

# Why Adopting Privacy Enhancing Technologies (PETs) Takes So Much Time

John Borking<sup>1</sup>

## Abstract

*This paper tries to explain what factors influence the adoption of privacy enhancing technologies (PETs). This research question first explores whether PETs is an innovation. It then applies Rogers' theory on the diffusion of innovation on PETs. Conceptual models are presented on the main factors of adoption of PETs and the necessary maturity of an organization before adoption of PETs can occur. The paper points out that a positive business case for the economic justification of investments in PETs is needed before a positive decision on the investment will be taken.*

## 1 Introduction

Cas & Hafskjold wrote: “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” [1].

Leisner & Cas 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” [2]. Sommer [3] 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”.

PETs have been defined as a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system [4].

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

A group researchers (Borking, Bos, Dijkman, Fairchild, Hosein, Ribbers, Tseng) have focused in the PRIME project [26] in 2007 and 2008 [5] on what business drivers lead organizations to adopt privacy enhancing technologies (PETs) for providing assurance for privacy.

The central research question was:

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?

## 2 Technological innovations

An innovation is generally defined as the application of something new. According to Rogers [6] 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

---

<sup>1</sup> John Borking is owner/director of Borking Consultancy in Wassenaar The Netherlands and was a former privacy commissioner for The Netherlands (1994-2005) and is a researcher at the Leyden University in The Netherlands

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 [7]. The OECD [8] defines technological innovations 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.”*

PETs, given the relative recent introduction of the concept [4], 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.

### 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’ [10]. 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 [6].

In the study of diffusion and adoption many studies try to identify relevant impacting factors, so that predictive statements can be made [11].

Rogers [6] 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.

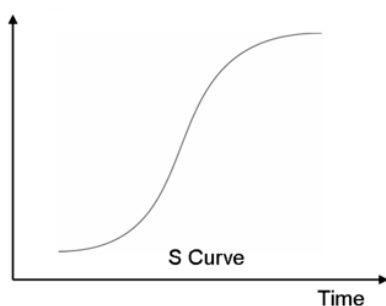


Figure 1. Rate of Adoption [6]

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 [12].

### 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 Jeyarai et al. [11] and Fichman [10] 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 appear to be those related to innovation characteristics, organizational characteristics, and environmental characteristics. Tung & Reck [13] reach this conclusion in their study.

Others have emphasized other influences on the adoption process: Fichman [10]: argues that adoption of IT based innovations require a different approach. Fichman [10], Rivera & Rogers [14] and Greenhalgh [15] 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 Figure 1.

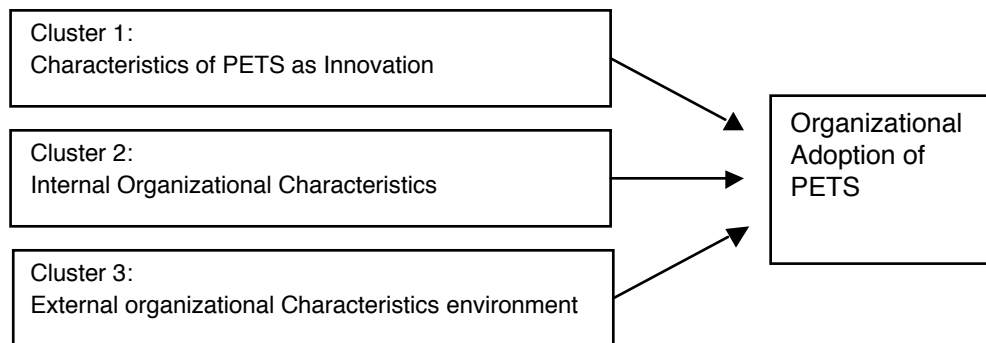


Figure 2 Conceptual model [5][16]

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.

### 5 Specific characteristics

Rogers [6] and Fichman [10] distinguishes five innovation characteristics and eight organizational characteristics, which affect the organizational adoption of innovations.

