# 7 The Economics of Privacy Protection in the Online World: A Business Perspective

Piet Ribbers, Tilburg University, p.m.a.ribbers@uvt.nl

In a first version of this paper I opened with the sentence "It is a great pleasure for me to contribute to Jo's Liber Amicorum"... We now have all experienced how cruel life can be and how things may suddenly change. The opening now is: It is with sadness that I contribute to Jo's Liber Amicorum in Memoriam.

I have known Jo since the beginning of my career at Tilburg University. The first time we met was at a conference of the EDISPUUT that I chaired; it was somewhere in the late 80s. He then struck me as a man with sharp comments in the scientific discussion, his remarks were however always accompanied with lots of humour. And that is the way that I have known Jo ever since: when Jo was in a meeting, he would not remain unnoticed. With him the scientific community of Information Management has lost an outstanding colleague, who combined high quality in his profession with good 'fellowship'.

My contribution to this Liber Amicorum in Memoriam is based on the work we did in PRIME, an EU project for which Jo had invited me to participate. PRIME stands for Privacy and Identity Management for Europe[1]. The thrust of this project was to explore and study privacy protection in the online world and to develop technology that would support the user in the protection of his privacy. The contribution of RSM concerned the so-called economics workpackage. This chapter is based on the thoughts we developed in this project, together with John Borking, Alea Fairchild and Jimmy Tseng.

## 7.1 Introduction

Businesses are utilizing personal data routinely for daily operations and as a means for customizing services to e.g. employees and customers. Collecting, storing and processing these data entail risks, in particular privacy risks. It is for example very tempting for others to steal that information, like in the data breach in Norway, in which telecom provider Tele2 got hacked and 60.000 accounts were stolen [ANP 2007]. It is known that in many companies privacy protection is not high on the priority list. To illustrate this, only 5% of all Dutch companies protect their privacy sensitive data according to requirements of the law [Koorn 2004]. Most companies only consider their privacy sensitive data after an issue like that of Tele2. In this paper we will argue that companies do have strong economic (besides ethical) motives to be concerned about privacy.

Privacy and privacy protection are in general at best considered from a legal perspective. An emerging question is however, whether and how economic considerations may affect a company's decision to engage in privacy protection and to utilize privacy enhancing technologies. In this paper we will first explore the concepts of privacy and PETs. Next measures to protect privacy are discussed. In the subsequent section we analyze possible reasons why companies should invest in privacy protection. We conclude with a discussion on how a business case analysis can contribute to an adequate privacy protection supported by PETs.

## 7.2 Privacy and Privacy Enhancing Technologies

Privacy is a difficult concept. In 1990 the Calcutt Committee in the UK stated that it was not possible to find a wholly satisfactory definition of privacy. Privacy is a property of personal data of a private person and of the rules of conduct between this person and processors of his personal data.

[1] [1] See: https://www.prime-project.eu/

Privacy relates to Confidentiality and Security. Confidentiality is not about personal data in particular; it is about data that has to be kept secret, or only be communicated to selected targets. [Borking 2007]. Usually this is data with a commercial, technical, scientific, patent pending, military or other background, which requires this data not to be made public. Confidentiality is one of the aspects of information security, the other aspects being Integrity and Availability.[2] These aspects are often abbreviated as CIA (C for Confidentiality, I for Integrity, and A for Availability).

As Borking explains, Privacy is based on four principles [Borking 2007]:

1. *Principle of Existence of Privacy*. A data subject possesses an identity and other pertinent and variable information that this person may consider to belong to his or her privacy domain. This collection of information is called personal data.

2. *Principle of Withholding*. The data subject has the right and should be equipped with the ability to withhold some or all of his personal data to other persons and organizations at this person's private choice.

