting, exchanging, storing and disposing of personal information?
6	Who are the intended recipient (information controllers), and with whom will personal information be shared, or/and exchanged?
7	How would the project seek to obtain consent from their service consumers (users of the system) with regards to collection of their personal information data?
8	How would service consumer be informed of the justification of the project?
9	How would the information collected be secured?
10	What privacy regulation and legislation apply or required?

Based on the outcome of this assessment (answers to questions on Table 2), a decision should be made, either to proceed, or stop further privacy impact assessment. If it is believed that the project will be used to process personal information data, then further PIA assessments are recommended, otherwise this concludes PIA assessment of the project. Suppose the outcome of the scene setting assessment turns out that the project is handling personal information data. This implies that a second stage PIA (screening assessment), which is a much more thorough assessment than the scene setting assessment, will be required. It is pertinent to mention that, the first stage PIA is mandatory for all projects.

Screening Assessment (Stage 2 PIA)

The second stage PIA is referred to as the screening assessment, during which project stakeholders are interviewed to determine the level of personal data the project intends to process, or has been processing, this is applicable to existing projects (see Figure 1). The aim of the screening assessment is to determine whether a small-scale or large-scale PIA is deemed necessary for the project. A small-scale privacy impact assessment is an abridged privacy risks assessment of a project. It is recommended when a small percentage of the project characteristics underline some privacy concerns. For example, if one or two features of the project characteristics imply privacy concern, then it is justifiable to recommend a small-scale PIA assessment. If more than three aspects of the project characteristics underline privacy concerns, then a large-scale PIA is justifiable. Having said that, there are cases when a small-scale PIA is recommended even a number of a project features seems to underline privacy concerns. For example, if it is perceived that personal data being processed are either none sensitive or the processing is infrequent. None sensitive personal data refers to personal data of a living individual that can only identify an individual when linked or combined with other personal data of that individual. For example, an email server project that collects only two sets of personal data during user registration such as name and email address of the user would justify a small-scale PIA, even though it aggregate significant volumes of personal information data. A large-scale PIA assessment is an extensive, thorough, and detailed privacy risks assessment. A large-scale PIA assessment is recommended when a good percentage of the project characteristics evaluated during a screening exercise underlines serious privacy concerns. For example, a data consolidation project of a health service that links data controllers or sources warrants large-scale privacy risks assessment. Both small-scale and large-scale privacy impact assessments require project stakeholders to be interviewed in order to determine the areas of the project that involve processing of personal information data, and the level of analysis or manipulation (source linkages) of personal data that are intended.

There is no empirical method of deciding which projects should undergo large-scale or small-scale privacy impact assessment. One approach that has been recommended to determining the level of assessment required for a project is the use of screening questions [13] developed by the ICO. The ICO’s proposed screening process is extremely helpful; unfortunately, the screening process does not guarantee that the same project when assessed by two separate organisations would lead to the same level of PIA recommendations. For this reason, proposed the Privacy Screening Framework (see Table 4), in addition, we designed a general purpose legal and privacy assessment questions (see Table 3) to assist organizations assess legal and privacy compliance of projects during PIA assessments.

Table 3: Legal & Privacy Compliance Check

	Legal & Privacy Compliance Check	
	Project Name:	
	Project Reference:	
	Organisation:	
	Asset Owner:	
	Name of PIA Assessor:	
	Names of Project Stakeholders:	
	Date Completed:	
No	**Question**	**Response**
1	Will the processing of personal data comply with all relevant and applicable privacy regulations/legislations? For example, Data Protection Act 1998, Data Protection Principles (1-8), The Privacy Act, Human Rights Act 1998, Freedom of Information Act 2000 etc?	
2	Are the business processes to be used (or been utilized) compliant with all relevant and applicable regulations/legislations?	
3	Are there standards and law that this project must comply to? For example, the Federal Information Security Management Act (FISMA), E-Government Act, Tort of Negligence, Tort of Passing off, Public Health requirements, etc?	
4	Are there other privacy related (statutory) compliance arising from privacy policy statement of the organization? For example Code of Connection, Information Governance Statement of Compliance (IGSoC), Caldicott Principles, Fair Credit Reporting Act?	
5	Are there privacy related mandates from the public that this project must satisfy? For example, Public Disclosure of Privacy Practices, and Security Breaches Disclosure Act.	
6	Will the project comply with the Privacy and Electronic Communications Regulations 2003, Fair Credit Reporting Act, Disclosure of Personal Information, etc?	
7	Will the data collected by the project be shared or transport outside the Province of Data Origin but used within the Country of Data Origin?	
8	Will the data collected by the project be shared or transport outside the Country of Origin?	
9	Will the data collected by the project be accessible, or processed, remotely from outside the Country of Data Origin?	
10	Will the data collected by the project be processed by individuals with certain personnel security clearances?	

