Chapter 15
Why Adopting Privacy Enhancing Technologies (PETs) Takes so Much Time

John J. Borking

15.1 About PETs and the Research Questions

Article 17 (1) of the Directive 95/46/EC (DPD) requires that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

> The Directive states, that *(. . .) such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.*[1]

The requirements referred to in the DPD must be implemented efficiently in the organization in order to give proper support to the citizen's right to privacy with respect to personal data. It is therefore important to devise a proper system of general processing measures and procedures that should be present in order to protect company processes and in connection with specific protective measures for the processing of personal data. Given the basic legal requirements for privacy protection and the risks of privacy incidents, it will be apparent that, if technical provisions are to be deemed adequate, they must go beyond the implementation of traditional security measures.

ICT offers solutions in the shape of privacy protection for users, consumers and citizens. The application of ICT to protect privacy has become widely known under the name Privacy-Enhancing Technologies (PET or PETs). PETs have been defined as a coherent system of ICT measures that protects privacy by eliminating

J.J. Borking (✉)
Borking Consultancy, Wassenaar, The Netherlands
e-mail: jborking@xs4all.nl

Dr. John J. Borking (1945) is owner/director of Borking Consultancy in Wassenaar The Netherlands and was a former privacy commissioner and board member of the Dutch Data Protection Authority. Address: Lange Kerkdam 27, 2242 BN Wassenaar, Netherlands; email: jborking@xs4all.nl

[1] Directive 95/46/EC, Official Journal L 281, 23/11/1995 P. 0031–0050.

S. Gutwirth et al. (eds.), *Computers, Privacy and Data Protection: an Element of Choice*, DOI 10.1007/978-94-007-0641-5_15, © Springer Science+Business Media B.V. 2011

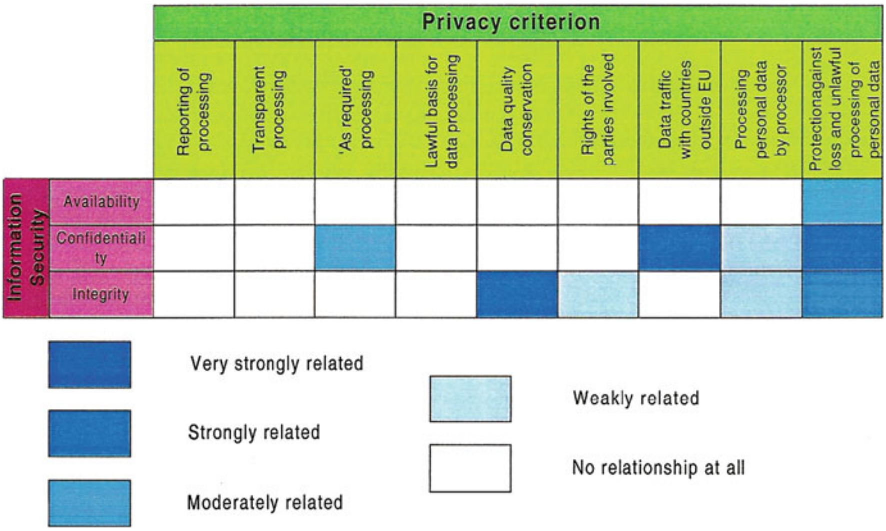
or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system (Borking, 2003; Hes and Borking, 2000; Van Blarkom et al., 2003; Communication from the Commission to the European Parliament and the Council on Promoting Data Protection, 2007). PETs are about technologies that *enhance* privacy and privacy protection is neither an equivalent of information security or confidentiality. The overlap and difference between privacy and information security and confidentiality, is visualised in the following Fig. 15.1.

PETs have to be used for implementing the legal specifications in the EU privacy directives 95/46/EC and 2002/58/EC, like data minimization, consent requirements, access rights of data subject, privacy safe construction of terminals in information systems (Borking, 2010).

PETs can guarantee data protection without making excessive demands on the processing of the data. By applying PETs and streamlining personal data processing, the organizations can continue to meet the high public expectations with respect to services and dealing with personal data (Koorn et al., 2004).

In Fig. 15.2, the different PETs options are positioned in relation to the effectiveness of the data protection. The diagram also shows the most important features of the different PETs options. The PETs staircase is not a growth model and does not have to be followed to the top. Once an organization has applied general PETs controls, it does not mean that it has to go on to "higher" levels of PETs. The suitability of the different PETs options depends on the individual situation.

The basic driver to invest in PETs is their potential to avoid privacy incidents and so to reduce the risks and subsequently the damage caused by privacy breaches.



		Privacy criterion								
		Reporting of processing	Transparent processing	'As required' processing	Lawful basis for data processing	Data quality conservation	Rights of the parties involved	Data traffic with countries outside EU	Processing personal data by processor	Protectionagainst loss and unlawful processing of personal data
Information Security	Availability	□	□	□	□	□	□	□	□	▒
	Confidentiali ty	□	□	▒	□	□	□	▓	░	█
	Integrity	□	□	□	□	█	░	□	░	▓

█	Very strongly related	░	Weakly related
▓	Strongly related	□	No relationship at all
▒	Moderately related		

Fig. 15.1 Differences between privacy protection, information security and confidentiality (Borking, 2010)

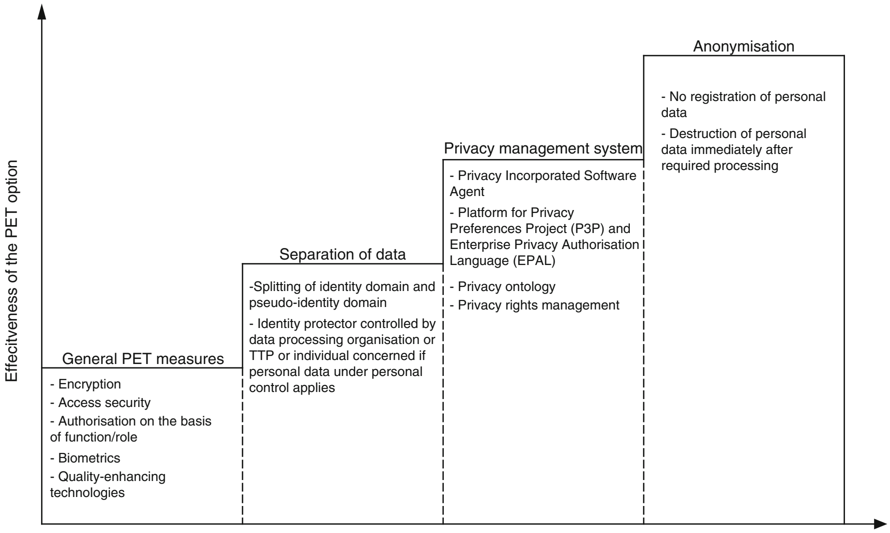

Effectiveness of the PET option
General PET measures
- Encryption
- Access security
- Authorisation on the basis of function/role
- Biometrics
- Quality-enhancing technologies
Separation of data
-Splitting of identity domain and pseudo-identity domain
- Identity protector controlled by data processing organisation or TTP or individual concerned if personal data under personal control applies
Privacy management system
- Privacy Incorporated Software Agent
- Platform for Privacy Preferences Project (P3P) and Enterprise Privacy Authorisation Language (EPAL)
- Privacy ontology
- Privacy rights management
Anonymisation
- No registration of personal data
- Destruction of personal data immediately after required processing

Fig 15.2 PETs staircase: the effectiveness of the different PETs options (Koorn et al., 2004)

In general terms a privacy incident can be defined as an event in which personal data are misused, because of the fact that personal data accompanied by a list with personal data constraints haven't been respected. The amended directive 2002/58/EC describes it as "'*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data, transmitted, stored or otherwise processed [. . .]*".

Privacy breaches may impact an organization in different ways. Tsiakis and Stephanides distinguish direct, short-term, and long-term economic consequences (Tsiakis and Stephanides, 2005). Direct consequences are the costs for repairing or changing systems, costs of stopping or slowing down production or processes, costs of legal action. Short term consequences comprise the loss of existing customers, contractual relations, and the loss of reputation. Companies may loose business because of privacy breaches, which harm their trust relationships with customers and other business relations. Safeguarding privacy has been identified as a major component of building trust (Camp and Wolfram, 2000). Long term consequences include the loss of stock value and market value. An example of the latter is DoubleClick in 2000. After a serious violation of their existing privacy statement on their website and the lawsuit that was the result of this violation, their stock declined with 20% (Chapman and Dhillon, 2002). This also occurred with Choicepoint after their public announcement that they were hacked, and approximately 10 million data records were stolen. Their stock declined with 17% since the data breach (Privacy Rights Clearinghouse, 2007).

Cas and Hafskjold wrote in 2006: *So far PETs have not contributed as much as would be possible to the protection of privacy; partly because of a lack of* *availability of PETs, partly because of a lack of user friendliness*. (Cas and Hafskjold 2006)

Leisner and Cas in 2006 further pointed out that *PETs are insufficiently supported by current regulations; in particular it is not compulsory to provide the option of anonymous access to services or infrastructures*. (Leisner and Cas 2006) Sommer remarked *We still face major obstacles towards a deployment of such (PETs) technology in the field at a large scale (. . .) the part of convincing business to design their business processes in a way such that data minimization can be implemented as envisioned in PRIME will even be harder than has been the technological part*. (Sommer 2008)

However it isn't the user friendliness or the lack of availability of PETs, but there are other reasons why PETs aren't used by governmental or commercial organizations.

A group researchers (Bos, 2006), Borking, Dijkman, Fairchild, Hosein, Ribbers and Tseng have focused in the PRIME project, (Fairchild and Ribbers, 2008) on what business drivers lead organizations to adopt privacy enhancing technologies (PETs) for providing assurance for privacy.