3. *Principle of Trusted Usage*. The person or organization that receives the personal data and stores it (the collector) has the obligation to keep to legal and regulatory constraints on dissemination and processing of personal data. Furthermore, this collector has the obligation to inform the person involved of its possession of personal data and to provide the opportunity for change. Only if so permitted, the collector may copy the personal data to one or more processors for further processing.

4. *Principle of Controlled Dissemination*. The data subject has the right to disclose some or all of his or her personal data to other persons and organizations, at this data subject's own choice. This data subject may issue constraints on the dissemination of the personal data to one or more processors for further processing. He has the right to change the personal data, to extend and restrict it, to withdraw this information and to change the constraints.

The term 'Privacy Enhancing Technologies' (PET) is used to define all the technical controls that can be used to protect personal data.

The concept of PETs was introduced in the mid nineties. The idea was that IT could be utilized to protect privacy sensitive data [CBP 1995]. A publication by the Dutch Ministry of the Interior distinguishes four clusters of PET measures: General PET controls, Separation of Data, Privacy Management Systems and Anonymization.

The four clusters also represent a classification of the relative effectiveness and of the level of technology applied in PET-measures (see Figure 1) [Koorn, 2004]. A basic pre-condition for all the clusters is the 'Privacy by design principle', which means that the system design takes into account and starts from the premise of protection of personal data.

[2] According to the Information Security Evaluation Criteria (ITSEC) the following definitions are used for confidentiality, integrity, and availability:
Confidentiality – prevention of the unauthorised disclosure of information
Integrity – prevention of the unauthorised modification of information
Availability – prevention of the unauthorised withholding of information or resources

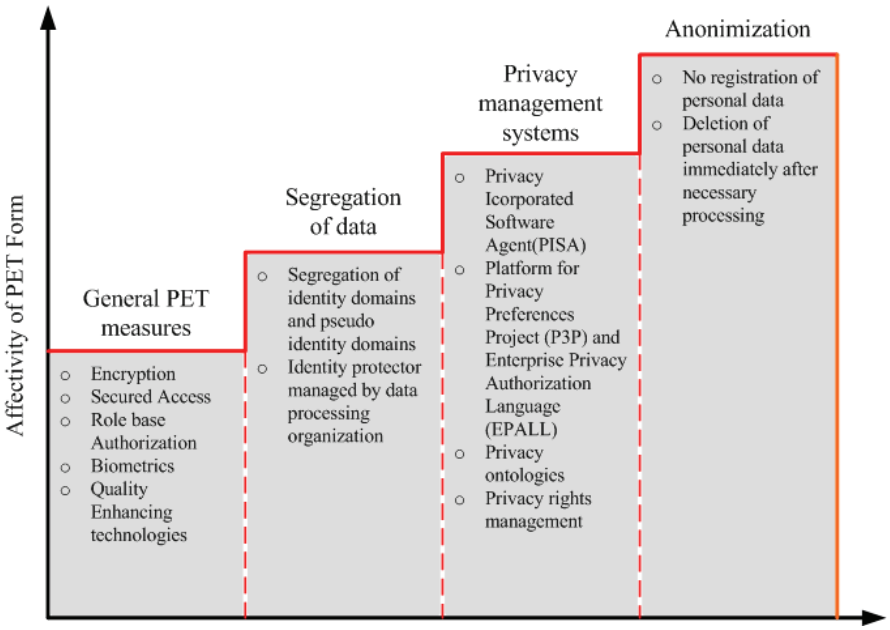


**Figure 1: staged effectiveness of PET (including technologies used per stage)**

Each of the clusters can be applied individually or in combination with each other. In combination they are proposed to be more effective.

### 7.3 How to protect privacy?

Adequate levels of data protection require the implementation of a coherent set of different types of (security) measures. We distinguish between organizational/procedural and technical measures and between 'ex ante' and 'ex post' measures.

