Privacy by Design

From privacy policy to privacy-enhancing technologies

R.F. Koorn
is a partner at KPMG IT Advisory. He has extensive experience in the fields of privacy, security, e-invoicing, information governance and the flexibility of IT. He has co-written the white paper on privacy-enhancing technologies for the Netherlands Ministry of External Affairs and the EU. He assisted the Dutch Data Protection Authority in the development of privacy mechanisms and audit frameworks. He has performed a number of assignments as a privacy consultant and auditor, both in Europe and in the United States, where he worked for two years on assignment for KPMG (San Francisco and Silicon Valley).

koorn.ronald@kpmg.nl

J. ter Hart
is a manager at KPMG IT Advisory, specializing in identity management, e-signatures, wireless security, e-invoicing and privacy. He has performed various consulting and auditing assignments, and is also co-author of the white paper on privacy-enhancing technologies.

terhart.joris@kpmg.nl

Ronald Koorn and Joris ter Hart

Privacy protection in organizations is often a matter of legal and procedural measures. However, privacy legislation is also concerned with the use of IT to improve the reliability and efficiency of compliance with privacy requirements. In this way, IT is not merely the primary cause of privacy issues, but also at least a part of the solution. This article discusses a number of relevant developments affecting privacy and the role of what is known as "Privacy by Design."

Introduction

After a brief introduction about privacy legislation, a number of privacy issues will be discussed. This discussion will explore organizational positioning and privacy awareness, as well as social and IT developments that affect both the perception of privacy and compliance with privacy requirements. The similarities and differences between privacy and security will be briefly considered. Next, a description will follow of the ways in which organizations have dealt with privacy issues since the introduction of legislation in this area, an overview that will be supported by recent KPMG research. This essentially involves a gradual but discernible development towards greater use of IT, culminating in the deployment of privacy-enhancing technologies. Finally, the main financial and implementation factors will be considered.

Development of privacy legislation

Privacy protection and privacy invasions have been around forever. Legislation existed to govern certain areas of privacy even in the Middle Ages, but the protection of privacy only really picked up steam after the second world war (for related and apparent reasons). The 1948 Universal Declaration of Human Rights states that territorial and communications privacy are considered fundamental rights.

The introduction and proliferation of IT in public and private organizations, and the privacy implications of its use and misuse, have provided a major impetus for further privacy legislation. The introduction of a privacy law in the German State of Hesse (1970) was followed by national laws in Sweden (1973), the United States (1974, applying exclusively to government), Germany (1977) and France (1978). This provided the basis for

OECD's[1] *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data* (1980) and the Council of Europe's *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data* (1981).

The Council of Europe convention has been adopted by more than twenty countries, while the OECD Guidelines have also been incorporated in various national laws. As is generally well known, the European Union has been giving privacy great priority since the early nineties, culminating in the Data Protection Directive[2] of 1995. This Privacy Directive came into force in various EU member states between 1995 and 2002, hence later than the deadline of October 1998 in most cases. Further background about the development of privacy laws is provided in [Kooro1] and [EPIC06]. The rest of this article will focus solely on privacy of information and communications; physical and territorial privacy falls outside its scope.

Data protection requirements and responsibility

Assignment of responsibility for privacy within organizations can vary considerably. Usually, the task falls to a lawyer in the Legal Department, but it may also be assigned to the Security Officer, Risk Manager, or sometimes even a marketing expert or IT auditor who takes care of privacy "on the side." In more mature organizations, privacy is often handled by a Privacy or Compliance Officer or department (when customer data is involved) or the HR department (when employee data is involved). Such organizations are also attentive to privacy governance.

The Privacy Officer role, once a part-time position, has in recent years undergone extensive professionalization in response to the full-time concern for privacy management.

In organizations where privacy is properly entrenched, privacy governance affects how these issues are handled. Practices may vary from a strong legalistic approach with stringent regulations and procedures to a balanced approach with emphasis on both organizational and IT measures. At the same time, communication between lawyers, process/system/data owners, project managers, IT professionals, marketeers and users remains a major obstacle to the proper design, implementation and enforcement of privacy protection. These individuals use different terminology and do not always appreciate each other's point of view. Based on our experience, we dare to say that fewer than 10% of complex organizations operate in full compliance with privacy legislation.

1 OECD: Organization for Economic Cooperation and Development.
2 European Directive EC95/46, also known as the European Data Protection Directive.

Awareness

Increased privacy awareness usually correlates with legislative surges. Although there is limited research on the awareness of and compliance with privacy requirements, surveys have nevertheless revealed that the level of awareness also vacillates. Surrounding the introduction of privacy legislation in the eighties and early nineties, privacy issues were not only receiving attention from governments but from the business community as well. Under the pressure of these new laws, most large organizations developed privacy policies and sector regulations, in most case subsequently implementing only a part of them. Other major incentives arose that were not directly connected with new legislation but were instead due to external factors and IT developments.