The central research questions were:

- When starts an organization bothering about privacy?
- What factors impact the adoption of privacy-enhancing technologies tools in information systems as a measure to protect privacy sensitive data, and how do these factors affect the adoption decision?
- What are the drivers and inhibitors for adoption by organizations of PETs?

15.2 Technological Innovations

The capability of an organization to innovate or to apply an innovation is important in today's competitive environment (Tidd et al., 2005). If an organization lacks this capability it will fail to apply necessary transformations, to introduce innovation and as a result may create a competitive disadvantage.

An innovation is generally defined as the application of something new. According to Rogers (2003) the question whether something new is an innovation has to be considered from a relative point of view. Something that in a particular environment or by a particular person is subjectively perceived as new can be regarded as an innovation. An innovation can also be related to many things, like an idea, a method, a technology or a product. Each of these types of innovations has its characteristics, which play a role in the adoption process.

Given the innovative character of ICT, research of innovation in particular technical innovations, tends to focus on technological innovations like software or electronic services (Tidd et al., 2005). The OECD defines technological innovation as:

> a technological new product or process that includes a significant improvement and has been actually put into use. The technological new product or process consists of a variety of scientific, technical, organizational, financial and commercial aspects. OECD (2005)

PETs, given the relative recent introduction of the concept (Borking, 2003; Hes and Borking, 2000; Van Blarkom et al., 2003; Communication from the Commission to the European Parliament and the Council on Promoting Data Protection, 2007), the progress that is being realized with its application, and the new approach they offer with regard to privacy protection can be regarded as innovation.

The requirements referred to in the DPD must be implemented efficiently in the organization in order to give proper support to the citizen's right to privacy with respect to personal data. It is therefore important to devise a proper system of general processing measures and procedures that should be present in order to protect company processes and in connection with specific protective measures for the processing of personal data. The restrictions that the organization of information systems can impose on the possibility that their users can comply with privacy legislation are evident. One simple example is where a system contains an inescapable "date of birth" field, while analysis of the company's processes shows that recording the birth date of all persons included in the system is excessive. System design can just as easily ensure that users correctly observe the law. As a rule, privacy protection will constitute a supplementary system of measures and procedures in addition to the usual processing and security measures, but it should be assigned a significant place in management processes in order to implement and maintain a balanced processing policy for personal data.

When an organization is asked what it has done to protect privacy, it is apt to emphasize the personal data security measures it has in place. Although the use of safeguards to prevent unauthorized access to personal data is an important aspect of privacy protection, it is not sufficient in its own right. This is because such safeguards rarely involve the encryption of stored data; consequently, effective protection depends entirely on the security measures being correctly implemented and functioning properly.

It is therefore preferable to take technical measures that protect the individual's privacy at the point of data collection. Such measures may do away with the need to generate or record any personal data at all. Alternatively, they may minimize or even obviate the need to use or store identification data.

Given the basic legal requirements for privacy protection and the risks of privacy incidents, it will be apparent that, if technical provisions are to be deemed adequate, they must go beyond the implementation of traditional security measures.

15.3 Diffusion and Adoption of Technological Innovations

A central theme in the research on innovation is in particular the way technological innovations are spread in a specific environment and how subsequently these innovations are being accepted and utilized. This area is known as "diffusion and adoption" (Fichman 1992). Diffusion relates to how innovations are spread across a specific society or industry. Adoption is defined as the process through which a person or organization evolves from first getting acquainted with the innovation till its eventual utilization (Rogers 2003).

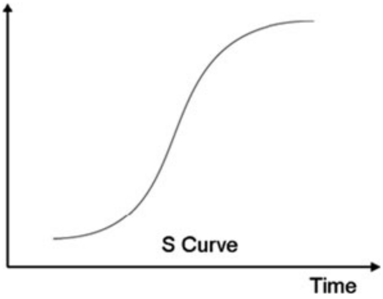


Fig. 15.3 Rate of adoption (Rogers, 2003)

In the study of diffusion and adoption many studies try to identify relevant impacting factors, so that predictive statements can be made (Jeyaraj et al., 2006).

Rogers (2003) considers adoption and diffusion as a process with a relatively known and constant pattern of evolution. He describes the rate of adoption as an S-shaped curve. See Fig. 15.3.

The idea of the S-shaped curve (limited interest for the innovation in the beginning, followed by an increased interest leading to an intensified use, which eventually will level off) applies to all types of adoption. Others, who state that also partial adoption, as a middle road between adoption and non-adoption, is a viable possibility, have supplemented Rogers' ideas; this reduces the contrast between adoption and non-adoption (Bayer and Melone, 1989).

15.4 Factors of Organizational Adoption of Technological Innovations

Rogers distinguishes various variables that influence the process of adoption of innovations. First he describes characteristics of the innovation itself: relative advantage or benefit, compatibility, complexity, testability, and visibility of the innovation. He also points their impact is determined by the perception of these factors by the potential adopter, and not so much by how they are in reality. Next he distinguishes various variables that characterize the organizations, which are open to adopt innovation: the general attitude of top management with regard to change, centralization, complexity, formalization, internal relatedness, organizational slack, size and openness of the organization to the environment.

Rogers' Diffusion of Innovation [DOI] Theory has gained quite a broad acceptance; the variables have been tested in multiple studies and found relevant. Also Fichman (1992) and Jeyarai et al. (2006) found that three clusters of factors explain the organizational adoption behavior: factors related to the technological innovation, to the adopting organization, and to the environment of both former factors. They investigated over a hundred variables that have been researched in different studies. They also performed an empirical test on the best predicting factors for the organizational adoption of IT-based innovations. Combined in clusters the dominant factors

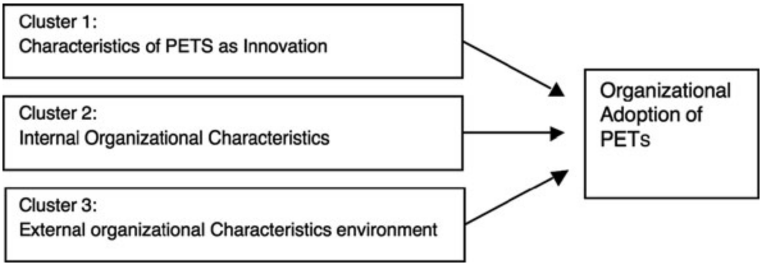

Cluster 1:
Characteristics of PETS as Innovation
Cluster 2:
Internal Organizational Characteristics
Cluster 3:
External organizational Characteristics environment
Organizational Adoption of PETs

Fig. 15.4 Conceptual model (Fairchild and Ribbers, 2008; Bos, 2006)

appear to be those related to innovation characteristics, organizational characteristics, and environmental characteristics. Tung and Reck (2005) reach this conclusion in their study.

Others have emphasized other influences on the adoption process: Fichman (1992) argues that adoption of IT based innovations requires a different approach. Fichman (1992), Rivera and Rogers (2004) and Greenhalgh et al. (2004) point to specific effects of innovations in network organizations on inter-organizational relationships. The approaches of Jearay, Fichman and Rogers form the foundation for the Conceptual Model shown in Fig. 15.4.

The first cluster of factors encompasses those variables that are related to the technical innovation itself, and so to PETs. The second cluster looks at those variables that are related to the internal characteristics of the adopting organization. The third cluster contains factors related to the environment of the adopting organization and innovation. In case of PETs, in particular privacy policies and regulations, and level of enforcement seem to be particularly relevant.

15.5 Specific Characteristics

Rogers (2003) and Fichman (1992) distinguishes five innovation characteristics and eight organizational characteristics, which affect the organizational adoption of innovations.

15.5.1 Innovation Characteristics

Relative advantage or benefit (+): the advantage offered by the innovation, compared to the former practice or technology.

Compatibility (+): The extent that an innovation resembles its predecessor.

Complexity (–): The effort needed to learn how to use the innovation.

Testability (+): The extent that small-scale experiments with the innovation are possible.

Visibility (+): the extent to which the innovation is visible for the outside world.

15.5.2 Organizational Characteristics

Top Management's attitude with regard to change: How open is top management to accept the changes that accompany the innovation?

Centralization: The degree of concentration of power and management.

Internal Organization complexity: The extent that members of an organization possess specialized knowledge and expertise.

Formalization: The level of bureaucracy in an organization.

Internal relatedness: The extent that internal members of the organization are interrelated.

Organizational slack: The extent that an organization possesses uncommitted resources.

Size: The size of the organization.

Openness: The degree that organizations are in contact with other organizations.

15.6 Encompassing Model

Fichman (1992) compared different adoption studies and built an encompassing model that explains organizational adoption of complex information technology innovations. The model consists of three clusters, while each cluster contains a few groups of factors.

The three clusters are:

a. The Technology and Organization combination;
b. The Technologies and Diffusion environments;
c. The Organizations and Adoption environments.

The Technology and Organization Combination cluster stands for factors that describe the relationship between the innovation and a specific organization. This boils down to the fit between the innovation and the organization, the perception of organizational characteristics and factors that describe the possibilities for an organization to implement the innovation.

The Technologies and Diffusion environments cluster regards those factors that describe the innovation and the specific environment from which they emanate. These are in particular the innovation characteristics and possible roles of advising institutions.

The Organizations and Adoption environments cluster deals with factors that describe the adopting organization and their environment. These are organizational characteristics and characteristics of the environment and industry.

15.7 Interviews with Experts

In order to find variables that characterize each cluster, literature analysis has been combined with expert interviews (2006–2007). Factors that have been proposed to be relevant in the literature have been compared with the results of expert interviews, and vice versa. Five experts in the field of PETs have been interviewed (Bos, 2006) and 4 workshops have been held in Sweden, UK, Netherlands and Switzerland (Fairchild and Ribbers, 2008). In the workshops representatives of a broad range of industries participated. The results of the interviews are presented below. The variables mentioned by the experts and organizations have been grouped according to the categories innovation, internal organization and environment (Fairchild and Ribbers, 2005; Bos, 2006).