### **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

### **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

## **6 Encompassing Model**

Fichman [10] 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 & Organization Combination; b.the Technologies & Diffusion environments and c. the Organizations & Adoption environments.

The Technology & 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 & 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 & 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.

## **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 [16] and 4 workshops have been held in Sweden, UK, Netherlands and Switzerland [5]. In the workshops representatives of a broad range of industries participated. The results of the interviews are presented in Table 1 below. The variables mentioned by the experts and organizations have been grouped according to the categories innovation, internal organization and environment. [5 & 16]

### **7.1 Factor: Innovation**

Relative benefit:	<b>Positive</b>
Compatibility	Negative
Complexity:	Negative
Costs:	Negative <sup>2</sup>
Testability	Positive
Role of advisory institutions:	<b>Positive</b>
Social recognition:	<b>Positive</b>
PETs woven into business processes:	Negative

## 7.2 Factor: Internal Organization

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

## 7.3. Factor: Environment

External pressure by privacy laws:	<b>Positive</b>
Complexity of privacy laws:	Negative
Existing offer of PET measures	<b>Positive</b>
Visibility	<b>Positive</b>

## 8 Explanations of the terms

### 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.

### 8.2 Compatibility

Only when PET resembles its predecessor the effect is positive.

### 8.3 Complexity

PETs is 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.

### 8.4 Costs

PETs is perceived as an expensive innovation (with unclear benefits). Much depends however on

---

<sup>2</sup> When showing the results of calculating the Return On Investment on PETs investments some participants showed a positive attitude change towards adoption [17]

the moment that PETs is introduced. If the introduction is when a new system is put into use, then costs are generally at an acceptable level. This is also basically the only realistic option. PETs is simply too complex to apply to existing systems, costs are then being perceived as higher than those of traditional measures.

### **8.5 Testability**

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

### **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 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 promote the use of PETs actively anymore, with a lower rate of adoption as a result.

### **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.

### **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.

### **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.

### **8.10 Structure and Size of the organization**

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

### **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.

### **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.

### **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.

### **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.

#### **8.15 Diversity of information systems**

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

#### **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.

#### **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.

The EU privacy directives are considered by management 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 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) is seen as a positive stimulus. However 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<sup>3</sup> privacy seal.

#### **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.

#### **8.19 Existing offer of PET measures**

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

#### **8.20 Visibility**

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

### **9. Conceptual Model**

The model in figure 2 shows that a number of factors are perceived to have a negative impact on the adoption process. One assumption is that PETs is difficult to implement efficiently and effectively. Also the internal organizational characteristics have a negative impact. 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

---

<sup>3</sup> EuroPrise (privacy seals) has been subsidized by EU Commission under the eTEN Programme. See: <http://www.european-privacy-seal.eu/about-europrise/fact-sheet>

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 [16]. There is only a limited use. Looking at the model, 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 as an incentive to apply PETs [5].

### **10. Identity and Access Management (IAM) Maturity Model**

To examine under what conditions an organization would adopt PETs into its business processes, 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.”*[18]

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 maturity level 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 objective measures [16, 19, 20, 21]. 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 [21] model, researchers then integrated maturity phases into these processes, and developed an IAM maturity model shown below:

<b>Authentication Management</b>	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 continuously adjusted
<b>User Management</b>	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
<b>Authorisation Management</b>	No authorization matrices, authorization is defined ad hoc	Authorization matrices defined but are not updated	Authorization matrices are updated periodically	Role Based Access Control used for critical applications	Role Based Access Control for all applications and continuous updated authorizations
<b>Provisioning</b>	Manual process locally	Limited Automated unreliable processes locally	Limited Automated but reliable processes locally	Limited Automated and reliable for multiple sources	Automated and reliable for multiple sources
<b>Monitoring/Audit</b>	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
	<b>Immature</b>	<b>Starting-up</b>	<b>Active</b>	<b>Pro-Active</b>	<b>Top Class</b>

Figure 3: Conceptual Identity and access management maturity model

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 [22]. The organization 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 maturity as a part of the IAM maturity model. However there already exist organizational maturity models for organizations dealing with the questions of IT projects [23]. 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 [6].