- *Use of the internet for personal data exchange:* Sites requiring on-line accumulation of personal and credit card data were initially met with skepticism from users due to uncertainty about the consequences for privacy and security. As the popularity of social networks like Facebook, Friendster, MySpace, *etc.* has increased exponentially, they are eagerly being used to provide and disseminate a great deal of personal data. In response, privacy and security statements have been posted on some websites and self-regulating programs have been used to instill trust in others (TRUSTe, WebTrust, Europrise, *etc.*).
- *Outsourcing and offshoring:* The transfer of business processes and IT systems to third parties that may be located abroad and often outside the EU (*e.g.* Asian countries) is a trend that has increased privacy awareness. In practice, the privacy protection of these service providers is sometimes even more rigorously scrutinized than the privacy practices within the outsourcing organization. The result is the formulation of processor agreements and the inclusion of security and privacy clauses in contracts and service level agreements (SLAs).
- *Global information systems, data center consolidation and shared service centers:* Multinationals are increasingly being involved in global exchanges of personal data. Especially in situations where the central HR or CRM system is situated outside the EU (*e.g.* in the US), employees, works councils, and data protection authorities require additional privacy safeguards, such as (model) contracts and explicit consent.
- *New technology:* Various technical developments make it possible for personal data to be exchanged more intensively through still more channels, thus increasing privacy risks. Examples include cloud computing ([KPMG10a]), electronic patient records, RFID, smart cards for various applications (*e.g.* public transport), biometrics, telemedicine, DNA databases, online profiling ([KPMG10b]), smart energy meters, *etc.*
- *Audits by data protection authorities:* Privacy regulators have been conducting privacy audits in various sectors since the mid nineties, partly on their own initiative and partly in response to complaints. Fines have also been issued, but penalties in the EU still remain relatively modest, even if considerable sums are now being assessed in Spain and, since mid 2010,

in the UK (up to £500,000). This enforcement activity has had a strong role in promoting awareness in such organizations as health-care institutions, police, commercial information agencies, financial institutions, municipal administrations, *etc.* Supervisory authorities in other sectors (*e.g.* finance and medicine) are showing increasing interest in including privacy in their inspections and reviews.

- *Fraud and abuse of social service:* Completely different concerns are raised by the legally expanded use made of public service databases to combat fraud. The parties involved only began to appreciate the privacy issues involved when such practices actually began to occur. In some instances, extensive database matching is being used to create an indiscriminate "digital dragnet" to catch illegal activity.
- *Threat of terrorism:* The terrorist threat has resulted in police and intelligence agencies acquiring increased powers that potentially compromise the privacy of suspects. Unfortunately, innocent civilians are also being affected, as demonstrated when the CIA obtained access to all the payment transactions routed through the SWIFT inter-banking network. To some extent, this access to sensitive personal data may be acceptable as it serves a higher purpose. At the same time, there is the danger that it creates a "Big Brother"-like situation. Insofar as direct conflict arises on this subject, politics and views about national security prevail over any individual privacy concerns.
- *Media attention to privacy incidents* (see Box 1 for some examples): The unlawful collection and misuse of personal data, otherwise known as identity theft, has become one of the biggest causes of fraud in the US, victimizing several hundred thousand Americans and involving losses in the billions of dollars annually.

Box 1: Examples of published privacy incidents

Role of public privacy incidents

Incidents of privacy breaches have undeniably had a large influence on privacy awareness. Examples of such incidents are everywhere. Due to lapses in privacy protection and inadequate security measures, extremely sensitive personal data has been published. The number of personal records subject to privacy breaches has now reached 500 million (see privacy incidents since 2005 at http://www.privacyrights.org/data-breach).

- The best known case in recent years was the loss of a CD containing data on 25 million British taxpayers.
- The data for over 100 million credit and debit cards was stolen through large-scale cyber fraud, resulting in numerous settlements already costing in excess of $200 million (involving TJX, Visa, Fifth Third Bancorp).
- In many countries, there are ongoing debates and court cases on whether the activities of Google StreetView are invasions of privacy.
- One prosecutor sent a computer with sensitive court case data out with the trash.
- The problems with Microsoft's Hotmail, Live! and Passport have become well-known.
- Members of an association of single women were stalked online.
- The British Home Office lost a USB stick with data on more than 250,000 participants in a major drug rehab project.
- Brothel visitors were filmed and then sent letters.
- At the British Department of Defence, a laptop went missing that contained unencrypted data on approximately 100,000 Army, Navy and Air Force personnel, including their partner data.
- The Netherlands Solicitor General used personal information obtained illegally by a credit bureau.
- At HSBC, unencrypted disks with millions of customer records were lost, and appropriate staff training was lacking (the result was a fine of over €3 million).
- An employee at T-mobile sold customer and contract data to a competitor.
- Deutsche Bahn illegally monitored its employees, leading to the highest breach of privacy fine in Germany (more than €1 million).
- The loss of backup tapes with the records of millions of policyholders resulted in a multi-million pound fine by the British regulator.
- The University of Berkeley was hacked, resulting in the data of 1.4 million Americans as well as the 160,000 students who used the medical facilities being "borrowed."
- The FIFA database of British football fans who attended the World Cup in South Africa was sold.
- A video was placed on YouTube in which a disabled person appeared without his consent.
- Personal data about online customers is solicited for spam purposes.
- Customers are approached by banks with offers of lower mortgages after these banks have run analyses of the customer's monthly mortgage interest payments at other banks.
- A free credit scoring was awarded to 17 million customers, along with a $50,000 compensation payment for each customer, due to ID theft at Countrywide Financial Corp.
- A multi-million dollar fine was levied for unsafe storage or deletion of medical data by a number of hospitals and drug-store chains in the US.
- *Etc., etc.*