Factor: Innovation

Relative benefit:	Positive
Compatibility	Negative
Complexity:	Negative
Costs:	Negative[2]
Testability:	Positive
Role of advisory institutions:	Positive
Social recognition:	Positive
PETs woven into business processes:	Negative

Factor: Internal Organization

Top Management's attitude towards change caused by PETs:	Positive and Negative
Structure and Size of the organization:	Negative
Complexity of organizational processes:	Negative
Presence of key persons:	Positive
Ties with advisory institutions:	Positive
Perception and level of awareness of privacy regulations:	Positive
Diversity of information systems:	Negative
Type of the data processed:	Positive

Factor: Environment

External pressure by privacy laws:	Positive
Complexity of privacy laws:	Negative
Existing offer of PETs measures:	Positive
Visibility:	Positive

15.8 Explanations of the Terms

The terms mentioned under the factors innovation, internal organization and environment are explained hereunder.

[2] When showing the results of calculating the Return On Investment on PETs investments some participants showed a positive attitude change towards adoption (Borking, 2008).

15.8.1 Relative Benefit

The advantage of PETs is that it offers a clear privacy protection, which, when properly applied, is in line with legal requirements. The potential relative benefit compared to other protective measures is big. It however appears to be difficult to value in economic terms the relative benefits of PETs compared to other protective measures. This is caused by the existing ambiguity around PETs and privacy. As a result, often more conventional measures are chosen instead. Calculating the ROI on privacy/PETs investment leads to more clarity.

15.8.2 Compatibility

Only when PETs resembles its predecessor the effect is positive.

15.8.3 Complexity

PETs have been perceived as a complex innovation. The implementation of PETs requires specific expertise in different disciplines. Except IT expertise also legal expertise is needed; this combination of is very scarce and has to be acquired externally.

15.8.4 Costs

PETs have been considered as an expensive innovation (with unclear benefits). Much depends however on the moment that PETs is introduced. If the introduction is when a new information system is put into use and directly integrated into this I.S, then costs are generally at an acceptable level. This is also basically the only realistic option. PETs are simply too complex to apply to existing systems, costs are then being perceived as higher than those of traditional measures.

15.8.5 Testability

The extent that small-scale experiments with PETs are possible is perceived as positive

15.8.6 Role of Advisory Institutions

Some organizations can play a key role in the diffusion of innovations. The Dutch Data Protection Authority has assumed this role with regard to PETs in the past till

2002, especially when giving advices with regard to large projects. This role and the attention given to PETs have impacted its adoption. At the moment the Dutch DPA does not get actively involved in the design of information systems anymore advising the use of PETs, with a lower rate of adoption as a result.

15.8.7 Social Recognition

The use of PETs does not receive a lot social recognition, which is the result of its limited visibility. Also privacy protection is not an issue with which organizations try to differentiate themselves unless it is a USP. The market for privacy protection is not transparent.

15.8.8 PETs Woven into Business Processes

An important characteristic of PETs is that its implementation requires integration in information systems. This requires a combination of legal and technical (ICT) expertise, which is hard to find.

15.8.9 Top Management's Attitude Towards Change Caused by PETs

If management is open to accept the changes that accompany PETs then it is seen as positive.

15.8.10 Structure and Size of the Organization

Contrary to the literature the interviews showed that large organizations aren't more positive about PETs than smaller ones.

15.8.11 Complexity of Organizational Processes

PETs-measures usually have to be customized for a specific organization or process. The more complex this is, the more difficult it is to implement PETs.

15.8.12 Presence of Key Persons

The utilization of PETs often depends on specific key persons in an organization, who know the concept and take the lead in the adoption process. Such a person has a strong impact on the adoption of PETs.

15.8.13 Ties with Advisory Institutions

The use of PETs sometimes depends on the ties that an organization has with advisory institutions (e.g. DPA). An organization that has no links with such institutions is not likely to put PETs into use.

15.8.14 Perception and Level of Awareness of Privacy Regulations

Privacy standards (norms) are often not perceived as being very important for business processes; also the consequences of not complying with the law aren't considered generally as important as the change to be caught when violating the privacy legislation is considered to be very low. As a result the adoption of PETs is in most organizations not high on the management agenda. However in the interviews with multinationals in the field of consumer electronics, energy, banking and telecommunications the pressure of privacy legislation is considered as relevant.

15.8.15 Diversity of Information Systems

The more diversity of information systems in organizations, the less likely PETs will be introduced in the organization.

15.8.16 Type of Processed Data

When the level of risk associated with privacy breaches is high, then there is a bigger incentive to apply PETs.

15.8.17 Pressure by Privacy Laws

Privacy laws exert little pressure on organizations to really put PETs into use. Only in a few cases the law refers to PETs, however the decision makers are left free what to choose as protective measures.

Management of the interviewed organizations considers the EU privacy directives as of a too general and abstract character. In general there is little awareness of PETs. The focus of decision makers is on the key business processes; privacy is often a secondary issue. However the interest for privacy is increasing. The Commission's Communication on promoting Data Protection by Privacy Enhancing Technologies (PETs) (COM (2007) 228 Final, Brussels, 2.5.2007) is viewed as a positive stimulus. A mandatory requirement to use PETs is felt by the stakeholders as necessary. There is also very limited demand for privacy audits, because there is no felt need to have one unless the audit results in a visible result, like obtaining the EuroPrise[3] privacy certificate (seal). At its essence, EuroPrise (from the Independent Centre for Privacy Protection Schleswig-Holstein with Accredited EuroPriSe Legal and/or Technical Experts) is a voluntary certification program by which any company or individual could: (a) Gain assurance that its product or service is in compliance with EU data protection laws, and (b) Send a message to the marketplace and to consumers (end-users) stating: We take user's privacy seriously. EuroPrise states on its website www.european-privacy-seal.eu/ that this privacy certificate aims to facilitate an increase of market transparency for privacy relevant products and an enlargement of the market for Privacy Enhancing Technologies and finally an increase of trust in IT.

15.8.18 Complexity of Privacy Laws

Organizations often do not know/understand what privacy laws require them to do. Because privacy laws are overly complex and ambiguous, they do not use the right set of protective measures.

15.8.19 Existing Offer of PETs Measures

The lack of PETs-measures have a negative influence on the adoption of PETs, especially as many organizations are using standard package software in which PETs-measures haven't been foreseen. When PETs measures can be applied in an organization (like anonymization or privacy management systems) are available then it is a positive factor.

15.8.20 Visibility

When PETs in systems and services can be proven by privacy seals/certificates then it is a positive factor

15.9 Summary of the Results

A number of factors are perceived to have a negative impact on the adoption process. Decision makers assume is that PETs are difficult to implement efficiently and effectively. Also the internal organizational characteristics have a negative impact.

[3] EuroPrise (privacy seals) has been subsidized by EU Commission under the eTEN Programme. The EuroPrise project started op June 10 2007 and ended February 28, 2009. http://www.european-privacy-seal.eu/about-europrise/fact-sheet.

Although there is enough code developed, the limited offer of PETs tools by software suppliers appears to have a negative impact. Only the legal and regulatory pressure with regard to privacy protection has an undivided positive impact on the adoption process. However, the existing legislation provides too little reference to the concept of PETs, to make a difference in the adoption process. The promotion by advisory bodies appears to have a strong positive influence.

A conclusion of this study is that the adoption of PETs is problematic (Bos, 2006). There are only of a limited use. Looking at the conceptual model (Fig. 15.3), in particular those factors that are related to regulatory and legal compliance, to improved coordination and advice and information with regard to PETs, seem to help to solve this problem. The relative advantage of PETs is perceived by SMEs to be zero. However in interviews with large international organizations the use of PETs in relation to preventing reputation damage is seen as positive. Both educational activities and adaptation of the law seem to be necessary. Legal requirements are generally observed; however in privacy laws there is insufficient reference to PETs. Also the minimum level of privacy protection required by the law is perceived as insufficient for constituting an incentive to apply PETs (Fairchild and Ribbers, 2008).

15.10 Identity and Access Management (Iam) Maturity Model

To examine under what conditions an organization would adopt PETs into its business process, researchers explored how an IAM maturity model can be adapted to examine privacy adoption maturity in organizations. The hypothesis behind the choice for the IAM maturity model is that as protection of personal data is closely linked with identity issues, the increased attention for identity in the organizational processes must lead to the awareness of informational privacy.

> A maturity model is defined as *a staged structure of maturity levels, which defines the extent to which a specific process is defined, managed, measured, controlled and/or effective, assuming the organization develops and adopts new processes and practices, from which it learns, optimizes and moves on to the next level, until the desired level is reached.* Smit (2005)

During the last decade several maturity models have been developed in specific research areas such as business IT alignment, software development and information security. All of these models have one thing in common; they all describe the maturity of one or more processes within an organization. As a basis for this IAM maturity model, a number of existing models were examined. The descriptions of these maturity levels differ among the models, but are quite similar in general. Every model characterizes the first maturity phase as being chaotic and dealing with processes on an ad hoc basis. The second one is characterized by the planning of processes. The third maturity level is characterized by the implementation of standards aimed at particular processes and outputs for processes are defined. Quantitative management characterizes the fourth maturity level.

Processes and quality are controlled based on quantitative measures. Based on the measures taken out of the quantitative measures implemented in maturity level four, maturity level five improves the organization. These improvements are continuous, incremental and connected to the business objectives' measures (Bos, 2006; Fagerberg et al., 2005; Stanford Organizational Maturity Levels; Vandecasteele and Moerland, 2001). The following general phase descriptions can be discerned:

Phase 1: Only few processes have been defined and processes are conducted on an ad hoc base.

Phase 2: Processes that seem to work and be in order are repeated.

Phase 3: Processes are standardized and documented to review if they are executed accordingly.