Table 3 consists of ten (10) questions comprising legal, regulatory and legislative assessment of personal data handling, processing and sharing. The idea behind the provision of the legal and privacy compliance check is to ensure that PIA assessments are consistently evaluated by each organization by following the same prescriptive guideline. After carrying out legal and privacy compliance checks of a project, the next activity in the PIA assessment is the privacy screening assessment.

PRIVACY SCREENING FRAMEWORK (PSF)

The privacy screening framework is our proposed framework that provides the required prescriptive guidance for carrying out large-scale PIA assessments. The PSF framework is flexible, adaptable and self-directing. It is flexible because the PIA assessor can choose to add or remove any non-applicable sections of the framework without influencing the end result of the assessment. PSF is adaptable and self-directing because the PIA assessor is required to carry out the assessment, and can modify any sections of the framework that is deemed not applicable to the project's locality or operating environment (see Table 4). For example, when conducting a PIA assessment of a project in the UK, it may not be relevant to evaluate the project based on US-specific privacy legislations except where bilateral mandates are applicable. Similarly, privacy risk assessment of US-based projects should be evaluated against US-specific privacy legislations and applicable industry regulations, plus bilateral or multilateral privacy understandings, where applicable. Thus, it is equally the case with privacy risk assessment of project hosted in other EU countries such as Belgium, Germany or France.

The privacy screening framework is composed of eight (8) sections. Section 0 is about the project details, comprising project name, reference, organization, asset owner and name of PIA assessor. Section 1 is technology assessment, which focuses primarily on privacy risk assessment of three main areas – privacy-invasive technologies, event and information monitoring technologies, and data capturing and screening technologies. Section 2 is project justification assessment. It is aimed to ensure that the purpose and justification of the project are made known to the public or the users of the system. It has two subcategories – justification for data handling and justification for new data acquisition. Section 3 is identity assessment, which focuses on privacy risks associated to the use, combination and linkage of personal identifiers, such as username, date of birth, national insurance number etc (see Table 1). Section 4 is data assessment. This assesses the quantity and significance of personal data being processed (used, stored or transported). Section 5 is data handling assessment, which focuses on privacy risks associated with data collection policies, procedures and quality assurance. Section 6 is awareness assessment. It deals with privacy risks associated with the security of the information system processing personal information data for the project; in addition, it deals with secure disposal and destruction of the information system holding personal information data, when no longer in use. Finally, section 7 is miscellaneous, which affords the risk assessor the opportunity to profile other pertinent privacy risks particular to systems utilized for the project. For example, privacy concerns with legacy systems, bespoke design and customized solutions etc.

Table 4: Privacy Screening Framework (PSF)

Section	Privacy Screening Framework	
0	**Project Details**	
	Project Name: **Project Reference:** **Organisation:** **Asset Owner:** **Names of Assessors:** **Date of Assessment:**	
1	**Technology Assessment**	
a	**Privacy-invasive technologies**	**Response**