Organizational measures are measures for designing an organization structure that creates conditions for protection of personal data. Examples are:

- the existence of a privacy policy,
- the implementation of Data Life Cycle Management
- definition of functions with specific roles and authority
- segregation of functions in order to create an internal system of checks and balances

Technical measures are logical and physical measures to apply with regard to information systems (such as access control, storing the use of data). Application of PETs belongs to technical measures (see figure 1). It is important to realize that the application of Pets may/will lead to 'migration of controls', which is the transfer of organizational measures to technical measures.

'Ex ante' measures create organizational and technical conditions, which create a system for trustworthy processing of personal data (e.g. a system of authentication, access controls etc); through 'ex post' measures the correct functioning of the controls have to be established (e.g. logging, audit trails, monitoring).

### 7.4 Why should a company invest in privacy protection?

A privacy incident can broadly be defined as an event in which personal data are misused. These events can be the intentional but illegal sale of customer data, the loss of equipment with personal

data, and steeling of personal data. There is little information available about the real costs of privacy and privacy incidents: it is still an under-researched area. The personal records stolen in privacy incidents are however significant. The Privacy Rights Clearinghouse, which keeps record of the privacy incidents in the United States, reports about 700 privacy incidents with over 307 million personal records stolen from 2005 up until 2007 [Privacy Rights Clearinghouse 2007]. On average 440 personal records were stolen with a minimum of 10 records and a maximum of 94 million records. This site also shows that privacy incidents happen on a daily basis. The number of privacy incidents is still increasing.

There are different reasons for an organization to provide adequate privacy protection. First, organizations have to comply with the law. In the Netherlands the introduction of the Personal Data Protection Act (*Wet bescherming persoonsgegevens*/WBP) in 2001 in accordance with the European Data Protection Directive 95/46 of 1995 affects all organisations in the public and private sectors. The Act covers computerised and non-computerised data processing, and requires that the parties involved in data processing ensure that WBP rules are correctly applied.

The legal approach in justifying privacy protection in organizations is currently the dominant approach. There are however also straightforward economic arguments to invest in privacy protection. Privacy breaches appear to be costly. Breaches will reach the press and will probably damage the company's brand(s) and reputation. As a result they may affect its market position and lead to loss of existing customers. Costs have to be incurred to recover from this: public relations costs, involvement of (senior) management, redesign of information systems, training of users etc. There is little emperical research on the costs of privacy protection and privacy breaches. Two studies in the USA present data of US based companies [Ponemon 2004] [Ponemon 2007].

The 2004 IBM & Ponemon study contains responses of 44 U.S.-based multinational companies. Each organization was asked to estimate its direct (direct cash-outlay), indirect (other resources spent) and opportunity costs (costs of lack of compliance) related to privacy and data protection in 2004. Table 1 gives an estimate of the average total spend per organization by cost category for all the participating organizations (in 2004 US$).

| Cost category | Direct | Indirect | Opportunity | Total Costs |
|---|---|---|---|---|
| Total spending estimates | 2,415,341 | 2,297,643 | 2,768,513 | 7,481,497 |
| Percentage Spend by category | 32% | 31% | 37% | 100% |

**Table 1: Average privacy cost per company in the 2004 survey**

Where the 2004 study focuses on how much companies spend on privacy protection, the 2007 Ponemon Benchmark study examines the costs of a data breach incurred by 35 organizations. The reported number of individual records breached ranged from less than 4000 records to more than 125,000 records from companies in 15 different industry sectors. The most important conclusions from this study are:

- Data breach costs continue to increase: The total average costs of a data breach grew to $197 per record compromised, compared to $138 in 2005 and $ 182 in 2006. The average total reported costs per company was more than $6.3 million per breach, with a range from $225,000 tot $35 million[3].

- Costs of lost business continue to grow to $128 from $75 per record compromised in 2005, representing 65% of breach costs.

- The number of breaches caused by third parties such as an outsourcer or consultant is increasing (from 21% in 2005 to 40% in 2007); also the costs of a third party data breach are significantly higher: $238 per record compromised compared to $171 for internal breaches in 2007.