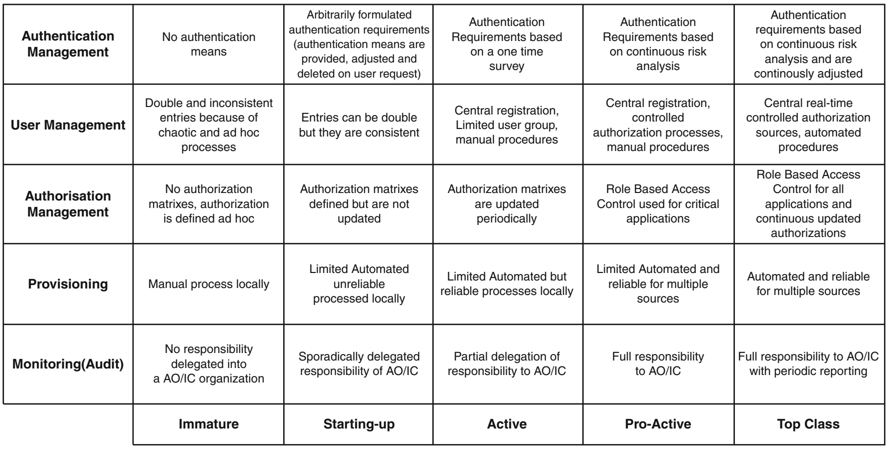
Phase 4: Performance and success are measured and quality measures are done

Phase 5: Processes are systematically improved with the help of quantitative feedback of results, test results and innovative ideas.

Based on a KPMG (Vandecasteele and Moerland, 2001) model, researchers then integrated maturity phases into these processes, and developed an IAM maturity model shown below (Fig. 15.5):

The filled out maturity model can in turn be translated into a more general description of maturity phases for IAM in general. This means that the whole IAM situation is described per maturity phase. Describing the situation in general leads to a more practical and understandable image of the Identity and access management processes.

Through all of these five maturity phases the awareness and importance of IAM processes increases within the organization (Van Gestel, 2007). The organization



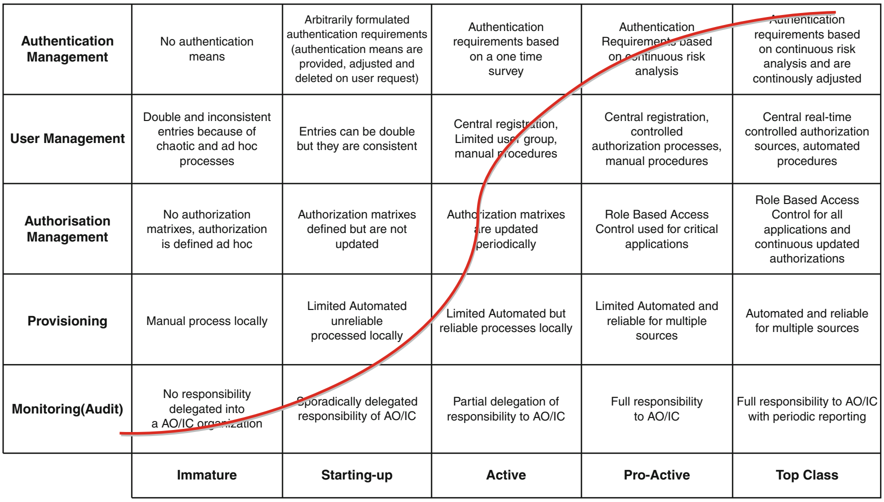
Authentication Management	No authentication means	Arbitrarily formulated authentication requirements (authentication means are provided, adjusted and deleted on user request)	Authentication Requirements based on a one time survey	Authentication Requirements based on continuous risk analysis	Authentication requirements based on continuous risk analysis and are continously adjusted
User Management	Double and inconsistent entries because of chaotic and ad hoc processes	Entries can be double but they are consistent	Central registration, Limited user group, manual procedures	Central registration, controlled authorization processes, manual procedures	Central real-time controlled authorization sources, automated procedures
Authorisation Management	No authorization matrixes, authorization is defined ad hoc	Authorization matrixes defined but are not updated	Authorization matrixes are updated periodically	Role Based Access Control used for critical applications	Role Based Access Control for all applications and continuous updated authorizations
Provisioning	Manual process locally	Limited Automated unreliable processed locally	Limited Automated but reliable processes locally	Limited Automated and reliable for multiple sources	Automated and reliable for multiple sources
Monitoring(Audit)	No responsibility delegated into a AO/IC organization	Sporadically delegated responsibility of AO/IC	Partial delegation of responsibility to AO/IC	Full responsibility to AO/IC	Full responsibility to AO/IC with periodic reporting
	Immature	**Starting-up**	**Active**	**Pro-Active**	**Top Class**

Fig. 15.5 Conceptual identity and access management (IAM) maturity model (Fairchild and Ribbers, 2008)

going through all these sequential phases not only needs to adjust its identity and access management processes, but also its own organizational structure and policies need to be adjusted. These adjustments like the adjustments to the IAM processes need to be evolutionary not revolutionary. Since IAM can entail the creation of roles or positions within the existing organizational structure, the impact of an IAM implementation can be quite significant. In order to deal with these changes the organization needs to be ready and willing to accept these changes or adjust the IAM project to suit the organizational structure, meaning that the organization and IAM need to be adjusted to each other for IAM to be successful after implementation. This could be an argument to introduce organizational structure as a part of the IAM maturity model. However there already exist organizational maturity models for organizations dealing with the questions of IT projects (Davenport, 1993). Introducing organizational maturity into the maturity would also introduce organizational facets that are not immediately related to Identity and access management. The development of IAM in organizations follows a S-curve as described by Rogers (2003), starting at the immature/monitoring level and ending at the top class/authentication management level. See Fig. 15.6.

In the White book on Privacy Enhancing Technologies by Koorn et al. (2004), is stated that PETs are composed out of several technologies divided in four different PETs categories (see Fig. 15.1):

1. General PETs controls (i.e. identity and access management);
2. Separation of data (identity and pseudo-identity domains);
3. Privacy management systems for personal data that can't be encrypted at the intake because many laws require the collection of clear (non- encrypted) data;
4. Anonymisation.



	Immature	Starting-up	Active	Pro-Active	Top Class
Authentication Management	No authentication means	Arbitrarily formulated authentication requirements (authentication means are provided, adjusted and deleted on user request)	Authentication requirements based on a one time survey	Authentication Requirements based on continuous risk analysis	Authentication requirements based on continuous risk analysis and are continously adjusted
User Management	Double and inconsistent entries because of chaotic and ad hoc processes	Entries can be double but they are consistent	Central registration, Limited user group, manual procedures	Central registration, controlled authorization processes, manual procedures	Central real-time controlled authorization sources, automated procedures
Authorisation Management	No authorization matrixes, authorization is defined ad hoc	Authorization matrixes defined but are not updated	Authorization matrixes are updated periodically	Role Based Access Control used for critical applications	Role Based Access Control for all applications and continuous updated authorizations
Provisioning	Manual process locally	Limited Automated unreliable processed locally	Limited Automated but reliable processes locally	Limited Automated and reliable for multiple sources	Automated and reliable for multiple sources
Monitoring(Audit)	No responsibility delegated into a AO/IC organization	Sporadically delegated responsibility of AO/IC	Partial delegation of responsibility to AO/IC	Full responsibility to AO/IC	Full responsibility to AO/IC with periodic reporting

Fig. 15.6 IAM topology with organization class segments for maturity

These technologies in turn require a certain IT infrastructure. It also becomes clear from the White book that implementing PETs requires a solid foundation in the form of Identity and Access Management in order to minimize the use and access to sensitive personal data. With the help of Identity and Access management, PETs tries to minimize the use of and access of sensitive personal data. Especially the use of the PETs that secure access makes this clear. Secured Access however is only the first step for PETs. Privacy Enhancing Technologies also strive to segregate sensitive information in order to secure a person's identity. Not only segregation however is used to achieve this goal. Depending on the organizational information needs, information can also be immediately removed after use or not even registered in the first place.

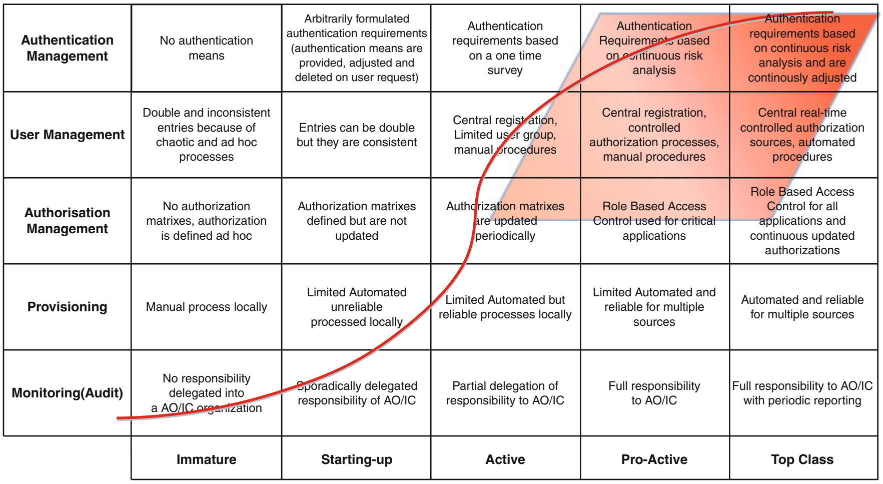
Along the maturity curve of IAM runs the S-shaped maturity curve of awareness for privacy protection (Hahn et al., 2008), although interviews with management of organizations indicate that this S- curve starts in a much later phase of the IAM S-curve.