Box 2: Security vs. privacy

A widespread misconception, especially among IT professionals and various security officers, is to equate security with privacy. It is often assumed that "if we have security measures in line with the Information Security Standard (e.g. ISO 27001/2), then we have also taken care of privacy." This is a misconception because security only satisfies one of seven key privacy principles (see overlap in Figure 1).

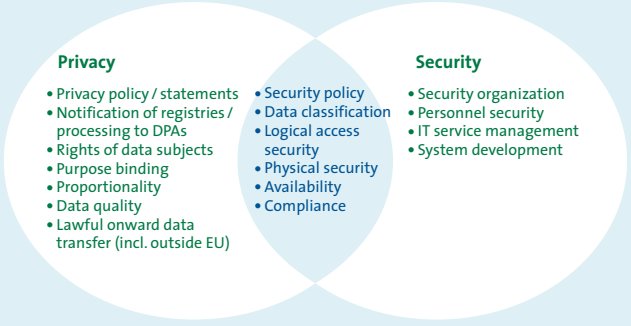

Figure 1: **Similarities and differences between security and privacy**

The legal and procedural factors concerning privacy have little or nothing to do with security. Figure 1 indicates the common factors and the distinguishing features that need to be emphasized. As suggested in this article, the challenge posed by privacy issues is applying privacy enhancing technologies that do more than improve security measures.

In addition, security and privacy require different approaches: security still focuses predominantly on building walls around large personal information databases. In contrast, privacy protection is aimed at minimizing the personal data collected and processed, while ensuring that this data is handled carefully through its lifecycle, wherever it flows or resides.

There are also situations where improving security could affect privacy. Such practices relate to the application of additional identification data, the use of biometrics and the performance of detailed background checks. The same applies to some anti-fraud and anti-terrorism measures. For this reason, there must be a new balance between security and privacy.

Evolution in approaches to privacy

After the introduction of privacy legislation, the approach to privacy issues initially focused on policy, procedural and legal factors and the adoption of traditional security measures. This consisted of the following generic steps:

- Appointment of a privacy officer for the entire organization or for each domain (HR and customer information)
- Development of a privacy policy or sometimes a privacy manual
- Inventory of personal data processing (mostly this was narrowed down to listing the personal data stored on central systems, followed by subsequent high-level clarification of the objectives and processes of these systems)
- After the enactment of privacy legislation, reporting of these systems to the appropriate data protection authorities
- Formulation and implementation of guidelines and procedures for personal data disclosure and correction, *etc.* (*e.g.* "scripts" for use in all channels of customer interaction, such as the internet, call center or reception desk)
- Inclusion of security provisions in contracts and SLAs with business partners and service providers
- Implementation of traditional security measures such as logical access and the construction of "Fort Knox walls" to protect personal data.

There are under-appreciated issues with promoting privacy awareness and with the ongoing organizational and technical challenges of implementing a privacy policy – including issues in development projects for new services and/or systems. The use of privacy procedures has gradually expanded, and it has become necessary to introduce technical measures to enforce better compliance with privacy policies. As part of this technical implementation, organizations undergoing such a transition are adding enhanced authentication procedures (based on ownership attributes), differential screening with authorization profiles, programmed inspections and integrity testing with fictitious information. Personal data sent over public networks is also increasingly being encrypted.

Current status of privacy measures

Do we now have it all together? No, since a number of privacy principles are still not organizationally or technically guaranteed. They involve issues such as:

- Execution of a Privacy Impact Assessment to indicate the effects that new services, partnerships and systems have on privacy, as well as the privacy risks that should be mitigated or reduced
- Improving the quality of personal data (partly due to data duplication and poor design of master data management)
- Integration of privacy safeguards into the information and IT architectures
- Avoidance of excessive collection or combination of data due to such factors as increased computerization and interlinking of information systems throughout organizations

- Incorporation of strict privacy clauses in IT outsourcing contracts
- Secure communication with various types of third parties (*e.g.* e-mails with attachments containing personal data)
- Constant testing with anonymous personal data without loss of representativeness
- Flexibility to cope with situations, such as some active online internet users ("digital natives") wishing to share more personal information than the rather ossified privacy legislation allows, as others paradoxically desire more (online) privacy protection while offering personal data to companies in exchange for economic benefits ([KPMG10c])
- Assigning access to data groups and individual fields containing sensitive personal data based on business roles or even on a dynamic need-to-know basis
- Logging which employees have accessed which personal data (especially of colleagues and celebrities)
- Processing of sensitive personal data either anonymously or by using pseudonyms
- Maintaining retention schedules and ensuring secure deletion and shredding of personal data (*i.e.* for eDiscovery)
- Requiring approval and records where data is provided to third parties, domestically or abroad (*i.e.* outside the EU).