1a1	Does the project involve new or inherently privacy-invasive technologies? E.g. The use of technologies such as smart cards, RFID, biometrics, locator monitoring technologies, visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic, security events and information management etc?	
1a2	Are all technologies applied to the project well-understood by the organisation?	
1a3	Are there demonstrable concerns that the technologies used in the project may impact privacy?	
1a4	Are privacy impacts (from the project) well-understood by the organisation, and by the service consumers	
1a5	Are there measures applied to avoid or mitigate negative privacy impacts, or at least reduce them to satisfactory levels of those whose privacy is affected?	
b	**Event and information monitoring technologies**	**Response**
1b1	Does the project involve the use of event and information monitoring technologies such as Security Event and Information Management (SEIM), Security Event Management (SEM) or Security Information Management (SIM) systems such that user traffic, user (service consumer) actions and user locations can be monitored?	
1b2	Are organization and service consumers aware that their traffic is being monitored?	
1b3	Is the use of the SEIM/SEM/SIM due to regulatory or security compliance, if yes, please specify?	
1b4	If service consumer data are collected, are these subjected to reprocessing that could lead to the identification of an individual?	
c	**Data capturing and screening technologies**	**Response**
1c1	Does the project involve the use of data capturing, admission and screening technologies such as Biometrics, RFID, Blood sampling toolkit, Lab equipment, X-ray and digital imagery, Data monitors such that user identifiable attributes, characteristics or features are monitored, captured or/and stored?	
	Is the use of the data capturing and screening tool due to regulatory or security compliance, if yes, please specify?	
1c2	Are the organisation and service consumers aware that their traffic are being monitored	
2	**Justification Assessment**	
a	**Justification for data handling**	**Response**
2a1	Are there justifications to why personal data is being handled, and are these being communicated to the service consumers?	
2a2	Do service consumers understand the benefits of the project to them?	
b	**Justification for new data acquisition**	**Response**
2b1	Is the acquisition of pieces of new personal data required, such as user registration details – username, date of birth, national insurance number or social insurance number etc?	
2b2	Will pieces of new additional data collected combined with existing personal information data?	
2b3	Do service consumers understand the benefits of the additional data supplied in the overall evaluation of the project?	
3	**Identity Assessment**	
a	**Does the project involve an additional use of existing identifier**	**Response**

3a1	Will the project make use of a combination of existing identifiers (example, username, date of birth, enrolment date, address etc) in its processing or analysis?	
3a2	If yes to **3a1**, how many identifiers will be combined?	
3a3	And which identifiers from **3a2**?	
b	**Does the project involve use of new identifiers for multiple purposes**	**Response**
3b1	Will the project require a new identifier (such as, username, date of birth, enrolment date, address, national insurance number etc) and would this new identifier be combined with existing identifiers?	
3b2	If identifiers are combined, which are those?	
3b3	Will an identifier be used for multiple purposes such as those used for registration/enrolment, authentication and identification or service improvement contact?	
c	**Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous**	**Response**
3c1	Will the registration process of the service requires three or more personal identifiable information such as (name, address, national insurance number, date of birth, email address, mother's maiden name etc)?	
3c2	Will the authentication process of the service requires the use of new identifiers, such as post code, pass phrase or PIN (personal identifiable number)?	
3c3	Will the project cache or store personally identifiable information of users (service consumer) during registration?	
3c4	Does the registration process require two or more processes, that is, enrollment and verification (for example, collection of basic personal details and onerous PII details)?	
4	**Data Assessment**	
a	**Will the project result in the handling of a significant amount of new data about people, or significant change in existing data-holdings**	**Response**
4a1	Will the project result in the handling of a significant amount of new data about citizens or users such as name, address, date of birth, national insurance number, mother's maiden name etc. Example national criminal database?	
4a2	Will the project result in the handling of a significant change in existing data-holdings?	
4a3	Will the project combine both new and existing pieces of personal information data?	
b	**Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage**	**Response**
4b1	Will the project result in the handling of new data about a significant number of service consumers, public or citizens?	
4b2	What is the estimated number of service consumers, public or citizens required to use this service?	
4b3	What category of service consumers, public or citizens is expected to use the service?	
c	**Does the project involve new linkage of personal data with other data sources, or significant change in data linkages**	**Response**
4c1	How many data linkages or data sources (transfer, consolidation or storage) of personal data are in use?	
4c2	Will data collected for other purposes used in this project?	