If the rights to access can be bound to a certain group, profile, person or user within an organization then IAM can be used to make sure that the user or user group only gets access to the information for which they are authorized. IAM then can also be used to provide the means of identification to make sure that the right user gets access to the user profile that is authorized to access certain sensitive information. Next to user management, authentication management and authorization management, provisioning and monitoring and audit can also play an important part in a PETs implementation. For instance when a central database of information is accessed by different organizations provisioning (automated or not) can play an important to keep user accounts for that database up to date at the different locations. Monitoring and Audit plays an important role when reviewing the current status of user accounts and controlling if authorized users only are accessing data. Thus depending on the requirements of the organization on its PETs implementation a certain level of maturity is required for the relevant IAM processes.

For the implementation of PETs, certain maturity of the organization is required. It is highly unlikely that immature organizations will implement PETs, let alone that these organizations have any awareness of privacy protection. The level of maturity for IAM is a strong indication for the introduction of PETs in an organization (Fairchild and Ribbers, 2008).

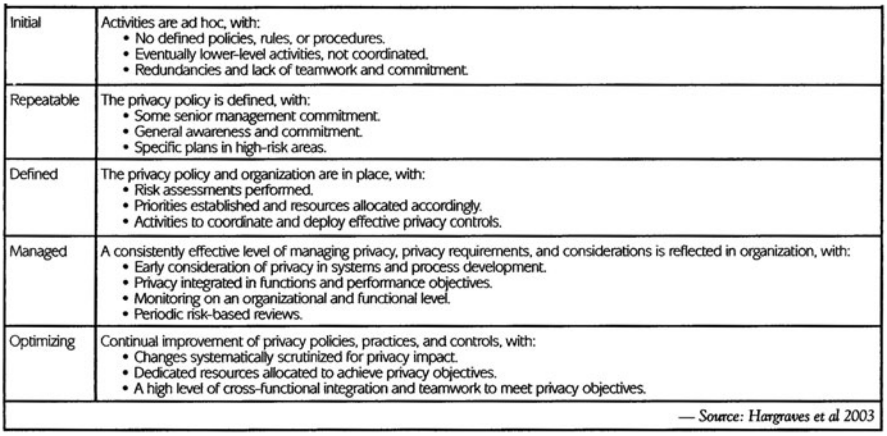
Based on interviews of the management of large (multi-national) organizations it becomes clear that the choice of advanced PETs occur in the pro active and top class maturity segments (Borking, 2010) (See parallelogram in Fig. 15.7).

This leads to assume that there can be recognized three S-curves concerning the application of PETs: one for the adoption of PETs with as most important positive stimulating factor the pressure of the legislation which regulates the protection of personal data and the role of the recommending privacy supervisors (i.e. DPAs, Privacy Commissioners); one for the application of IAM processes where the maturity of the IAM processes must be high; and one for the integration of the protection of privacy with the company processes as reflected in GAP privacy level model running from the initial level till the optimal level (see Fig. 15.8).



Authentication Management	No authentication means	Arbitrarily formulated authentication requirements (authentication means are provided, adjusted and deleted on user request)	Authentication requirements based on a one time survey	Authentication Requirements based on continuous risk analysis	Authentication requirements based on continuous risk analysis and are continosly adjusted
User Management	Double and inconsistent entries because of chaotic and ad hoc processes	Entries can be double but they are consistent	Central registration, Limited user group, manual procedures	Central registration, controlled authorization processes, manual procedures	Central real-time controlled authorization sources, automated procedures
Authorisation Management	No authorization matrixes, authorization is defined ad hoc	Authorization matrixes defined but are not updated	Authorization matrixes are updated periodically	Role Based Access Control used for critical applications	Role Based Access Control for all applications and continuous updated authorizations
Provisioning	Manual process locally	Limited Automated unreliable processed locally	Limited Automated but reliable processes locally	Limited Automated and reliable for multiple sources	Automated and reliable for multiple sources
Monitoring(Audit)	No responsibility delegated into a AO/IC organization	Sporadically delegated responsibility of AO/IC	Partial delegation of responsibility to AO/IC	Full responsibility to AO/IC	Full responsibility to AO/IC with periodic reporting
	Immature	**Starting-up**	**Active**	**Pro-Active**	**Top Class**

Fig. 15.7 Level of maturity for PETs in parallelogram



Initial	Activities are ad hoc, with: • No defined policies, rules, or procedures. • Eventually lower-level activities, not coordinated. • Redundancies and lack of teamwork and commitment.
Repeatable	The privacy policy is defined, with: • Some senior management commitment. • General awareness and commitment. • Specific plans in high-risk areas.
Defined	The privacy policy and organization are in place, with: • Risk assessments performed. • Priorities established and resources allocated accordingly. • Activities to coordinate and deploy effective privacy controls.
Managed	A consistently effective level of managing privacy, privacy requirements, and considerations is reflected in organization, with: • Early consideration of privacy in systems and process development. • Privacy integrated in functions and performance objectives. • Monitoring on an organizational and functional level. • Periodic risk-based reviews.
Optimizing	Continual improvement of privacy policies, practices, and controls, with: • Changes systematically scrutinized for privacy impact. • Dedicated resources allocated to achieve privacy objectives. • A high level of cross-functional integration and teamwork to meet privacy objectives.
	— *Source: Hargraves et al 2003*

Fig. 15.8 Generic privacy maturity levels

The three s-curves' combination results in Fig. 15.9:

As can be concluded from Fig. 15.9, the moment of decision for the adoption of PETs appears to be at the higher levels of the IAM maturity (organizations in the Top Class and Pro-Active maturity level, with the exception for organizations at the level: active that update authorization matrixes periodically) (Fairchild and Ribbers, 2008) and in the lower levels of privacy maturity, thus where IAM measures reach the level of PET measures. There are exemptions for those organizations that belong to the category of (micro/mini) SMEs where trust is a critical success factor, like in the medical profession, barristers, notaries etc. Although processes mentioned in

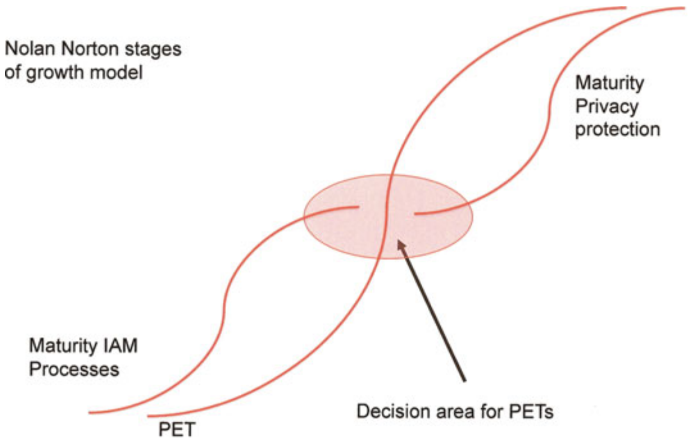

Nolan Norton stages of growth model
Maturity Privacy protection
Maturity IAM Processes
PET
Decision area for PETs

Fig. 15.9 Nolan Norton growth S-Curves concerning IAM-, Privacy en PETs (Borking, 2010)

the maturity model are non-existent in these organizations, it may be expected that these SMEs will protect personal information of their clients encrypted or will use rudimentary PETs tools.

15.11 Changing the Negative Adoption Factor of Costs into a Positive One

The perceived costs for PETs measures are an important negative adoption factor. However there isn't very much understanding about the business case for investment in PETs.

In order to best understand the likely adoption of PETs we must understand the challenges that privacy poses for organizations. This can be done best through engaging with experts and practitioners. To achieve this, the researchers conducted a number of consultations with industry experts, through direct discussions and by using a workshop-format (Fairchild and Ribbers, 2008).

Traditionally when the researchers put forward the question whether organizations have some inherent interest in privacy, a list of drivers emerges. These drivers include: compliance with legal obligation, fear of reputation damage from privacy failure, the need to generate trust with clientele, and the promotion of a good corporate practice. Yet if this was truly the case then privacy enhancing technologies would be already implemented everywhere across both industry and government organizations. Reality appears more complex (Fairchild and Ribbers, 2008).

But organizations need also to know what the business case of investments in PETs is (Economic motives for the use of PETs) in order to support the privacy protection required by the law and/or the policy of the firm. As many data are uncertain, scenarios have to be designed and assessed to give decision makers an understanding of the behavior of cost and benefit factors and their eventual effect on the business case outcome.

15.12 Business Case for Pets Investments

Investments in (risk reducing) PETs require insight into the costs and the quantitative and qualitative benefits. It is essential for the decision-making process concerning the investment for PETs (Borking, 2010).

The decision to spend money on privacy in any direction has to be financially justified. There is no point in implementing an expensive solution if a less expensive solution would offer the same risk reduction and because of that a better privacy protection. Beyond the legal compliance, it makes no sense to invest in a solution if its true costs are greater than the value it offers.

From the perspective of a business, privacy implies an investment to be measured in Euros saved as a result of reduced cost, or in additional revenues and profits from new activities that would not have occurred without an investment in privacy.

From the risk management literature a number of metrics have been identified to measure security risks; some of them apply to privacy risks as well (Fairchild and Ribbers, 2008).

15.13 Annual Loss Expectancy

One of the most common measures for the assessing the risk of a harmful event is Annual Loss Expectancy, or ALE. ALE is the product of the expected yearly rate of occurrence of the event times the expected loss resulting from the occurrence. Other yardsticks here are SLE and ARO. SLE stands for the Single Loss Exposure; this is the true cost of a security incident. ARO means annual rate of occurrence; this is the frequency in which a risk happens on a yearly basis. The annual loss expectancy foreseen from all of an organization's operations would be the sum of the expected yearly losses that could result from multiple (privacy) threats. Determining adequate inputs to this ALE equation is however very difficult, due to lack of statistical data.