Previous findings and the results of our privacy survey (see Box 4) show that there is still a great deal to be done. This section will provide further detail on a number of measures, along with a set of ingredients for an improvement plan.

In this respect, it is important to tailor all activities to the specific organization. A limited application of measures guaranteeing privacy is not necessarily bad. The measures taken must be based on a deliberate consideration of costs and benefits (economically and socially). Of course, laws and regulations should always be considered. Having insufficient measures to ensure compliance with legislation is punishable by law. It is also important to realize that managing privacy risks, like all risk management processes, is a continuous and cyclical process.

An effective risk management program for privacy should provide a mechanism by which an organization can manage privacy risks in a manner consistent with its business goals and needs, legal obligations and expectations from the market. An effective approach starts with recognizing that privacy is not only a technical issue but also a strategic PR and HR issue, involving personal data in hard-copy format (*e.g.* HR files, printouts, audio recordings, video tapes or even biometric data).

A program of privacy risk management requires combined expertise from a variety of departments and specialists (such as Legal, IT, Line Management, Security, Compliance, Marketing/Sales and Audit), and also requires professionals with experience in information risk management, business processes and privacy legislation.

It seems that external pressure in the form of stricter enforcement, higher fines and/or a publicized incident involving a privacy breach (*e.g.* large-scale identity theft) is necessary in order to place privacy on the management agenda. Pressures like these are the reasons why privacy issues have already been addressed in countries like the UK, Germany and the US. When will other countries experience similar urgency? That's what it seems to take before the public will support a powerful privacy program.

Need for privacy-enhancing technologies

In answer to most of the above issues, technical measures can be applied to limit dependence on organizational procedures and privacy awareness, while ensuring consistency. The term "privacy-enhancing technologies" (PET) is used to identify all the IT resources that can be used to protect personal data. The section entitled "Forms of PET" provides further detail about the possible PET measures that can be applied.

The application and development of "Privacy by Design" and PET is a recognizable trend. As indicated above, the technique was initially used mainly to protect previously collected personal data. Nowadays PET is also being used by a limited number of organizations to implement technical measures close to the data source and to keep the quantity of identifying data to an absolute minimum. Wherever it is not necessary, identity is not established or is disconnected from other personal information. An important essential step involves organizations becoming critically selective of the personal details that they require to provide their services. Often, more data is accumulated out of mere habit and kept much longer than is necessary or allowed. This excess data must be managed and protected, while having no use and being therefore merely a source of costs and risks. The easiest way to avoid either is to limit data collection and processing to only what is strictly required for the business purposes for which the processing is taking place. No more and no less. An important issue in this respect concerns determining if the processing of personal data ([PKIO02]):

- is necessary ("identity rich")
- is necessary to a limited extent ("identity poor"), or
- is avoidable or maintains anonymity ("identity free").

Types of privacy technologies

Well-known and widely used elementary forms of PET are logical access security and encryption. Within logical access security, it is especially important to properly manage unique-

ly identifying personal information and corresponding authorization data. An important type of PET involves the segregation of data into multiple domains. One domain contains the identifying data, the other the remaining personal information. Financial, legal or medical data may be recorded in one or more domains – separate from the domain with the identity data. The data in each domain is not privacy-sensitive because it is not traceable to an individual. In this type of PET, identity-protection software ensures that only authorized system users can access or interlink the various data domains. A variant of data segregation involves a system function verifying the details that are stored in the database, without releasing these details. The function only responds to a query by answering yes/no or indicating a specific category. Figure 2 is a simplified graphic representation of the segregation of data into multiple domains.

Further integration of data and software is produced by a type of PET in which data can be accessed by means of specific software – the so-called privacy management system. In it, the translation of regulatory policy requirements is automated. For each data element and each system function, there is an immediate check verifying whether an activity is in accordance with the policy regulations. The ultimate type of PET involves anonymizing personal data. It includes software that does not collect the identifying personal data at all, or deletes IDs when the data is no longer required – preferably immediately after collection and initial processing. Ideally, this data does not even have to be saved. Anonymization is the strongest form of personal privacy protection, which by default meets all legal requirements. Anonymization is not always applicable in situations requiring personal data, which are better served by using one of the previously mentioned forms of PET.

Figure 3 shows a PET "stairs" diagram in which the effectiveness of the protection of personal data is governed by the applied PET type. The PET stairs do not represent a growth model and need not proceed to the "overflow point." When an organization has implemented general PET measures, this does not mean that the organization must grow into "higher" levels of PET. The suitability of various types of PET is mainly dependent on the type and complexity of the information system, the desired ambition level and the sensitivity of personal data.

Broadly speaking, general PET measures are currently the most commonly applied, followed by separation of data and anonymization. The implementation of privacy management is in its infancy and is limited in scale.