In the White book on Privacy Enhancing Technologies by Koorn et al. [24], is stated that PETs is composed out of several technologies divided in four different PETs categories. 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 [25], 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 role 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 [5].

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.

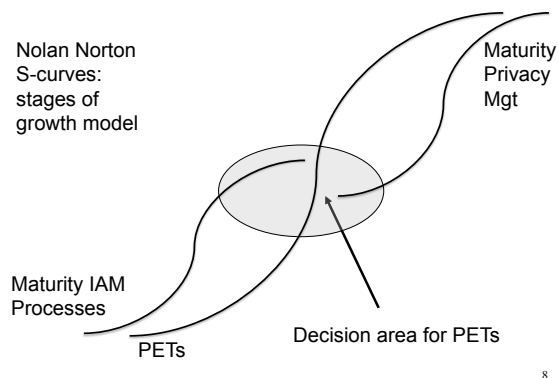


Figure 4. S-Curves voor IAM-, Privacy en PETs [27]

As can be concluded from figure 4, 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) [5] and in the lower levels of privacy maturity. 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 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.

### **Is there a Business Case for PETs?**

The perceived costs are a negative adoption factor. However not 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.

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 [5].

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. Fairchild & Ribbers used Discounted Cash-Flow methods like the Net Present Value – where the future cash-flow is discounted using a cost of capital – and the Internal Rate of Return – which is the rate that equates the discounted value of the positive and negative cash-flow, for assessing the business case of PETs investments [5]. A quick and dirty analysis for the economic justification of a PET investment can be done with the use of ROI-PI (*Return On Investment*-for PET) equation. This equation is as follows:

$$ROIPI = \frac{Revenue + IntangibleBenefits + ValueOfRiskMitigated - TotalCosts}{TotalCosts} \times 100\%$$

However, PETs researchers need much more empirical data on the impact of privacy breaches on individuals and organizations before firm conclusions can be reached.

### **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 to 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 PET 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 PET and concrete requirements in the legislation (such as a privacy impact (PIA) or threat analysis assessment is necessary for promoting the PET 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 PET 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.

However, it is also important that organizations understand their business case of investments in PETs. Empirical data of privacy incidents have to become available, as a result of which the consequences of such incidents can be assessed better and an investment in PETs can be justified more convincingly. 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.

### References:

- [1] J.Cas & Ch. Hafskjold, Access in ICT and Privacy in Europe, Experiences from technology assessment of ICT and Privacy in seven different European countries, Geneva 2006 p.41
- [2] I.Leisner & J.Cas, Convenience in ICT and Privacy in Europe, Experiences from technology assessment of ICT and Privacy in seven different European countries, EPTA, Geneva 2006 p.50
- [3] D.Sommer, The PRIME Architecture, in J.Camenish, R.Leenes & D.Sommer (eds), Privacy and Identity Management for Europe, Report for the EU Commission, Brussels 2008
- [4] J.Borking, The Status of Privacy Enhancing Technologies, in E.Nardelli, S.Posadziewjsji & M.Talomo, Certification and Security in E-Services, Boston 2003, p.223; See also R. Hes & J. Borking: Privacy Enhancing Technologies: the path to anonymity (2<sup>nd</sup> revised edition), Report from the Dutch Data Protection Authority AV no 11 Den Haag; 2000; G.W. van Blarkom, J.J.Borking & J.G.E.Olk, Handbook of Privacy and Privacy-Enhancing Technologies, The Case of Intelligent Software Agents The Hague 2003 ISBN 90-74087-33-7, p. 22-30
- [5] A.Fairchild & P.Ribbers, Privacy-Enhancing Identity Management in Business, in Privacy and Identity Management for Europe, J.Camenish, R.Leenes & D.Sommer (eds.) Brussels, 2008 p. 69-100
- [6] E.M. Rogers, Diffusion of Innovations, New York: Free Press, 2003.
- [7] J. Tidd ea, Managing Innovation: Integrating Technological, Market and Organizational Change, Chichester: John Wiley & Sons, 2005
- [8] OECD Organization for Economic Co-operation and Development, Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data, 3<sup>rd</sup> edition, 2005. Available at: <http://www.oecd.org/>
- [9] T.J. Cooke-Davies, Measuring Organizational maturity; Human Systems Limited; [http://www.humansystems.net/papers/measuring\\_organizational\\_maturity.pdf](http://www.humansystems.net/papers/measuring_organizational_maturity.pdf);
- [10] R.G. Fichman, "Information Technology Diffusion: A Review of Empirical Research," Proceedings of the Thirteenth International Conference on Information Systems (ICIS), Dallas, 1992, p. 195-206.
- [11] A. Jeyaraj, J.W. Rottman & M.C. Lacity, "A review of the predictors, linkages, and biases in IT innovation adoption research", Journal of Information Technology, 2006/1, p. 1-23.
- [12] J. Bayer & N. Melone, "A Critique of Diffusion Theory as a Managerial Framework for Understanding Adoption of Software Engineering Innovations", The Journal of Systems and Software, 1989/2, p. 161-166.