4c3	Will the project use or combine personal data collected for other purposes with those collected during service consumer registration/enrolment?	
4c4	Will the project involve significant change in data linkages / data sources	
5	**Data Handling Assessment**	
a	**Does the project involve new or changed data collection policies or practices that may be unclear or intrusive**	**Response**
5a1	Will the project use new data collection policies that may be unclear or intrusive to service consumers?	
5a2	Will the project require the modification of existing data collection policies that may be unclear or intrusive to service consumers?	
5a3	Will the project involve new data collection practices or procedures that maybe unclear or intrusive to service consumers?	
5a4	Will the project require the modification of existing data collection processes or procedures that may be unclear or intrusive to service consumers?	
b	**Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory**	**Response**
5b1	Will the project use new data quality processes or procedures that may be unclear or intrusive to service consumers?	
5b2	Will the project use changed data quality processes or procedures that may be unclear or intrusive to service consumers?	
c	**Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory**	**Response**
5c1	Will the project require new data security arrangements or mechanisms that may be unclear or intrusive to service consumers?	
5c2	Will the project use changed data security arrangement processes or procedures that may be unclear or intrusive to service consumers?	
d	**Does the project involve new or changed data access or disclosure arrangements that may be unclear or unsatisfactory**	**Response**
5d1	Will the project use new data access or disclosure arrangements that may be unclear or intrusive to service consumers?	
5d2	Will the project use changed data access or disclosure arrangements that may be unclear or intrusive to service consumers?	
e	**Does the project involve new or changed data retention arrangements that may be unclear or permissive**	**Response**
5e1	Will the project use new data retention arrangements that may be unclear or intrusive to service consumers?	
5e2	Will the project use changed data retention arrangements that may be unclear or intrusive to service consumers?	
f	**Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before**	**Response**
5f1	Will the project make publicly available piece of personal information data readily accessible. For example, use of public Internet website that organize and aggregate personal information data, such as data mining?	
6	**Awareness Assessment**	
a	**System / project security**	**Response**
6a1	Will the system/project be known to the general public?	

6a2	Will the system/project be known to competition?	
6a3	Does the system have known or publicly known vulnerabilities?	
6a4	Will the system be used in a vulnerable environment?	
6a5	Will the system be deployed in a restricted test environment?	
6a6	Will the system be deployed in restricted live environment?	
b	**System secure sanitization and destruction**	**Response**
6b1	Has any component of the systems used for the project been decommissioned, re-used or destroyed?	
6b2	If yes to 6b1, were these systems securely sanitized before re-use, or securely destroyed such that personal data they hold cannot be reconstructed from an adversary?	
7	**Miscellaneous**	
7a	Please provide any comments you think may assist with the risk assessment of the system/network or platform being evaluated.	

Privacy Impact Assessment of an In-Service Project

A project is said to be in-service when it is already being used to delivery a type of service or another. In every aspect, it means the project has gone live. There are five phases to any project lifecycle: initiation phase, development phase, test phase, in-service phase, and decommission phase. Privacy impact assessment of an in-service project is the retrospective privacy risk assessment of a project that is already being used to deliver a service. This means that risk assessment of the project was previously completed only on the basis of business and security requirements, without prior assessment of privacy risks associated with the project.

Privacy impact assessment of an existing project is the retrospective assessment of privacy risks associated to that project. First, privacy assessment suitability of the project should be established as shown in Figure 1. Second, privacy risks relating to technologies or mechanisms deployed in the project, data collection and handling procedures applied (see Privacy Screening Framework - Table 4), and compliance to privacy legislations and regulations (see Table 3) should be evaluated. Finally, specific project privacy requirements should be addressed.

Assessing privacy risks of an existing (in-service) project can be challenging, while the outcome is often astonishing and expensive, because of the following:

1. Asset owners and senior information risk owners do not have a clue how damaging results from such assessments may turn up.
2. Outcome could imply privacy violation or breach.
3. Outcome could show that certain technologies are privacy intrusive or that the data collection and handling procedures contravene privacy regulations or legislations. This may lead to such technologies being decommissioned from the project, consequently resulting to significant financial losses to the organization.
4. Outcome could be costly because the result may mean that certain assets in the project may have to be decommissioned, withdrawn or destroyed. It could also result in significant financial penalties such as fines due to breach of privacy. For example, in August 2010, the UK Government's Financial Services Authority (FSA) fined Zurich Insurance record data loss fine of £2.3M due to a breach on privacy [14]. There are a number of cases of huge financial penalties being hit on organisations due to privacy breaches, and such breaches are now starting to be publicly disclosed as Government takes new stances to ensure organisations take privacy seriously.