PET costs

Is PET too expensive for your organization? No, there are several possible types of PET, ranging in cost. It is important to determine whether the costs associated with the solution are in proportion to the risks. Simple but powerful PET measures may bring about substantial improvement in data protection at little cost. To investigate whether a positive business case exists in your organization for the application of PET, three key questions must be answered. They are:

1. Will PET provide a significant contribution to the objectives of the organization?
2. What qualitative and quantitative benefits will PET provide in the organization?
3. What one-time and ongoing costs are required by PET?

The costs of PET can be significantly limited by taking account of privacy issues during the design stage. The quantitative and qualitative benefits of PET for the organization, society and the

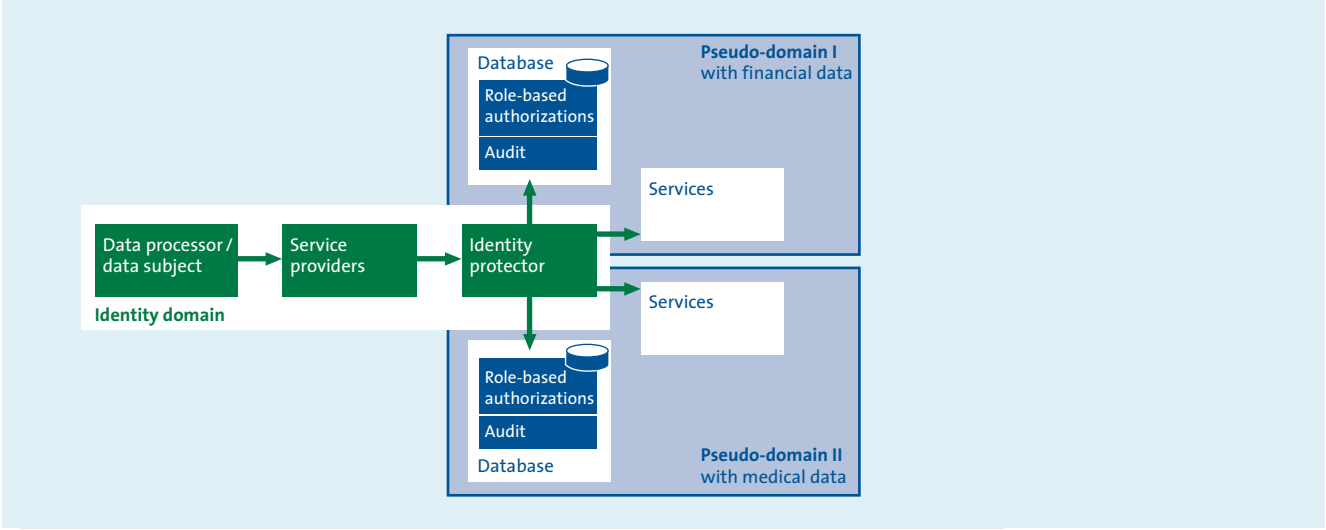

Figure 2: **Segregation of data into multiple domains with identity-protection software**

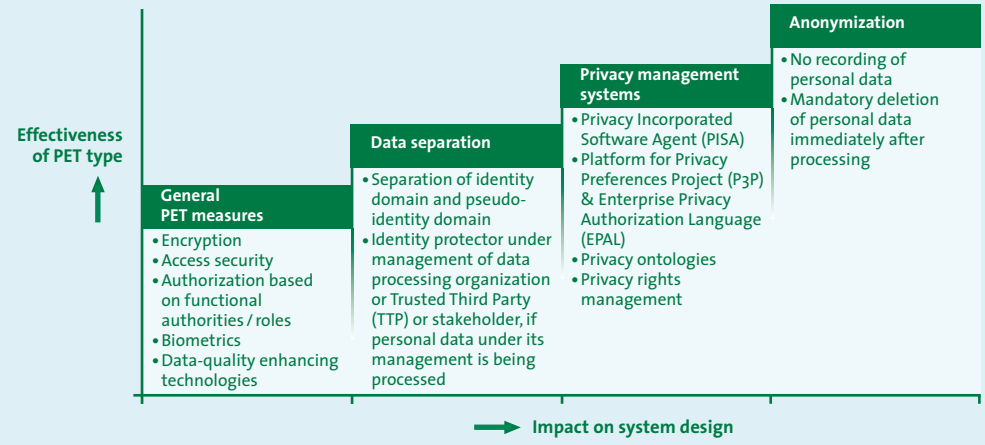

Figure 3: **PET stairs**

registered public or customers are substantial. The costs of including PET in the designs of most projects amount, on average, to only a few percent of the total budget and are therefore rapidly recovered. This relatively modest expense distinguishes them from other privacy measures that need to be incorporated into information systems after the design or development phase has been completed.

Cost levels are also affected by whether or not PET is being implemented in existing or newly developed systems. When PET is applied to existing systems, the costs are obviously higher than the costs involving new systems. The reason is that most of the costs of PET are one-off, and the one-time activities are part of the entire system development process. When PET-specific activities are retrofitted to existing systems, the latter must be adapted. As a result, certain activities are carried out twice, causing the costs of introducing PET to rise.

