

# **Study on the economic benefits of privacy-enhancing technologies (PETs)**

**Final Report to**

**The European Commission  
DG Justice, Freedom and Security**

Prepared by



July 2010

## About London Economics

London Economics is one of Europe's leading specialist economics and policy consultancies and has its head office in London. We also have offices in Brussels, Dublin, Cardiff and Budapest, and associated offices in Paris and Valletta.

We advise clients in both the public and private sectors on economic and financial analysis, policy development and evaluation, business strategy, and regulatory and competition policy. Our consultants are highly-qualified economists with experience in applying a wide variety of analytical techniques to assist our work, including cost-benefit analysis, multi-criteria analysis, policy simulation, scenario building, statistical analysis and mathematical modelling. We are also experienced in using a wide range of data collection techniques including literature reviews, survey questionnaires, interviews and focus groups.

Head Office: 11-15 Betterton Street, London, WC2H 9BP, United Kingdom.

w: [www.londecon.co.uk](http://www.londecon.co.uk) e: [info@londecon.co.uk](mailto:info@londecon.co.uk)

t: +44 (0)20 7866 8185 f: +44 (0)20 7866 8186

## Acknowledgements

We would like to thank the participants of the Workshop on the Economic Benefits of PETs, hosted by DG Justice, Freedom and Security on 12 November 2009 (<http://tinyurl.com/2b23ll>), for comments on an earlier version of this report. In particular, we acknowledge valuable contributions by Mr Caspar Bowden (Microsoft) and Mr John Borking (Borking Consultancy). We also owe a debt of gratitude to Professor Alessandro Acquisti (Carnegie Mellon University) and Ms Marit Hansen (Independent Centre for Privacy Protection Schleswig-Holstein) for enlightening discussions on the subject of PETs. Finally, we are grateful to the many individuals who provided us with information on the case studies that were conducted as part of the report.

---

# Contents

Page

|                                                         |            |
|---------------------------------------------------------|------------|
| Glossary                                                | vi         |
| Executive summary                                       | vii        |
| <b>1 Introduction</b>                                   | <b>1</b>   |
| 1.1 Terms of reference                                  | 1          |
| 1.2 Approach                                            | 2          |
| <b>2 PETs: definition and technical overview</b>        | <b>7</b>   |
| 2.1 Definition                                          | 7          |
| 2.2 Classification                                      | 8          |
| 2.3 Technical overview                                  | 14         |
| 2.4 Summary                                             | 28         |
| <b>3 PETs deployment: context and issues</b>            | <b>29</b>  |
| 3.1 Outline of the economic approach                    | 29         |
| 3.2 Individuals' demand for PETs                        | 32         |
| 3.3 Data controllers' deployment decision               | 45         |
| 3.4 PETs and competition                                | 52         |
| 3.5 Patterns of technology adoption                     | 56         |
| 3.6 Summary                                             | 59         |
| <b>4 Stakeholders' views</b>                            | <b>64</b>  |
| 4.1 Risks to privacy and the state of data protection   | 65         |
| 4.2 The role of PETs                                    | 69         |
| 4.3 Promoting PETs deployment                           | 76         |
| 4.4 Summary                                             | 77         |
| <b>5 Case Studies</b>                                   | <b>79</b>  |
| 5.1 Assessing the economic benefits of PETs             | 79         |
| 5.2 Case study I: GENOMatch                             | 83         |
| 5.3 Case study II: PriPAYD                              | 96         |
| 5.4 Case study III: Pseudonymisation services           | 103        |
| 5.5 Case study IV: location-based mobile services       | 107        |
| 5.6 Case study V: CCTV privacy zones                    | 112        |
| 5.7 Case study VI: Nightclub fingerprint identification | 117        |
| 5.8 Summary                                             | 120        |
| <b>6 Business survey</b>                                | <b>125</b> |
| 6.1 Response sample and respondent profile              | 125        |
| 6.2 Use of personal information                         | 128        |
| 6.3 PETs and the benefits of holding personal data      | 133        |
| 6.4 Summary                                             | 143        |
| <b>7 Options for public-private cooperation</b>         | <b>146</b> |
| 7.1 Theoretical arguments                               | 146        |
| 7.2 Case study evidence                                 | 149        |