[3] Regulations in more than 35 U.S. states require that individuals be notified if their confidential data has been stolen, lost or compromised (see: http://ncsl.org/programs/lis/cip/priv/breach.htm )

– The cost of lost business, being the result of breaking customer trust, is increasing from $75 in 2005 to $128 in 2007 per record compromised. The research shows that the negative publicity that is the result of a data breach incident causes reputation effect that may cause a number of customers to end their relationship with the company; also customer acquisition becomes more difficult.

– After a data breach companies frequently implemented technology solutions to protect privacy sensitive data, in particular encryption and data loss prevention solutions.

## 7.5 The Business Case for PETs

As said, the business interest for privacy is limited. Privacy is often embedded in general security measures. Also the use of PETs is limited. Privacy laws exert little pressure on organizations to really put PETs into use. Only in a few cases the law refers to PET, however the decision makers are left free what to choose as protective measures. This is an undesirable situation, not only from a societal perspective but also from a business perspective.

As a result of widespread digitization, organizations process more and more personal data electronically, whereby the connection of databases also makes personal data increasingly accessible.

This may be at odds with the EU privacy directives and with customers' expectation about how an organization should take care of their (privacy-) sensitive data. It is therefore important to find a good balance between data protection and efficient and effective data processing. Providing guarantees for data protection should in principle not form an obstacle to an efficient and effective organization. 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. The basic driver to invest in PETs is their potential to avoid "privacy incidents" and so to reduce the damage caused by privacy breaches.

Privacy breaches may impact an organization in different ways. Tsiakis and Stephanides [Tsiakis and Stephanides 2005] distinguish direct, short-term, and long-term economic consequences:

- Direct consequences are the costs for repairing or changing systems, costs of stopping or slowing down production or processes, costs of legal action, etc.

- Short term consequences include the loss of existing customers, the severance of contractual relations, and the loss of reputation. Safeguarding privacy has been identified as a major component of building trust.

- Long-term consequences include the loss of stock/ market value. DoubleClick gives an example of the latter in 2000: After a serious violation of their existing privacy statement and the lawsuit that was initiated the value of their stock fell by 20% [Chapman, Dhillon 2002]. This also happened with Choicepoint after their public announcement that they were hacked, and approximately 10 million data records were stolen. Their stock value lost 17% after this data breach.

Privacy protection is however not only a negative (i.e. a cost-) driver in a cost/ benefit analysis: in fact it represents a driver, which may both cause some costs and avoid other costs, but also may contribute to the competitive position of the firm. In particular good privacy protection, whenever properly communicated, will generally establish trust. Investing in PETs may thus provide the company with a market advantage. This is demonstrated e.g. by the Dutch company Surfboard Holding BV after their take-over of Ixquick. Ixquick, founded in 1998 in New York, hosts a meta search engine that makes use of several other search engines, like Google, Yahoo, Ask.com and classifies search results based on combined hits with those engines. Traffic had been stagnating for a number of years, until it was decided to introduce anonymity as an explicit strategy. Ixquick invested in PETs and published their new privacy policy. As a result their traffic went up with 16% in 2006 and another 17% in 2007.

An upfront business case or investment analysis serves as the economic justification for applying PETs. This should provide an answer to three key questions [Clarke 2007]:

- Do PETs make an essential contribution to the policy targets and objectives of the organization?
- What tangible and intangible benefits can PETs achieve in the organization?
- What are required investments and structural costs for PETs?

The most important consideration is the extent to which a contribution will be made to the organization's policy objectives. This consideration will often be decisive and forms the cornerstone of the business case analysis. If such a contribution is identified, the cost-benefit analysis can proceed. As the basic driver for investment in PETs is their potential to avoid privacy incidents, an upfront privacy risk analysis is needed.