To conduct privacy impact assessment of an existing project we recommend a quick assessment using our privacy impact assessment questionnaire (see Table 2). This assessment is meant to show if PIA is indeed relevant to the project or not. Based on the outcome of this assessment, further privacy assessments of the project will be decided. It is pertinent to mention that privacy impact assessment of in-service projects follow the same methodology as new projects (see Figure 1). This means that, first, privacy suitability assessment of the project (Stage 1 PIA). Second, based on the outcome of the Stage 1 PIA assessment, Stage 2 PIA will commence; otherwise the assessment is concluded. Following the second stage PIA, two sets of assessment is envisaged, either a small-scale or a large scale PIA assessment.

It is pertinent to re-iterate that the outcome of privacy impact assessment of an existing project can be insightful and expensive. We recommended organisations to consider conducting PIA as early as possible in the project lifecycle to minimize the consequences associated with in-service PIA. For example, PIA of an existing project could reveal that an organisation is in breach of privacy because of the use of technologies that are intrusive in the processing of personal information data. In another case, it may reveal that an organization does not comply with certain privacy regulations or legislations. Either case, the impact it will have on the organization is huge. For instance, it could lead to significant financial penalties, withdrawn accreditation, or/and subsequent termination of the project. In a normal circumstance, breach of privacy attracts a fine and requires fresh risk assessment of the project, which costs both time and money. In an extreme case, it will lead to significant financial penalty (as a result of breach of customer service agreement and resultant fine from the government), affects the organisation brand (negative media publicity), and especially in situations where disclosure of security or privacy breaches are required due to regional or provincial legislation. Finally, it may lead to termination of the project.

Privacy Impact Assessment of a New Project

With new projects it is recommended that privacy requirements are assessed from the outset and consideration to these requirements are made prior to implementation. This does not mean that privacy impact assessment of new projects is a panacea to all privacy concerns. As shown in Table 5, the difficulty to carrying out privacy impact assessment of new projects are that at the early stages of a project, very little is known of the various components of the project. For example, the entire design of the project may not have been fully developed. Stakeholders may not fully understand all the requirements of the project and detailed functional features of all the technological mechanisms to be deployed in the project may not have been known. Hence, privacy assessment of all the various components of the project, at this stage, is not feasible.

New projects afford an organization the opportunity to consider privacy requirements from the outset. As set out by local, national and international privacy agencies, privacy impact assessment is one way of ensuring that privacy concerns are addressed from the start of project initiation to the entire lifecycle risk management of the project. The fact that a project is new does not make privacy impact assessment of that project any easier compared to PIA assessment of an in-service project. As shown in Figure 1, the same framework is utilized to assess both new and existing projects.

A major concern observed with most privacy impact assessments is that organisations do not often have the right mix of privacy skilled experts to carry out privacy impact assessments. Often, people with limited privacy expertise from varying but related disciplines such as information assurance, information security or information technology are asked to carryout privacy impact assessments. Our recommendation for organisations is to enlist the service of privacy experts to assist with PIA exercise, especially when large-scale PIA is recommended. A lesson learned from carrying out privacy impact assessments is that interpretation of privacy requirements does so often differ among stakeholders.

Table 5 provides some comparisons between PIA of new and existing projects. It is evident that there are issues that are common to both new and existing projects, such as compliance to privacy legislations and regulations. Nevertheless, there are issues that fall under one category but not the other. For example, privacy impact assessment of existing projects may require retrofitting of privacy, or risk acceptance of privacy non-compliant practices; whereas, for new projects, privacy considerations are recommended from the outset, hence retrofitting of privacy requirements are not applicable.