|     |                                                   |     |
|-----|---------------------------------------------------|-----|
| 7.3 | Views of businesses and stakeholder organisations | 151 |
| 7.4 | Summary                                           | 151 |
| 8   | Conclusions                                       | 153 |
| 9   | References                                        | 156 |
|     | Stakeholder consultation documents                | 163 |
|     | rNPV of pharmaceuticals – model parameters        | 169 |
|     | Exploratory case Studies                          | 171 |
|     | Business survey                                   | 230 |

## Tables & Figures

Page

|           |                                                                                                         |     |
|-----------|---------------------------------------------------------------------------------------------------------|-----|
| Table 1:  | Consultation with national data protection authorities, business associations and consumer associations | 4   |
| Table 2:  | FIDIS (2007) PETs classification                                                                        | 10  |
| Table 3:  | META GROUP (2005) PETs classification                                                                   | 11  |
| Table 4:  | Clarke's (2007) PETs classification                                                                     | 13  |
| Table 5:  | PETs classification after Hacothen (2009)                                                               | 13  |
| Table 6:  | Summary of PETs reviewed                                                                                | 27  |
| Table 7:  | Prices for personal data sold via underground economy servers (2008)                                    | 36  |
| Table 8:  | Overview of data tracks of the average Austrian citizen                                                 | 38  |
| Table 9:  | Determinants of e-commerce participation in the EU: regression results                                  | 43  |
| Table 10: | Summary of event studies                                                                                | 54  |
| Table 11: | Return on investment from a Privacy Management System (PMS)                                             | 82  |
| Table 12: | Success rates during the development process                                                            | 91  |
| Table 13: | Direct cost of GENOMatch to data controllers                                                            | 91  |
| Table 14: | Example of clinical trial costs                                                                         | 92  |
| Table 15: | Effect of PET                                                                                           | 94  |
| Table 16: | Please use sentence case                                                                                | 101 |
| Table 17: | Indicative cost of pseudonymisation services                                                            | 105 |
| Table 18: | Conventional LBS deployment distribution of information                                                 | 109 |
| Table 19: | LBS partitioned information                                                                             | 109 |
| Table 20: | Costs of privacy zones in CCTV systems                                                                  | 114 |
| Table 21: | Benefits of privacy zones                                                                               | 116 |
| Table 22: | Case studies summary                                                                                    | 123 |
| Table 23: | Distribution of firms by activity                                                                       | 127 |
| Table 24: | Relationship between volume and detail of customer data held by survey respondents                      | 130 |
| Table 25: | Net economic impact for businesses deploying PETs                                                       | 140 |
| Table 26: | rNPV of pharmaceuticals – model parameters                                                              | 169 |
| Table 27: | Exploratory case studies: overview                                                                      | 174 |
| Table 28: | Exploratory case studies: selected summaries                                                            | 178 |
| Table 29: | Please use sentence case                                                                                | 211 |
| Figure 1: | Potential costs and benefits of PETs deployment                                                         | xi  |
| Figure 2: | Methodological approach for considering the economic benefits of PETs deployment                        | 3   |
| Figure 3: | The 'PET-Staircase'                                                                                     | 12  |
| Figure 4: | The consequences of misjudging the risk of misuse                                                       | 34  |
| Figure 5: | Rate of identity loss events (2000-2008)                                                                | 35  |
| Figure 6: | Consumer risk aversion                                                                                  | 39  |
| Figure 7: | Perceived security of transactions over the Internet                                                    | 40  |
| Figure 8: | E-commerce transactions and consumer concern in the EU (2008)                                           | 42  |
| Figure 9: | E-commerce transactions and broadband penetration in the EU (2008)                                      | 43  |