For example if a bank estimates the probability of a serious security incident at one of its subsidiaries during 2008 as one in a million and the direct and indirect cost of such incident as 150 million Euros, the ALE created by the risk of this security incident for 2008 will be € 15 million times 1/1,000,000 = € 150. Of course the actual costs of this risk will never be that of the ALE, but it will be either € 0 or €150 million. In most cases the situation will be less certain and the probability or cost may range between one in five hundred thousand and one in a million and the cost may vary between € 100 million and € 200 million. The ALE would then be between: (€100 M or €200 M) × (1/5,000,001/1,000,000) = €100 or €400 (Blakley et al., 2002).

15.14 Return on Investment (ROI)

A metric that is quickly gaining in popularity is Return On Investments and specifically Return On Security Investments (ROSI) (Sonnenreich et al., 2006). Cardholm writes that: "Return on Investment (ROI) is a straightforward financial tool that measures the economic return of a project or investment. It is also known as return on capital employed. It measures the effectiveness of the investment by calculating the number of times the net benefits (benefits minus costs) recover the original investment. ROI has become one of the most popular metrics used to understand, evaluate, and compare the value of different investment options" (Cardholm, 2006)

> The equation is (Borking, 2010): ROI = [(Savings from safeguards) + (profits from new ventures)] / costs of safeguards = [ALE (baseline) − ALE (with safeguards) + (profits from new ventures)] / costs of safeguards.

Hereunder follows an example. Suppose an organization decides to implement a Privacy Management System (PMS). The business case could be substantiated as follows:

If PMS were not implemented, the minimum *annual* costs for a company employing 1,000 staff to comply with privacy policies are estimated as follows:

1. *Annual costs*

   Salary costs for Privacy Protection Officer (100% time allocation) Euro 100,000;
   Management and secretarial salary costs Euro 40,000;
   Costs for privacy audit Euro 30,000;
   Security costs with respect to privacy compliance (excluding essential information security) Euro 20,000;
   Report maintenance, regulations, settling registered people's rights, information, image and other damage, etc. Euro 20,000.
   This leads to the total annual costs of Euro 210,000.

   When comparing the situation where a PMS is used, the picture is as follows:
2. *Development and implementation of PMS*

   For the acquisition of PMS has to be paid: Euro 150,000;
   Consultancy for PMS implementation (60 days) costs Euro 80,000;
   Start-up costs after implementation Euro 20,000.
   The total one-off costs are Euro 250,000.

To these costs have to be added:

a. Annual costs PMS
b. PMS operational costs are Euro 30,000;
c. Maintenance costs are ± 15% of acquisition cost per annum: Euro 22,500;

d. Costs for privacy audit: Euro 10,000;
e. Salary costs for Privacy Protection Officer (50% time allocation) Euro 50,000; In this situation the total costs are Euro 112,500.

The saving per annum compared with the situation when there wasn't an investment in PMS is Euro 210,000–Euro 112,500–Euro 97,500. Thus the extra investment costs for PMS would be already fully recovered after approx. 2 years and 2 months.

15.15 Return on Security Investment (ROSI)

ROSI (Fig. 15.10) is a special application of ROI. The Return On Security Investments (ROSI) formula, developed by a team at the University of Idaho led by researcher HuaQiang Wei, is the most well known ROSI calculation in the security industry. They used what they found in the research area of information security investments and combined it with some of their own theories, assigning values to everything from tangible assets (measured in dollars with depreciation taken into account) to intangible assets (measured in relative value, for example, software A is three times as valuable as software B). Different types of attacks, or incidents, were assigned as individual costs. To verify the model, the team went about attacking an intrusion detection box they had built, to see if the costs the simulation produced matched the theoretical costs. They did. Determining the cost-benefit became the simple task of subtracting the security investment from the damage prevented. ROSI is an approach to look at the investment costs of security protection and the risk the investment removes. Assuming that the annual benefit of a security investment will be received throughout the lifetime of the investment, ROSI calculates the sum of the annual benefits over its cost. Benefits are calculated by adding expected cost savings to the new profit expected from new activities and sales.

Cardholm states that "it is basically a "saving" in Value-at-Risk; it comes by reducing the risk associated with losing some financial value" (Cardholm, 2006). Three core elements are determinative for the output calculation of the investment, namely: costs, turnovers and non-financial measurable elements. ROSI can be calculated using the equation below.

The earlier discussed ALE can also be written as: Risk Exposure multiplied with %RiskMitigated or Risk mitigated because of the investment in security (Borking, 2010).

The difficult parts in ROI method is determining ALE and SLE the risk-mitigating benefits of the security investment, since it is very difficult to know the

$$Rosi = \frac{(RiskExposure \bullet \%RiskMitigated) - SolutionCosts}{SolutionCost}$$

Fig. 15.10 ROSI equation (Sonnenreich, 2006)

true cost of a security incident. According to Sonnenreich et al. (2006) there is very little known about those costs, because very few companies track those incidents.

Cardholm has a better approach with less uncertainty. His calculation is as follows:

$$\mathrm{ROSI} = \mathrm{R} - (\mathrm{R} - \mathrm{E}) + \mathrm{T},$$

or

$$\mathrm{ROSI} = \mathrm{R} - \mathrm{ALE}, \text{ where ALE } = (\mathrm{R} - \mathrm{E}) + \mathrm{T}$$

The terms in Cardholm’s equation can be described as:

- ALE: What we expect to lose in a year (Annual Loss Expectancy)
- R: The cost per year to recover from any number of incidents.
- E: These are the financial annual savings gained by mitigating any number of incidents through the introduction of the security solution.
- T: The annual cost of the security investment (Cardholm, 2006).

15.16 ROI for Privacy Protection

The ROI calculation methods can be applied also analyzing the return on investments that mitigates privacy risks, it means investments in PETs.

PETs investments differ from “normal” ICT investments, since the investment may not directly improve the workflow, or does not make a process more efficient. The costs from PETs are tangible and because of that are relatively easy to know. The benefits however are mostly intangible, because for example reputation improvement and a decreased risk for privacy incidents are not easy to quantify. However, these intangible benefits have the biggest value in a PETs investment.

Luckily, the value of risk mitigated can be calculated using the method of Darwin (2007). The Darwin Calculator can be found at www.tech-404.com/calculator.html.

The focus in this method will then be on the tangible benefits, the value of risk mitigated and the total costs, related to the PETs investments. This method will be named: Return on Privacy Investments (ROIPI).[4] How these figures will be calculated will be explained hereunder in more detail in the example of the Ixquick Europrise seal business case.

The formula is: ROIPI = {(Tangible Benefits +Value Of Risk Mitigated) – Total Costs} divided (/) by the total costs

When the ROIPI gives a positive result, it means that the investment is beneficial for the company since the benefits outweigh the costs. Note that if the value of risk

[4] Fritsch, 2008 and Dijkman, 2008 were the first that used the term ROPI. I prefer ROIPI preventing misunderstanding amongst auditors

mitigated is positive this also has a positive influence on the ROIPI. The strong point of this formula is that it is not necessary to derive at an accurate estimate. The ROIPI only has to be precise enough to support the decision-making.

ROIPI assumes that the organization will fully comply with the law. This isn't often the fact. Violation of privacy, i.e. the illegal use of personal data, generates a lot of revenue and the chance that violation will lead to a prosecution is almost nil, due to the lack of resources of the National Data Protection Authorities.

15.17 Ixquick

Ixquick is a meta search-machine. The website of Ixquick might be found at www.ixquick.com. Ixquick revenue model is the number of hits times the advertising benefits. The revenue is highly correlated to the search queries done through the site.

In 2003 and 2004, Internet traffic went down. In 2005, Internet traffic only went down with 5% and stabilized. In 2006 and 2007 the traffic increased again, due to the fact that Ixquick anonymized the IP addresses and search results in June 2006. Because of the anonymization, the traffic in 2006 and 2007 increased considerably. Due to the optimalization of the privacy protection of the users of the Ixquick meta search engine, triggered by the requirements for obtaining the EuroPrise privacy certificate,[5] the number of visitors of the website increased again substantialy in 2008, thanks to the investment in the PETs tool anonymization. With the increased traffic the revenue od Ixquick went up as well.

The reason of Ixquick for using PETs was that it is a unique selling point; Ixquick became and is still the first fully anonymized meta search engine. Besides this reason the other driver was privacy risk minimalisation.

The investment costs for the PETs tools were Euro 129.800, inclusive the extra investments needed for meeting the requirements of the EuroPrise certificate. The expenditure for the optimalized privacy protection amounted to € 37.000 for the technical and legal expertise. For press releases and communication costs announcing the Euro Prise privacy certificate award in July 2008 (Andriessen, 2008) € 8.000 was spent. The mentioned costs were non-recurrent one-off expenses.

Moreover there are also recurring costs for the maintenance and the further development of the system amounting to € 16.500 per year. The total costs for the whole PETs investment was: € 183.300.

The ROIPI equation can now be used for calculating whether Ixquick's privacy protection investment was the right decision of Ixquick's management.

ROIPI = {(Tangible Benefits + Value Of Risk Mitigated) − Total Costs} / (divided) by the total costs.

[5] http://www.european-privacy-seal.eu/about-europrise/fact-sheet

The total PETs costs are Euro 183.300. The tangible benefits of using PETs tools are the extra revenues in because of the increased data traffic. The directly tangible advantage for Ixquick due to the use of PETs for the period of PETs investments (2005–2008) is estimated by the author[6] at Euro 345.800. To estimate the factor "risk mitigated" the calculation tool of Darwin (2008) has been used. It will be assumed that in a privacy incident 10.000 records were stolen. Based on the daily users of the Ixquick search machine, the actual risk was much higher. The risk class of this data is of risk class II according to the guideline of the Duch Data Protection Authotity (CBP) (Borking, 2003; Hes and Borking, 2000; Van Blarkom et al., 2003; Communication from the Commission to the European Parliament and the Council on Promoting Data Protection, 2007) since the data consist of searches, these can consist of IP address, social security numbers and credit card numbers.