Implementing Privacy by Design

An important lesson from previous PET projects is that it is critical to consider the requirements for collecting personal data at a very early stage in the project. Such analysis involves determining the manner of data protection, the potential solutions and the associated costs and benefits. The subsequent

Box 3: "Privacy by Design" in Canada: IT may not just cause privacy problems but also resolve them!

Research conducted by the Alberta government demonstrated that 57% of the content in its databases consists of personal information that may directly or indirectly identify individuals. As a consequence, constructing privacy architecture within the Provincial Government of Alberta (Canada) was seen as a logical step. This constituted an extension of the existing IT infrastructure and the Government of Alberta Enterprise Architecture (GAEA). The Alberta government used this privacy architecture to achieve its privacy policy for IT and ensure that the use of advanced technology meets legal privacy requirements.
The requirements for the privacy architecture were defined in detail in meetings with the relevant policy officials responsible for IT infrastructure and industry representatives, which were organized government-wide.

The results of these workshops led to a list of twelve requirements, which were defined in detail in the policy paper on GAEA privacy architecture requirements. Not only was there an agreement about common privacy terminology, the necessary user interfaces and the use of technology to enforce the privacy policy, but also about an identity system based on meaningless but unique numbers (these numbers not being based on already existing identification numbers). These numbers reference deliberately separated personal domains that are, thus, only approachable in parts. The concept of key identification numbers is based on the deployment of identity protectors and layered identity domains. After specifying the requirements for the privacy architecture, a test model was developed that was then reviewed by the same work group. The information obtained was finally consolidated in a privacy management system, which received the HP Privacy Innovation Award.

conclusions will ensure that personal data collection is simply formulated as one of the essential (non-functional) requirements and is therefore naturally integrated into system design and development. Practical experience has certainly demonstrated that the later addition of PET into an information system is possible, but this upgrade runs sometimes deeper into the information system and underlying database than expected. In general, greater effort and higher costs are involved. And the same holds true when upgrading to advanced PET-related types and measures.

Table 1 represents the various stages that must be completed in order to successfully implement PET. PET-specific issues relating to each stage are indicated in the stage when they have to be addressed.

For an application of the Privacy by Design principle to the smart energy grid in Canada, see [IPCO10].

Future

We expect privacy and privacy-enhancing technologies to become an integral part of system development. The general public and consumers in particular demand that organizations handle personal data with great care and efficiency. Care and efficiency requires single registration at source and confidential usage throughout all the data processing stages in the system and any associated links in the information supply chain. To meet these demands and to guarantee the quality of data, organizations must make increasing use of IT solutions. In our view, the majority of governmental organizations will be the first to adopt privacy-enhancing technologies in one form or another, followed by companies that process sensitive personal data or that must comply with strict legislative and regulatory requirements (*e.g.* medical, pharmaceutical and financial sectors). The supply and demand of PET solutions will have to keep pace with these developments.

Project stage	Key issues for Privacy by Design
Purpose and need	• What personal data is absolutely needed to provide services and why is it necessary ("data minimization")? • What effect will this new or adjusted system have on privacy ("Privacy Impact Assessment")?
Data analysis and classification	• What level of data protection should be achieved, given the Privacy Impact Assessment and the personal data classification? • Will the application of PET contribute to the protection of privacy or is privacy already being safeguarded and PET therefore unnecessary? • Which type(s) of PET will be used? • What are the quantitative and qualitative costs and benefits?
High-level design	• How does data flow through the information system(s)? • What interfaces with other systems, departments and third parties exist in the information supply chain? • What is the data model for each data flow through each step of the process, from collection, saving and storage, up to and including deletion?
Detailed design	• How is the technical design of the chosen PET integrated into the technical design of the information system?
Development	• Is it necessary to specifically develop the chosen type of PET or is an appropriate standard solution available?
Testing	• Does the PET function properly as an integral component of the system? • Does the implemented type of PET meet user-friendliness requirements?
Implementation	• Does the use of PET change the way in which users must work and, if so, how are the users informed about or prepared for such changes? • Must specific tools (e.g. tokens, client software) be distributed to users and administrators?
Administration and Maintenance	• Which specific application management activities must be carried out for the privacy measures in addition to regular activities? • Will the system automatically meet the retention policy?
Evaluation	• Are the PET measures effective? • Should the information system be audited or certified? • What are the experiences of users and managers and what needs to be improved?

Table 1: **Stages in the PET implementation plan**

Conclusion

It seems that external pressure in the form of stricter enforcement, higher fines and/or a widely publicized incident of privacy breach, such as large-scale identity theft, has to come about before privacy is placed on the management agenda. Reasons like these have led to privacy issues being addressed in countries like the UK, Germany and the US. When will other countries suffer the same compulsion? Only then does it seem that there is enough support to execute a powerful privacy program.