---

## Tables & figures

Page

|                                                                                                                     |     |
|---------------------------------------------------------------------------------------------------------------------|-----|
| Figure 10: Awareness of tools or technologies improving data security                                               | 44  |
| Figure 11: The 'S-curve'                                                                                            | 57  |
| Figure 12: Distribution of firm privacy valuations ( $x_i$ )                                                        | 58  |
| Figure 13: Potential costs and benefits of PETs deployment                                                          | 62  |
| Figure 14: Are the risks to privacy and the protection of personal data associated with online activity increasing? | 67  |
| Figure 15: Is the deployment of PETs an effective means of minimising the risks associated with online activity?    | 69  |
| Figure 16: Is the deployment of PETs currently widespread?                                                          | 70  |
| Figure 17: Has the deployment of PETs changed significantly over the past 5 years?                                  | 71  |
| Figure 18: To what extent could the deployment of PETs yield economic benefits to data controllers?                 | 72  |
| Figure 19: To what extent could the deployment of PETs yield non-economic benefits to data controllers?             | 74  |
| Figure 20: Factors limiting PETs deployment                                                                         | 75  |
| Figure 21: Classification scheme for business case techniques                                                       | 81  |
| Figure 22: The stages of drug development                                                                           | 84  |
| Figure 23: GENOMatch system architecture                                                                            | 86  |
| Figure 24: Risk-adjusted NPV of drug X                                                                              | 93  |
| Figure 25: Current PAYD model                                                                                       | 98  |
| Figure 26: Black box, high-level specification                                                                      | 99  |
| Figure 27: Privacy-friendly PAYD model                                                                              | 99  |
| Figure 28: LBS with location intermediary                                                                           | 109 |
| Figure 29: Privacy zones in CCTV                                                                                    | 113 |
| Figure 30: No. of responses to business survey per Member State                                                     | 126 |
| Figure 31: Size distribution of no. of employees of respondents                                                     | 128 |
| Figure 32: Type of personal data held                                                                               | 129 |
| Figure 33: Number of records, by data type                                                                          | 130 |
| Figure 34: Type of personal data (customers, suppliers 3rd parties), by business size                               | 131 |
| Figure 35: Number of records, by company size                                                                       | 132 |
| Figure 36: Type of personal data, by sector                                                                         | 133 |
| Figure 37: Overall benefit of personal data, by size of data controller                                             | 134 |
| Figure 38: Benefit of personal data on customers, by size of data controller                                        | 134 |
| Figure 39: Privacy risk to businesses                                                                               | 136 |
| Figure 40: Net economic impact of PETs                                                                              | 137 |
| Figure 41: Awareness of PETs                                                                                        | 138 |
| Figure 42: Awareness and perceived benefits                                                                         | 139 |
| Figure 43: Effectiveness of PETs                                                                                    | 140 |
| Figure 44: Awareness and perceived effectiveness                                                                    | 141 |
| Figure 45: Factors preventing deployment of PETs                                                                    | 142 |
| Figure 46: Consumer concern and business awareness of PETs                                                          | 143 |

---

## Tables & Figures

Page

|                                                                                        |     |
|----------------------------------------------------------------------------------------|-----|
| Figure 47: Users of FinanzOnline (as of March 2009)                                    | 181 |
| Figure 48: Proportion of sales tax return filings via FinanzOnline (as of April 2009)  | 181 |
| Figure 49: Proportion of income tax return filings via FinanzOnline (as of April 2009) | 182 |
| Figure 50: Electronic file exchange via EDIAKT                                         | 184 |
| Figure 51: Two examples of EDIAKT II objects                                           | 185 |
| Figure 52: EDIAKT metadata                                                             | 186 |
| Figure 53: Average usage of SRF filled in through electronic system                    | 195 |
| Figure 54: Screenshot personal information held by TNS Infratest                       | 203 |
| Figure 55: Architecture of genome projects database system                             | 207 |
| Figure 56: The technological architecture of e-school system                           | 210 |
| Figure 57: Schools in Estonia (and Sweden) using the eSchool system (September 2009)   | 211 |
| Figure 58: The CdB certificate                                                         | 225 |
| Figure 59: The one-stop-shop concept                                                   | 226 |
| Figure 60: Distribution of sectors across Member States                                | 232 |
| Figure 61: Type of personal data held on CUSTOMERS, by business size                   | 233 |
| Figure 62: Type of personal data held on STAFF, by business size                       | 233 |
| Figure 63: Type of personal data held on SUPPLIERS, by business size                   | 234 |
| Figure 64: Type of personal data held on 3rd parties, by business size                 | 234 |
| Figure 65: Benefit of personal data on suppliers, by size of data controller           | 235 |
| Figure 66: Benefit of personal data on staff, by size of data controller               | 235 |
| Figure 67: Benefit of personal data on 3rd parties, by size of data controller         | 236 |
| Figure 68: Average benefit of personal data by sector                                  | 237 |
| Figure 69: Awareness of PETs - SMEs                                                    | 238 |
| Figure 70: Awareness of PETs – non-SMEs                                                | 238 |