Based on the Darwin calculator (2008) the value of risk mitigated is Euro 1.050.300 on the 80% level (loss of 10.000 records) and the Dollar/Euro exchange rate in November 2008.

Using the values, the ROIPI equation produces as result:

Total Costs= Euro183.300
Tangible Benefits= Euro 345,800
Value Of Risk Mitigated= Euro 1.050.300
The intangible costs and benefits are appreciated as Euro 0.

Thus

$$\text{ROIPI} = \{(345.800 + 1.050.300 + 0) - 183.300\}/183.300$$
$$=\text{ROIPI} = 66,165 = \text{approx. } 662\% \text{ of the PETs investment.}$$

As this ROIPI value is very high, the conclusion is that the investment is very worthwhile. This number is also very high because of the value of risk mitigated. The ROIPI equation is especially preferable for SMEs because of its simplicity. This formula is a quick and reliable indicator whether the investment is worthwhile.

The intangible costs and benefits have been appreciated as zero euro, but if these intangible elements would be calculable, then the result would be even more favorable. However the ROIPI value is here significantly large enough to carry out the PETs investment and to justify the investment from a business economy point of view.

Others advocate rightfully that organizations should discard the above equations and instead use discounted cash flow methods for investments that have different costs and benefits in different years. The theoretical flaw in ROI (and so in ROSI, ROIPI and related approaches) is that it processes financial figures irrespective of the dates that will be received or paid. The value of 1 euro today is not the same as of 1 Euro in 2 years time. The Discounted Cash flow methods (DCF) encompass two

[6] The real financial figures are confidential

separate methods, the internal rate of return (IRR) and the Net Present Value (NPV). The allotted space for this chapter doesn't allow elaborating on the IRR method.

15.18 Net Present Value (NPV)

The Net Present Value (NPV) of a project or investment is defined as the sum of the present values of the annual cash flows minus the initial investment. The annual cash flows are the Net Benefits (revenues minus costs) generated from the investment during its lifetime. These cash flows are discounted or adjusted by incorporating the uncertainty and time value of money. NPV is one of the most robust financial evaluation tools to estimate the value of an investment (Cardholm, 2006).

The calculation of NPV involves three simple yet non trivial steps. The first step is to identify the size and timing of the expected future cash flows generated by the project or investment. The second step is to determine the discount rate or the estimated rate of return for the project. The third step is to calculate the NPV using the equations shown below:

$$\text{NPV} = \text{initial investment} + (\text{Cash flow year 1 divided by } (1 + \text{r})^1)$$
$$\ldots (\text{Cash flow year 1 divided by } (1 + \text{r})^{\text{n}})$$

Or

$$\text{NPV} = \text{Initial investment} + \sum_{t=1}^{t=\text{end of project}} \frac{(\text{Cash Flows at Year } t)}{(1+r)^t}$$

The meaning of the terms is as follows:

- Initial investment: This is the investment made at the beginning of the project. The value is usually negative, since most projects involve an initial cash outflow. The initial investment can include hardware, software licensing fees, and start-up costs.
- Cash flow: The net cash flow for each year of the project: Benefits minus Costs.
- Rate of Return (r): The rate of return is calculated by looking at comparable investment alternatives having similar risks. The rate of return is often referred to as the discount, interest, hurdle rate, or company cost of capital. Companies frequently use a standard rate for the project, as they approximate the risk of the project to be on average the risk of the company as a whole.
- Time (t): This is the number of years representing the lifetime of the project.

Experts are convinced that a company should invest in a project only if the NPV is greater than or equal to zero. If the NPV is less than zero, the project will not provide enough financial benefits to justify the investment, since there are alternative investments that will earn at least the rate of return of the investment (Cardholm, 2006).

Ribbers developed a specific NPV equation for investments in PETs. Within the context of the NPV method, the following data have to be collected:

- the *initial investment in privacy protection* [I(p)], which encompasses cash outlays for Privacy Risk Analysis, process modeling, PETs, implementation of PETs, productivity loss, change management.
- the *yearly recurring cashflow*, which contains all yearly financial effects of the proposal. This calculation bears on an analysis of expected cashflow patterns that would occur with and without the investment; it reflects a difference between two defined situations. The so-called "without" situation will usually be the continuation of the current situation. This can for example be a situation with existing privacy protection in place, where the added value of PETs is considered. The "without" situation might also be a situation without any privacy protection. The definition of the "without" situation depends on the starting position of the decision-maker.

Ribbers proposes to take into account the following cash flow components: Annual Loss Exposure (ALE), Reputation Recovering Costs (RRC), Expected Revenue Accrual (ERA), Recurring Privacy Costs (RPC) (Fig. 15.11) (Fairchild and Ribbers, 2008).

ALE is the multiplied projected costs of a privacy incident and its annual rate of occurrence. Basically this encompasses revenue losses, legal claims, and productivity losses because of privacy breaches, repair costs and lost business.

RCC contain those expenses needed to restore the reputation of the company damaged by privacy breaches; examples are additional costs for PR and Marketing. Moreover if a privacy breaches affects the share price of the company (see ChoicePoint, Double Click), possibly breaches affects the share price of the company (see ChoicePoint, Double Click), banks and other financial institutions may require possibly additional financial guarantees.

ERA represents, on the positive side, possible marketing impacts on market share and revenue of publicized implementation of PETs.

RPC contains the yearly (additional) privacy costs caused by the proposal; this will encompass needed privacy threat or impact analyses, audits, privacy officers etc.

As said, the analysis compares the project situation with the situation without the project. Basically this comes down to analyze the cash flow differences between the two situations. This can be done either by applying a factor RM (Risk Mitigated) to the situation without the investment or by subtracting the full-expected cash flow of the two situations from one another.

The RM factor for the applied privacy risk reducing/protection solution indicates what part of ALE and RRC has been compensated by the solution. Mitigated Risk is expressed as a reduction of the expected number of privacy breaches per year.

The resulting NPV of a privacy protection solution is consequently as follows:

$$NPV = - I(p) + \sum_{j=1}^{n} \{(ALE + RRC)\, RM + ERA - RPC\} / (1+i)^{j}$$

Fig. 15.11 Privacy investment net present value (Fairchild and Ribbers, 2008)

15.19 The Case of the National Victim Tracking and Tracing System (ViTTS)

The nation-wide implementation in the Netherlands of the Victim Tracking and Tracing System (ViTTS) is an important contribution to an effective disaster management. The system provides regional medical officials with a concrete support to execute their tasks, through access to the required relevant contextual information; it supports the allocation of injured persons to local and regional hospitals, and it provides the relevant competent authorities with necessary information. Moreover, municipalities will be better placed to execute mandatory registration procedures under the municipal disaster plan, and hospitals will be provided with timely information about the numbers of victims and the nature of their injuries. Due to the fact that sensitive personal medical information is processed about victims, the DPD requires optimal protection of such sensitive personal data. Privacy issues with respect to the health sector are particularly sensitive.

The EU PRIME[7] research team[8] has applied the NPV calculation approach in several case studies. One of the case studies is ViTTS. The following data have been collected from ViTTS.

The initial investment in privacy protection *I(p)* comprises the following components:

– System analysis and design, prototyping, test runs:	Euro 15,000
– Privacy audit and Privacy risk assessment:	Euro 50,000
– Smart Cards for on line authentication and encryption:	Euro 25,000
– Implementation costs of PETs measures:	Euro 80,000

The total initial investment in reducing the risks of privacy incidents: Euro 170,000

Privacy breaches affecting the process of handling victims would have serious consequences and should be at all cost avoided. The privacy threat analysis showed that without privacy protection the VITTS system would undergo privacy breaches on a regular basis. The damage that would result from that can be estimated as follows.

[7] PRIME (Privacy and Identity Management for Europe) Contract No. 507591 Research periode 2004–2008

[8] The PRIME researchers were P.Ribbers (UoT), A.Fairchild (VUB), J.Tseng (EUR), R-J.Dijkman (UoT) and J.J.Borking (BC)

The direct consequence of a breach (SLE – Single Loss Exposure) would be loss of reputation of the national government, possible wrong allocation of victims to hospitals with ineffective treatment and possibly deceases as a consequence. This may lead to significant legal claims. Claims of Euro 100,000 per case are not exceptional.

Such a breach would necessitate a nation-wide roll out of system adaptations: for which is needed two man-months per designated preventive health care safety region at Euro 100 per hour:

Total costs	Euro 347,000
Test and Trials to prove effectiveness of the system:	
Euro 80,000 per region:	
Total cost	Euro 800,000
Training and education roll out:	Euro 50,000
The total recovering costs (RCC) would amount to:	Euro 1,197,000

The expected revenue accrual (ERA) can be estimated as follows. The most important reason for designated preventive health care safety regions to adopt the system is the built-in optimal privacy protection. So without privacy protection or with a much less rigid privacy protection there wouldn't have been developed such a system.

The estimated salary costs to replace the system by manual procedures would amount to 3 FTEs per region, which amounts to Euro 180,000 per region.

Nationwide this would result in a cost of:	Euro 1,800,000
The total benefits of protecting privacy and reducing the risks of privacy incidents can be estimated at:	Euro 2,277,000
(in this number legal claims are not included)	

Scenario

For the NPV calculation it is assumed:

1. a time horizon of 6 years
2. a serious privacy breach every 2 years
3. a cost of capital of 5%

Applying the equation results into the following:

I(p):	Euro 170,000

Recurring cash flows:

– costs avoided every 2 years:	Euro 2,277,000
– yearly recurring privacy costs:	Euro 400,000
– privacy costs in year 3 (no costs in year 6 given the assumption):	Euro 25,000

Under this assumption the calculation would be as follows:

$$\text{NPV} = -170{,}000 + 2,277,000(0.9707029 + 0.822702 \\ +0.710681) - 25,000(0.863838) - 400,000\ (5.242137) = \text{Euro}+ \\ 3,268,368$$

This (positive) business case does not include possible legal claims.