Table 5: A Comparison of Privacy Impact Assessment of Existing and New Projects

Specific Issues to New and Existing Projects		
S/N	**New Project**	**Existing Project**
1	At the early stages of the project initiation phase, functional requirements of the different components of the project may not be known and well understood, hence privacy impact assessment of the project at this stage may be inconclusive.	Functional requirements are known, but the realisation that the project maybe combining multiple personal information identifiers may not have been considered.
2	Often, all the technologies, or mechanisms to be used in the project may not be properly identified, hence privacy assessment relating to technology or mechanism, or even the design cannot be properly evaluated.	Because the project is already in-service, even when privacy risks are identified, addressing all the identified risks may impact service, hence business needs often override privacy requirements.
3	Ownership of risk may become an issue, especially when information security roles and responsibilities have not been defined and agreed on.	Ownership of risk is also an issue with existing projects, especially when prior privacy risks have not been conducted.
4	Expertise in conducting privacy impact assessment for new projects within a single organisation (for example, small to medium-size organisation) is a challenge.	Expertise in conducting privacy impact assessment is also a challenge for existing projects, because: a) Skills to do so may not exist within one organisation, and, b) Expertise to assess existing projects, and manage relationships and interfaces that exist with in-service project can be onerous.
5	The scope or extent to which personal information to be collected will be processed (shared, stored, combined, exchanged) may not be known and well understood.	Where privacy impact assessment may reveal a high likelihood of privacy violation, business needs may override privacy requirements, especially if addressing privacy issues may result to service impacting consequences or significant financial expense.
6	The extent to which different personal information identifiers may be combined, processed or analysed may not be fully determined.	There may be a bias to suppress privacy risk in relation to business needs since privacy impact assessment was carried out retrospectively.
7	The justification of the project to service consumers (users of the systems, public or citizen) may not have been discussed or communicated to the public or wider service	The justification for existing projects are known, but the use of additional personal identifiers may have not been justified for existing projects, and when there is a scope change to existing project,

	consumers.	this is not often communicated to the service consumers.

Risk relating to Aggregation of Personal Identifiable Data

Personally identifiable information (PII) requires special handling/processing procedures in accordance to the Data Protection Act (DPA) Principles 1-8, the Privacy Act and other national and international privacy legislations. This is because the impact of privacy breaches to an individual, which could vary from prolonged personal distress to significant personal financial losses. Unfortunately, privacy breach of a project collecting PII data of citizens will impact a larger population of individuals, resulting to prolong distress to a population of individuals. The cumulative and interdependent risks resulting from the collection of significant number of aligned sensitive personal information data require proportionate risk mitigation procedures, and additional controls may seem plausible to address risk resulting from aggregation of these PII data. When carrying privacy impact assessment of a project, it is worth taking into consideration (at stage 2 of the PIA assessment) whether personal data from numerous data collectors or sources will be aggregated. That is when a significant number of personally identifiable information is collected or combined proportionate privacy-assurance controls should be required. For example, additional storage, processing and handling requirements may be needed.

Personally identifiable information requires special handling, sharing, storage and retention procedures. While these procedures are essential to protecting PIIs, additional handling and sharing procedures may be required if a significant amount of personal data is required. Further, if these information would be handled in new ways or ways that involved new linkages of personal data, additional controls should be used to address risks resulting from this new practice.

Solutions and Recommendations

In this chapter guidance to conducting privacy impact assessment of both new and in-service projects are provided. Fundamentally, the Privacy Impact Suitability Assessment (PISA) framework is provided to enable organisations successfully carry out privacy impact assessment, knowing that every project should be assessed for privacy risks. The PISA framework is useful and straightforward to use and apply to any project with respect to privacy risks assessments.

To ensure PIA assessments are consistent and straightforward, we proposed the Privacy Screening Framework, which assists privacy assessors to assess projects prescriptively against all the seven categories of privacy risks. The PSF framework is flexible, adaptive and self-directing; which means that the person undertaking the assessment (assessor) can choose to adapt the framework to suit the needs of a particular project. The framework can be utilized and applied by any person. The framework is straightforward and derived based on lessons learned in carrying out PIA assessments for a number of organisations on a number of projects. Further to the frameworks provided, we provided the legal and privacy compliance check (see Table 3) to ensure consistency when assessing privacy regulations and directives compliance.

With the understanding that the earlier privacy assessment is planned in the project initiation programme the better the organization will be in addressing privacy requirements, issues or concerns. We recommend that privacy impact assessment should become an essential part of the risk management process of every project. We hope that this will help organisations plan PIA from the outset of the project, knowing that retrofitting of privacy assessment can be costly as we have seen with PIA assessment of in-service projects.