## Glossary

### Terminology abbreviations

|       |                                                              |
|-------|--------------------------------------------------------------|
| CBA   | Cost-benefit analysis                                        |
| COBRA | Cost, benefit and risk assessment                            |
| CZK   | Czech koruna                                                 |
| DKK   | Danish krone                                                 |
| DP    | Data protection                                              |
| ICO   | Information Commissioner's Office (UK)                       |
| ICPP  | Independent Centre for Privacy Protection Schleswig-Holstein |
| IP    | Intellectual property                                        |
| LBS   | Location-based service                                       |
| NPV   | Net present value                                            |
| PAYD  | Pay-as-you-drive                                             |
| PETs  | Privacy-enhancing technologies                               |
| PMS   | Privacy management system                                    |
| rNPV  | Risk-adjusted net present value                              |

### Member State abbreviations

|    |                |    |                |
|----|----------------|----|----------------|
| CZ | Czech Republic | IT | Italy          |
| DK | Denmark        | HU | Hungary        |
| DE | Germany        | MT | Malta          |
| EE | Estonia        | NL | Netherlands    |
| ES | Spain          | AT | Austria        |
| IE | Ireland        | UK | United Kingdom |



## Executive summary

### Subject of the study

The European Commission DG Justice, Freedom and Security commissioned London Economics to undertake a study on the economics benefits of Privacy Enhancing Technologies (PETs) for organisations and institutions using and holding using personal data, the data controllers. A particular focus of the study is the situation with regards to SMEs. Further specific issues examined by the study include:

- whether/ how the impact of PETs can be measured; and
- whether cooperation/joint action such as Public Private Partnerships of data controllers with national authorities or international organisations would enhance economic benefits.

The study covers 12 EU Member States that were selected after consultation with DG Justice, Freedom and Security. They are:

- The Czech Republic;
- Denmark;
- Germany;
- Estonia;
- Spain;
- Ireland;
- Italy;
- Hungary;
- Malta;
- the Netherlands;
- Austria; and
- the United Kingdom

### The approach to the study

London Economics used a two-pronged approach to the analysis:

The approach was two-pronged. **First, the theoretical part** of the study provides a framework for the understanding of PETs and the deployment decision faced by data controllers. This part is split into 2 Sections:

- The first provides an overview of the technologies that together form the ‘PETs universe’ and discusses different classifications for PETs that have been proposed in the literature.
- The second looks in greater detail at the determinants of PETs deployment from an economic perspective.

The theoretical part is based on a review of the relevant academic literature. It spans the fields of security and innovation economics, competition economics, IT security and theories of innovation. Given the dearth of empirical data on many issues related to PETs, results obtained in the experimental economics literature contributed significantly to our understanding of the issues.

**The empirical part** of the study is based on three separate data collection exercises:

- The first is a stakeholder consultation exercise, during which London Economics conducted interviews with representatives of three stakeholder groups (national data protection authorities, business associations and consumer associations/advocacy bodies) in the 12 selected Member States.

The consultation focused on stakeholders' perceptions about the privacy-risk situation in their country, the spread of PETs, the economic and non-economic benefits of PETs, as well as the options for cooperation between the public and private sectors to enhance privacy protection through PETs.

Responses were received from the data protection authorities in all 12 Member States as well as from 8 consumer associations and 5 business associations.