Our privacy survey (see Box 4) indicates that organizations in both the public and private sectors experience substantial difficulties in implementing privacy measures and complying with legal provisions, even after 20 years of legislation. Nevertheless, these organizations have a positive opinion about the quality of their privacy protection. They primarily base this view on the fact that they have implemented a number of procedural and technical measures, mainly on the operational level. Framework and preparatory measures at the strategic or tactical levels are, however, often lacking.

Privacy protection is still predominantly being approached in response to compliance requirements; the positive economic effects are barely acknowledged. Furthermore, the adequacy of implemented measures are seldom evaluated. Despite many organizations believing that they are privacy compliant, it is hoped that future organizations will be able to back up such optimistic claims with privacy audits or certificates and the absence of major privacy incidents.

Implementing technical measures not only enables more effective and efficient data protection; the use of technical measures specifically requires a critical examination of personal data collection, its necessity and the need for its protection. This approach increases the integrity and confidentiality of the data and enables a more effective and efficient processing of personal data. Privacy-enhancing technologies need to become less a series of measures intended to ensure compliance with procedures and more a set of privacy provisions directly incorporated in the design of IT systems and infrastructure.

We therefore wish to conclude this article with the following high-level business case for Privacy by Design.

Privacy by Design is more than a manner of protecting personal data:

- Wanting Privacy by Design:
  - PET improves the quality of data processing.
  - Dependence on appropriate compliance with processes and procedures is reduced by automatic enforcement of privacy rules.
  - Implementation of PET can be a means of allowing the general public and customers to have better access to and control over their personal data.
  - Use of PET creates a positive image for the organization.
- Needing Privacy by Design:
  - PET can simplify compliance with privacy legislation.
  - PET creates the conditions under which the general public can trust an organization's operations.
  - PET makes it possible to process (sensitive) personal data and provide services that would not be permissible otherwise.
- Implementing Privacy by Design:
  - PET has already been frequently implemented (see sample cases in [BZK04]).
  - PET only has a limited effect on the development costs of new information systems, given that the technologies are already present. In general, it primarily "costs" the work required to conceive and design privacy-proof architectures.
- The inclusion of PET in your information (system) architecture provides a basis for efficient application of PET to your various information systems.

Box 4: KPMG Privacy Survey

In collaboration with TNS-Nipo, KPMG conducted a survey of nearly 300 organizations in the public and private sectors on privacy awareness and their approaches to privacy protection. The survey questions probed the extent to which privacy was an important concern for organizations and the manner in which they were dealing with the protection of privacy.

The most important results were:

- Organizations do not have a firm grip on the term "privacy" and do not sufficiently understand what it means to their business. This lack of understanding is caused by the complex legislation involved, the lack of time/priority and the complexity of IT. In addition, privacy and data security were often improperly regarded by respondents as synonymous (almost half of the respondents considered their information security measures as sufficient for full privacy compliance).
- Organizations are therefore particularly geared to compliance and, in general, give the impression of being mature insofar as the implementation of operational privacy measures are concerned.
- The final responsibility for privacy and activities safeguarding privacy is still greatly fragmented.
- The number of privacy incidents remains relatively high, especially in the financial and public sectors where approximately 15% of organizations suffered an identified privacy incident in the last three years. The KPMG Data Loss Barometer exhibits a similar view of data loss and identity theft ([KPMG09]).
- More than of half of the surveyed organizations are monitoring employee e-mail or internet traffic.
- The potential "economic value" of privacy (*e.g.* the benefits that the creation of customer profiles can have) is insufficiently explained. This means that organizations are likely still missing the opportunities that the adequate handling of personal data could deliver (see [KPMG01]).
- Two thirds of the surveyed organizations believe that they are currently in compliance with privacy laws, although they scarcely assess the extent to which they have implemented privacy safeguards and measures.

The survey results are reported in detail in [KPMG10d].

Box 5: Sample step-by-step privacy plan

As noted earlier, it is important to recognize that the management of privacy risks is a continuous and cyclical process. An effective approach starts with recognizing that privacy protection is not an IT issue but that it also has strategic and tactical importance for all customer and HR data in electronic and paper format.

The following steps can help to safeguard privacy within an organization. They need not be implemented in the indicated order, as the sequence depends on the existing level of information governance and privacy maturity.

Step 1: Ensure that sponsorship and leadership involves senior management. Though a standard recommendation, privacy will remain condemned to being a merely legal or IT security project unless it garners support from senior (line) management. Sufficient support will ensure adequate funding and continuity. In many cases, this means that a General Counsel or Compliance Officer will have to stimulate management to act. In other cases, the introduction and implementation of a substantial transformation (*e.g.* a system consolidation involving several countries and business domains) will provide a stimulus for investment in privacy.

Step 2: Appoint a project manager (preferably not a lawyer!). Provide this project with sufficient resources and accumulated expertise. Identify key personnel and data owners in various areas of the organization (Line Management, HR, Marketing/Sales, Legal Office, Information Security, Audit) who will participate in the project. The selected groups should consist of professionals with experience in business processes, customer service, information/IT risk management and privacy laws.