- [13] L. L. Tung & O. Reck, "Adoption of electronic government services among business organizations in Singapore", *Journal of Strategic Information Systems*, 2005/14, p. 417-440.
- [14] M.A. Rivera & E.M. Rogers, "Evaluating public sector innovation in networks: extending the reach of the national cancer institute's web based health communication intervention research initiative", *The Innovation Journal: The public Sector Innovation Journal*, 2004/9, p. 1-5.
- [15] T. Greenhalgh ea, "Diffusion of innovations in service organizations: Systematic review en recommendations", *The Milbank Quarterly*, 2004/4, p. 581-629.
- [16] Tj.Bos, *Adoptie van privacy-enhancing technologies bij publiekprivate instellingen*, Den Haag 2006
- [17] J.Borking, *The Business Case for PET and the EuroPrise Seal*, Report for EuroPrise EU Research project on Privacy Seals, Kiel 2008; The EuroPrise research project has been subsidized by the EU Commission under the eTEN Programme. The EuroPrise project started op June 10 2007 and ended February 28, 2009. See: <http://www.european-privacy-seal.eu/about-europrise/fact-sheet>
- [18] N. Smit; Erasmus University Rotterdam and Verdonck Kloosters and Associates, *Business Continuity Management – A maturity model*; November 1, 2005.
- [19] J. Fagerberg ea, *The Oxford Handbook of Innovation*, New York: Oxford University Press, 2005.
- [20] Stanford; *Organizational Maturity Levels* <http://www2.slac.stanford.edu/comp/winnt/system-administration/Organizational%20Maturity%20Levels.doc>
- [21] J. Vandecasteele & L. Moerland; *Groeimodel voor IV-functie – Het systematisch weergeven van een herinrichtingproces*; KPMG Management Consulting, Amstelveen, December, 2001
- [22] G.P.C. van Gestel, *Creating an Identity and Access Management Maturity Model*, Tilburg 2007
- [23] Th.H. Davenport: *Process Innovation – Reengineering work through Information Technology*. Harvard Business School Press, 1993.
- [24] R. Koorn, H. van Gils, J. ter Hart, P. Overbeek, P. Tellegen & J. Borking, *Privacy Enhancing Technologies – Witboek voor beslissers*; (Whitebook for Decision Makers - Ministry of Internal Affairs and Kingdom Relations) Den Haag, 2004.
- [25] U. Hahn, K.Askelson & R.Stiles, *Managing and Auditing Privacy Risks*, Itamonte Springs, Florida, 2008. See: <http://www.theiia.org/guidance/technology/gtag/gtag5/>
- [26] Projectname:PRIME (Privacy and Identity Management for Europe) Contract No. 507591 Research period 2004-2008
- [27] J.J.Borking, *Organizational Motives for Adopting Privacy Enhancing Technologies (PETs)* Vienna 2008. See [http://prise.oeaw.ac.at/conf\\_contrib.htm](http://prise.oeaw.ac.at/conf_contrib.htm)