The business case for the investment mitigating the risk of privacy incidents is positive. Other scenarios lead to a positive business case as well. The privacy protection will even be profitable under the unrealistic assumption of a privacy breach only occurring once (and taking legal claims into account).

15.20 Conclusion

In this contribution the causes have been discussed why PETs, compared to the millions of computer systems which process personal data, hardly is used and that organizations trust on rather traditional organizational and technical data protection measures. The adoption of PETs by an organization appears be influenced by a large number of factors and the level of maturity of that organization.

S-curves for Identity and Access Management, for the maturity of organizations, for privacy protection and for the application of PETs itself, give an explanation for the slow application of the PETs solutions to adequately protect personal data. When the positive adoption factors are exploited belonging to the general PETs S-curve for promoting PETs, then a faster adoption of PETs by organizations which a large intensity of information processing (thus more need for privacy protection) may be realized. Good education concerning the technical possibilities of PETs and concrete requirements in the legislation (such as a privacy impact (PIA) or threat analysis assessment is necessary for promoting the PETs applications. If the legislation would stipulate the option that users should be in the position to choose for approaching services anonymously, then the use of PETs measures would be stimulated. In summary only legal and regulatory pressure (and the promotion by such advisory or supervisory bodies as the data protection agencies (DPA)) with regard to privacy protection is perceived to-date as having an undivided positive impact on the adoption process.

Costs for investment in PETs is an important negative adoption factor. This negative adoption factor can be converted into a positive one. The ROI and NPV calculation methods are useful tools for management for assessing the (planned) investments in PETs, reducing the risks of privacy incidents considerably.

The ROI and NPV calculation methods are useful tools for management for assessing the (planned) investments in PET, reducing the risks of privacy incidents considerably.

ROI, ROSI and ROIPI provide useful insights. For a “quick and dirty” assessment of a PET investment ROIPI is useful especially for SMEs, like in the Ixquick business case. However ROIPI and other ROI methods are based on evaluating reductions in risks and do not take a time factor into account. The best approach would be to consider investments in PET as regular investments, characterized by cash flow patterns.

The Net Present Value approach is applied on the ViTTS case. This approach is effective in the context of assessing investments in PET, reducing privacy risks and enhancing privacy protection.

As many data are uncertain due to the lack of recording privacy incidents, scenarios have to be designed and assessed to give decision makers an understanding of the behavior of cost and benefit factors and their eventual effect on the business case outcome. A mandatory disclosure and registration of privacy incidents as foreseen in the modification of the EU Directive 2002/58/EC, will contribute to this end, provided these disclosures will be recorded in an European register accessible for every citizen (Bayer and Melone, 1989).

References

Andriessen, V. “Nederlandse Internetzoekmachine Ixquick ontvangt eerste Europese privacycertificaat.” In *Het Financieele Dagblad*,15 juli 2008.

Bayer, J., and N. Melone. “A Critique of Diffusion Theory as a Managerial Framework for Understanding Adoption of Software Engineering Innovations.” *The Journal of Systems and Software* 9, 2 (1989): 161–166.

Blakley, B., E. McDermott, and D. Geer. Information management is Information Risk Management. in *Proceedings NSPW’01*, Cloudecroft, New Mexico, 2002.

Borking, J. “The Status of Privacy Enhancing Technologies.” In *Certification and Security in E-Services*. E. Nardelli, S. Posadziejewsji, and M. Talomo. Boston, MA: Kluwer Academic Publishers, 2003, p. 223.

Borking, J.J. “Assessing investments mitigating privacy risks.” In *Het binnenste buiten, Liber Amicorum ter gelegenheid van het emeritaat van prof. dr. H.J. Schmidt, hoogleraar Recht en Informatica te Leiden*, edited by L. Mommers, H. Franken, J. Van den Herik, F. Vander Klauw, and G-J. Zwenne. Leiden: Leiden University Press, 2010.

Borking, J.J. “The Business Case for PET and the EuroPrise Seal,” Report for EuroPrise EU Research project on Privacy Seals 2008; http://www.european-privacy-seal.eu/about-europrise/fact-sheet

Borking, J.J.F.M. *Privacyrecht is Code, Over Het Gebruik van Privacy Enhancing Technologies*. Deventer: Kluwer, 2010.

Bos, Tj. *Adoptie van privacy-enhancing technologies bij publiek/private instellingen*. Den Haag: Ministerie van Binnenlandse Zaken, 2006.

Camp, L.J., and C. Wolfram. Pricing Security. in *Proceedings of the CERT Information, Survivability Workshop*, Kluwer Academic Press, Boston MA, 2000.

Cardholm, L. Adding Value to Business Performance Through Cost Benefit Analyses of Information Security Management, Thesis, Gävle, 2006.

Cas, J., and Ch. Hafskjold. *Access in ICT and Privacy in Europe, Experiences from technology assessment of ICT and Privacy in seven different European countries*. Geneva: EPTA, 2006, p. 41.

Chapman, S., and G.S. Dhillon. Privacy and the Internet: The Case of DoubleClick, Inc. – Social Responsibility in the Information Age: Issues and Responsibilities. XXX, Fort Lauderdale-Davie, 2002.

Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM (2007) 228 Final, Brussels, 2.5.2007.

Darwin. www.tech-404.com/calculator.html, 2007, 2008.

Davenport, Th.H. *Process Innovation – Reengineering work through Information Technology*. Boston, MA: Havard Business School Press, 1993.

Fagerberg, J. et al. *The Oxford Handbook of Innovation*. New York: Oxford University Press Oxford, 2005.

Fairchild, A., and P. Ribbers. "Privacy-Enhancing Identity Management in Business." In *Privacy and Identity Management for Europe*, edited by J. Camenish, R. Leenes, and Sommer, D. Report for the EU Commission X, Brussels, 2008, pp. 69–100.

Fichman, R.G. Information Technology Diffusion: A Review of Empirical Research. in *Proceedings of the Thirteenth International Conference on Information Systems (ICIS),* Dallas, (1992), pp. 195–206.

Greenhalgh, T., et al. "Diffusion of innovations in service organizations: Systematic review en recommendations." *The Milbank Quarterly* 4 (2004): 581–629.

Hahn, U., K. Askelson, and R. Stiles. *Managing and Auditing Privacy Risks*, ltamonte Springs, 2008 http://www.theiia.org/guidance/technology/gtag/gtag5/

Hes, R., and J. Borking. *Privacy Enhancing Technologies: The Path to Anonymity (2nd revised edition)*. Report from the Dutch Data Protection Authority AV no. 11 Den Haag, 2000.

Jeyaraj, A., J.W. Rottman, and M.C. Lacity. "A review of the predictors, linkages, and biases in IT innovation adoption research." *Journal of Information Technology* 21, 1 (2006): 1–23.

Koorn, R., H. Van Gils, J. Ter Hart, P. Overbeek, P. Tellegen, and J. Borking. *Privacy Enhancing Technologies – Witboek voor Beslissers*; (Whitebook for Decision Makers – Ministry of Internal Affairs and Kingdom Relations) Den Haag, 2004.

Leisner, I., and J. Cas. *Convenience in ICT and Privacy in Europe, Experiences from technology assessment of ICT and Privacy in seven different European countries*. Geneva: EPTA, 2006, p. 50.

OECD Organization for Economic Co-operation and Development, *Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data, 3rd edition*, 2005. Available at: http://www.oecd.org/

PRIME, acronym for project name: Privacy and Identity Management for Europe, Contract No. 507591 Research period 2004–2008

Privacy Rights Clearinghouse: A Chronology of Data Breaches. 2007. Available at: http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP

Rivera, M.A., and E.M. Rogers. "Evaluating public sector innovation in networks: extending the reach of the national cancer institute's web bases health communication intervention research initiative." *The Innovation Journal: The public Sector Innovation Journal* 9, (2004): 1–5.

Rogers, E.M. *Diffusion of Innovations*. New York: Simon & Schuster, 2003.

Smit, N. *A maturity Model*. Zoetermeer: EUR, 2005.

Sommer, D. "The PRIME Architecture." In *Privacy and Identity Management for Europein*, edited by J. Camenish, R. Leenes, and D. Sommer. Report for the EU Commission, Brussels, 2008.

Sonnenreich, W., J. Albanese, and B. Stout. "Return on Security Investment (ROSI) A practical approach." *Journal of Research and Practice in Information Technology* 38, 1, (Feb. 2006).

Stanford Organizational Maturity Levels, http://www2.slac.stanford.edu/comp/winnt/systemadministration/Organizational%20Maturity%20Levels.doc

Tidd, J., et al. *Managing Innovation: Integrating Technological, Market and Organizational Change*, Chichester: Wiley, John & Sons, Incorporated, 2005.

Tsiakis, T., and G. Stephanides. "The Economic Approach of Information Security." *Computers & Security* 24, 2005.

Tung, L.L., and O. Reck. "Adoption of electronic government services among business organizations in Singapore." *Journal of Strategic Information Systems* 14, (2005): 417–440.

Van Blarkom, G.W, J.J Borking, and J.G.E Olk. *Handbook of Privacy and Privacy-Enhancing Technologies, The Case of Intelligent Software Agents*. The Hague: College Bescherming Persoonsgegevens, 2003, pp. 22–30.

Van Gestel, G.P.C. Creating an Identity and Access Management Maturity Model, Thesis, Universiteit van Tilburg, Tilburg, 2007.

Vandecasteele, J., and L. Moerland. *Groeimodel voor IV-functie – Het systematisch weergeven van een herinrichtingproces*. Amstelveen: KPMG Management Consulting, 2001.