With regard to the second question, the benefits offered by PET can be quantitative or qualitative. For example the application of PETs may lead to a so-called migration of controls, where procedural and organizational measures are replaced by technical measures for data protection, and the savings to be expected from such a change (staff level, equipment complexity) can be quite readily assessed. Qualitative benefits - like positive reputation effects - are hard to express in monetary terms and tricky to measure.

As for the third question, the costs of PETs vary because of the range of possible PET controls that can be implemented. Each type of PET control differs in its technique, organizational impact etc. For example in the case of data anonymisation, the one-off investments are important; structural costs have a lesser impact. Personal data are no longer processed, which means that the data protection requirements can be less stringent. The data model and implementation are simpler, precisely because no personal data are processed. There are also more standard solutions available for making personnel data anonymous. There is also no need for rolling out authentication tools, and the costs of the general security measures are also reduced. Another example is encryption, which is less expensive than the application of PKI-based smart cards protected with biometrics.

Other factors will affect the costs as well. The fact whether PETs are applied to existing systems (legacy) or are integrated into the design of new systems is important.

The information systems architecture in which PETs have to be applied also matters. A key consideration is whether there is a single centralized database or a collection of decentralized information systems and databases with possibly different data models. In a decentralized type of architecture with decentralized information systems, data and processing is spread across different not connected databases and ISs. The decentralized databases do not contain the same data. The application of PETs then relates to multiple databases, possibly with different data models, in different organizational units and so to data spread across the company. The effort needed to apply PETs is then multiplied. A similar situation exists in a 'supply-chain' type of architecture where data are exchanged between two or more organizations, where each organization has its own databases.

The conclusion is that business cases for privacy protection can be made. In PRIME we developed approaches for this. The question is why are companies not applying them? The problem is that costs of privacy protection and breaches are known and significant, and benefits are potentially even more significant, however uncertain.

Moreover, as said, here is little empirical information available. Managers seem to take a risk seeking attitude in this regard.

## References

[ANP 2007] Privacy sensitive information of 60.000 Norwegians stolen via internet. On line available.

[Borking 2007] Borking, J. (2007). Legal analysis of privacy principles [on-line] available http://petweb.nr.no/petweb/index.php/Legal_analysis_of_privacy_principles

[CBP 1995] J. Borking, 'Privacy Protecting Measures in IT Environment Necessary', *Information Management*, 10, 1998, pp. 6-11

[Chapman, Dhillon 2002] Chapman, s, Dhillon, G.S., Privacy and the internet: the case of DoubleClick, Inc. – Social Responsibility in the Information Age: Issues and Responsibilities. Hershey – Information Science Publishing, 2002.

[Clarke 2007] Clarke, R.: Business case for privacy-enhancing Technologies, 2007.Available at http://www.anu.edu.au/people/Roger.Clarke/EC/PETsBusCase.html#BC

[France 2000] E. France, 'Using Design to Deliver Privacy', in One World, One Privacy, towards an Electronic Citizenship, 22nd International Conference on Privacy and Personal Data Protection, Venice, 28-30 September 2000, p. 216

[Koorn 2004] Koorn, R.F & Ter Hart (2004): Privacy: van Organisatorisch beleid naar Privacy Enhancing Technologies. Compact (3), 15-22.

[Koorn, 2004] R. Koorn et al: Privacy-Enhancing Technologies – White Paper for Decision-Makers, The Hague 2004.

[Ponemon 2004] IBM & Ponemon Institute: The Cost of Privacy Study,' February 17 2004

[Ponemon 2007] Ponemon, PGP Corporation and Vontu Inc: 2007 Annual Study: US Cost of a Data Breach – Understanding Financial Impact, Customer Turnover, and Preventive Solutions.

[Privacy Rights Clearinghouse 2007] Privacy Rights Clearinghouse. (2007). A Chronology of Data Breaches. [on-line] available http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP

[Tsiakis and Stephanides 2005] Tsiakis and Stehanides: The economic approach of information security. Computers & Security, 24, 2005.