When planning privacy impact assessment, considerations should be made of risks resulting due to the sheer volume of personally identifiable information the project would process. And when data from different sources will be used, the impact of aggregation of these data should be considered. This should serve as an indicator as to when additional privacy controls may be required due to aggregation effect. Finally, we recommend that privacy impact assessment should be carried out by privacy experts within an organization, and where people with the right skills cannot be found, the services of external privacy agencies should be enlisted.

There is a new privacy legislation in the UK that empowers the UK Information Commissioner's Office to exact financial penalty to any organization in breach of privacy. This will, and has ushered a reawakening of privacy consciousness in organizations, especially, governmental organizations and agencies.

FUTURE RESEARCH DIRECTIONS

We plan to automate the PIA frameworks proposed in this chapter into a toolkit that will assist organizations when carrying out privacy risk assessments. The proposed toolkit will be available for download, or used from www.research-series.com. The provision of automated toolkits to assist with conducting PIA can be helpful, but the challenge will be on the coverage of relevant privacy legislations. This is because local or provincial privacy legislations are different among countries; hence, it will be challenging to cover all applicable privacy legislations in the toolkit.

CONCLUSION

In this chapter, we discussed challenges to managing privacy impact assessment of personally identifiable information. The different issues relating to privacy impact assessment of new and in-service projects are demonstrated and discussed. It was found that in-service projects were challenging to be privacy assessed, and the outcome of privacy impact assessment to an in-service project could be insightful and expensive; and consequently could result to significant financial losses to the organization when found in breach of privacy. Privacy impact assessment frameworks were proposed, discussed and utilized to demonstrate their usefulness when conducting PIA assessments. Each framework was described such as the privacy impact suitability framework, legal and privacy compliance check and privacy screening framework. Finally, issues surrounding aggregation of personally identifiable information were discussed with the view to highlighting associated risks while recommending essential privacy controls to addressing these risks.

ADDITIONAL READING SECTION

Onwubiko, C. (2008). *Security Framework for Attack Detection in Computer Networks*. Germany: VDM Publishing.

Stolfo, S. J. & Tsidik, G. (2010). Privacy-Preserving Sharing of Sensitive Information. *IEEE Security & Privacy, 8(4), 16-17.*

Kenneally, E. E. & Claffy, K. (2010). Dialing Privacy and Utility. *IEEE Security & Privacy, 8(4), 16-17.*

Ministry of Justice (2010). Undertaking Privacy Impact Assessments: The Data Protection Act 1998, 13 August 2010. Retrieved October 2010 from www.justice.gov.uk/guidance/docs/pia-guidance-08-10.pdf

Charlesworth, A. (2007), Privacy Impact Assessments: International Study of their Application and Effects. Law School, Bristol University, October 2007. Retrieved October 2010 from http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_apph_eur_2910071.pdf

Information Commissioner's Office (2010). An overview of the Data Protection Act 1998. Retrieved October 2010 from http://www.ico.gov.uk/upload/documents/library/Data_Protection/Introductory/DATA_PROTECTION_ACT_OVERVIEW.PPT

The National Archives (2010). Data Protection Act 1998. Retrieved October 2010 from http://www.legislation.gov.uk/ukpga/1998/29/contents.

Robert Gellman (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. World Privacy Forum. February 23, 2009

Wikipedia (2010). Data Protection Act 1998. Retrieved October 2010 from http://en.wikipedia.org/wiki/Data_Protection_Act_1998.

NIST (2010). The Federal Information Processing Standard (FIPS) 199, Standards for Security Categorisation of Federal Information and Information Systems. Retrieved November 6, 2010 from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

Whitehouse (2006). Office of Management and Budget (OMB) Memorandum M-06-15. Safeguarding Personally Identifiable Information. Retrieved November 6, 2010 from http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m-06-15.pdf.

Rodney J. Petersen (2003). Security, Privacy, and the Protection of Personally Identifiable Information. EDUCAUSE/Internet2 Computer and Network Security Task Force. Retrieved November 6, 2010 from http://net.educause.edu/ir/library/powerpoint/SEC0315.pps.