Step 3: List and classify the personal data that is currently being collected. Fully understand why the organization is collecting, using and/or transferring various types of personal data. All these activities must be part of the organization-wide information lifecycle management processes. Other important questions are: Does the current personal data collection satisfy the current need, or is more personal data accumulated and retained than is actually required? How do we handle private employee data in the work environment (*e.g.* social networking, private e-mail, telephone / PDA use, *etc.*)?

Step 4: Identify and analyze the methods used to collect personal data. This step may be executed simultaneously with the previous one, and entails analyzing websites, applications, registrations, marketing campaigns, acquisition of marketing databases containing personal information, *etc.* Identify how and with which means the members of the general public, customers or employees have been informed and have granted consent for processing.

Step 5: Perform a Privacy Impact Assessment. After analyzing the data being collected, data flows and data management processes, a Privacy Impact Assessment can be performed to identify privacy risks. The process involves the following assessments.

- What precisely is meant by privacy and privacy protection, and what do the context, legal privacy requirements and privacy demands from internal and external stakeholders mean to the organization?
- What are the threats and opportunities (what it could cost the organization and what benefits it might provide); see [KPMG01] for a discussion about the upside of privacy, the opportunities?
- How can all these issues be translated into a concrete approach encompassing strategic, tactical and operational levels?

Various governmental bodies, boards of standards and data protection authorities are currently developing or even imposing Privacy Impact Assessments (including several agencies in Canada, Australia, Hong Kong, New Zealand and the UK, see for instance [ICO09] and [ISOT08]).[3]

Step 6: Appoint a privacy officer, and an organization-wide privacy governance having enough authority to address privacy issues throughout the organization.

Step 7: Develop an organization-wide privacy policy and translate it into organizational, procedural and technical measures (a "Privacy Control Framework"). Ensure that employees and customers are aware of this policy and the procedures involved, and that they understand their implications. Decide whether model contracts, safe harbor or binding corporate rules are preferred solutions for global data exchange. Embed privacy into regular governance and compliance (reporting) processes.

Step 8: Train employees, including management. Train both current and new employees, without neglecting contracted personnel. Pay specific attention to individuals who have frequent contact with customers and access to sensitive data.

Step 9: Make sure that personal data is secure. Personal information stored electronically, filed as paperwork or involved in internal and external communications must be secured to a technically sophisticated extent, and protected against unauthorized or unwanted access (in line with classification from step 3).

Step 10: Ensure that third parties and suppliers are also privacy compliant. Ascertain that they provide at least the same level of protection and can provide material evidence or independent assurance of this fact.

Step 11: Review and improve privacy protection, use privacy audits to ascertain the level of protection, raise awareness, further strengthen the privacy control framework implemented, and communicate a privacy certificate externally.

3 Some privacy impact assessments are merely compliance assessments concerned with meeting the requirements stipulated in privacy legislation. A proper privacy impact assessment should also consider the privacy effects of new services and systems on customers, employees and the general public.

References

[BZK04] Netherlands Ministry of External Affairs, *Privacy Enhancing Technologies for Decision-makers*, 2004 (http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf).

[EPIC06] EPIC/Global Internet Liberty Campaign/Privacy International, *Privacy and Human Rights: An international survey of privacy laws and practices*, 2006 (http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559458).

[ICO09] ICO (Information Commissioner's Office), *Privacy Impact Assessment Handbook*, 2009 (http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html).

[IPCO10] Information and Privacy Commissioner of Ontario, Hydro One and Toronto Hydro Corporation, *Privacy by Design – The Gold Standard Best Practices for the Smart Grid*, June 2010 (http://www.ipc.on.ca/site_documents/achieve-goldstnd_execsumm.pdf).

[ISOT08] ISO TC68/SC7, ISO 22307:2008 *Financial Services – Privacy impact assessment*, 2008.

[Koor01] Koorn, R.F. and M. Dontje, *Internationale privacyaspecten en de Wbp*, Compact 2001/4 (publication in Dutch).

[KPMG01] KPMG, *A New Covenant with Stakeholders: Privacy as a competitive advantage*, 2001 (http://aci.kpmg.com.hk/docs/evolving%20issues/managing%20privacy.pdf).

[KPMG09] KPMG, *Data Loss Barometer, Insights into Lost and Stolen Information*, Issue 2, 2009 (http://www.datalossbarometer.com).

[KPMG10a] KPMG 2010 Cloud Computing survey: *From Hype to Future*, 2010 (http://www.kpmg.com/NL/nl/IssuesAndInsights/ArticlesPublications/Pages/FromHypetoFuture.aspx).

[KPMG10b] KPMG, *Data Protection and Privacy Issues in Online Advertising*, Issues Brief, 2010 (http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/flashpoint-data-protection-privacy-brief.pdf).

[KPMG10c] KPMG, Consumers-Convergence-IV , July 2010 (http://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Documents/Consumers-Convergence-IV-july-2010.pdf).

[KPMG10d] KPMG, *Privacy Protection: unconscious incompetence*, white paper, 2010.

[PKIO02] Logius/PKIoverheid, *PET en de PKI voor de overheid*, November 2002 (publication in Dutch).