Asif Tufal (2010). The Torts of Negligence. Retrieved November 6, 2010 from http://a-level-law.com/tort/Negligence/Flowchart.pdf.

KEY TERMS & DEFINITIONS

Personal Data: Personal data is data that relates to a living person who can be identified by those data, or from those data plus other information which is in the possession of, or is likely to come into the possession of, the data controller. For example, first name, last name or/and date of birth of a living person.

Sensitive Personal Data: These are identifiable personal data whose release would put those persons at significant risk of harm or distress, unless otherwise disclosed by the persons. For example, a person's medical records, bank details, social insurance number (national insurance) or tax records etc.

Personal Identifiable Data (PID): These are sensitive and personal data that can be used to identify an individual. Personal identifiable data is the same as Personally Identifiable Information (PII), while the former is associated to Europe; the latter is associated with America. Examples of PII include a combination of one or more personal identifiers such as full face photographic images and any comparable images plus name, or date of birth plus address and health records. A full list of personal identifiers is shown in Table 1.

Data Protection Act (DPA): This is a piece of legislation that governs how personal information of living individuals are processed. Processing of personal information means, how personal information are obtained, shared, recorded or stored (held). This piece of legislation was enacted in 1998 in the United Kingdom (UK).

REFERENCE

[1] Information Commissioner's Office (ICO) Cabinet Office, UK (2009). Privacy Impact Assessment Handbook Version 2.0. Retrieved October 6, 2010, from http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

[2] Educause, (2010). Privacy Risks Assessment. Retrieved October 6, 2010 from http://www.educause.edu/node/645/tid/30444?time=1281348515

[3] EINSTEIN 2: US-CERT. Retrieved March 11, 2011 from http://en.wikipedia.org/wiki/Einstein_(US-CERT_program)

[4] Marco Gruteser and Dirk Grunwald (2004). A Methodological Assessment of Location Privacy Risks in Wireless Hotspot Networks in Security in Pervasive Computing, Lecture Notes in Computer Science, 2004, Volume 2802/2004, 113-142, DOI: 10.1007/978-3-540-39881-3_5

[5] Trevor Peirce, (2009). RFID Privacy & Security. IEEE International Conference on Communications, ICC 2009, Dresden, Germany, June 2009

[6] S. Abu-Nimeh and N. R. Mead, (2001). Privacy Risk Assessment in Privacy Requirements Engineering. 2nd International Workshop on Requirements Engineering and Law, Georgia, USA, 2009.

[7] Shirley Radack, (2010). Guide To Protecting Personally Identifiable Information (PII). NIST ITL Security Bulletin for April 2010. Retrieved November 6, 2010 from http://csrc.nist.gov/publications/nistbul/april-2010_guide-protecting-pii.pdf

[8] HIPAA (2006). Saint Louis University Institutional Review Board HIPPA TIP Sheet, 31st March 2006. Retrieved November 21, 2010 from www.slu.edu/Documents/provost/irb/hipaa_tip_sheet.doc

[9] HMG IA Standard No. 6 (2009). Protecting Personal Data and Managing Information Risk, Cabinet Office, CESG National Technical Authority for Information Assurance, Issue 1.2, March 2009.

[10] Directive 2002/58/EC, (2002). Protection of Privacy to Electronic Communications. Retrieved November 20, 2010, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

[11] US-CERT, (2008). Privacy Impact Assessment EINSTEIN Program. Department of Homeland Security, National Cyber Security Division, United States, May 19, 2008. Retrieved October 8, 2010 from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf

[12] Cabinet Office, (2008), The Data Handling Procedure in Government: Final Report, June 2008. Retrieved October 6, 2010 from http://www.cesg.gov.uk/products_services/iatp/documents/data_handling_review.pdf

[13] Information Commissioner's Office (ICO), (2009). Privacy Impact Assessment Handbook Version 2.0. Appendix 1 – PIA Screening Process. Retrieved October 29, 2010, from http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/3-app1.html

[14] Daniel Shane, (2010). Zurich Insurance hit with Record Data Loss Fine, August 2010. Retrieved October 22, 2010 from http://www.information-age.com/channels/security-and-continuity/news/1277718/zurich-insurance-hit-with-record-data-loss-fine.thtml