- The second data collection exercise is a survey of businesses in the 12 Member States. The survey gauged respondents' views on the use of PETs and personal data as well as the associated costs and benefits.

A total of 1,337 responses were received, covering all 12 Member States. The survey response sample includes a large number of SMEs (defined as businesses with fewer than 250 employees). The latter account for 73% of all responses and the full survey response sample covers all major sectors of the economy, with the service sector predominating.

- The third data collection exercise consists of detailed case studies. The case studies were conducted in a two-stage process:

In a first stage, 20 exploratory case studies were conducted across 10 of the selected Member States to provide a concrete context for the insights emerging from the other strands of the analysis (theoretical and survey-based) and to identify candidates for the more detailed case studies following at the next stage.

In the second stage, 6 case studies were selected to illustrate in greater detail the issues surrounding the PETs deployment faced by data controllers. Each case study includes:

- a detailed discussion of the PETs in question;
- an analysis of the motivation behind the deployment of PETs;
- an assessment of the costs and benefits of PETs deployment for the data controller; and
- an investigation into the role played by public sector bodies in the context of the deployment.

In a **last part**, based on the theoretical and empirical evidence collected through the different analytical steps, the study provides a high-level overview of the options for cooperation between the public and private sectors to enhance the benefits of PETs for data controllers.

## **PETs: definition and technical overview**

PETs is a complex concept that comprises a broad range of individual technologies at different levels of maturity. PETs are constantly evolving, often in response to ever more advanced threats.

Data security technologies are PETs if they are used to enhance privacy. But, it should be noted that they can be used in inherently privacy-invasive application, in which case they cannot properly be counted as PETs.

Data minimisation and consent mechanism are an important part of PETs. Many PETs combine various technologies, including data protection tools (e.g., encryption) and ‘pure’ PETs (e.g., data minimisation tools) to form integrated PET systems of varying complexity.

A variety of different classifications of PETs has been proposed, primarily based on technological characteristics. A classification according to economic characteristics remains elusive and may be impossible because of the context-specific nature of the economic effect of PETs.

In interactions with data controllers and other stakeholders, the complexity of the PETs concept might act as a barrier to understanding the nature of the technologies and their usefulness. The use of more specific terminology (e.g., ‘data protection tools’, ‘data minimisation tools’, ‘consent mechanisms’, etc.) might be preferable in many cases.

## **PETs deployment: context and issues**

The decision by a data controller of whether to deploy PETs is multi-faceted and contingent on external factors, including the legal and regulatory environment, as well as the economic costs and benefits of PETs in specific applications.

### **Individuals’ demand for PETs**

In theory individuals’ demand for PETs is a potentially important driver of deployment. Whether individuals value PETs depends on their assessment of the usefulness of PETs and the risk posed by the disclosure of personal data. This risk can be the risk of tangible (e.g. financial) losses as well as the risk of privacy invasion that causes harm to individuals at a more intangible level.

If individuals are well informed and acting rationally, the demand for increased PETs deployment is a function of:

- individuals’ risk aversion;
- the risk of data loss/privacy invasion; and
- the efficacy of PETs in reducing the risk.

The evidence on demand response is weak. Surveys indicate relatively high levels of concern about privacy in online settings and research has shown that consumers are willing to pay a premium for privacy under certain conditions.<sup>1</sup>

However, stakeholders who were consulted for the present study attest to a widespread indifference on the part of individuals when it comes to actual buying decisions and there is also evidence from experimental studies that support this view.<sup>2</sup>

Empirical evidence also suggests that the cost of reputation loss (in terms of stock market impact) following incidents of data loss is relatively low and dissipates quickly.<sup>3</sup>

Behavioural economics has identified various *behavioural biases* that can explain the lack of a demand response to privacy incidents that would act as an incentive for increased PETs deployment. The most important one relates to the weak link between actions (the disclosure of personal data) and consequences (e.g., nuisance mail, fraud, theft, profiling etc.).

### Data controllers' deployment decision

Data controllers' deployment decision is determined by many of the same factors that shape the demand by individuals, including the fear of data loss, which in the case of data controllers can involve data on employees, suppliers, customers, etc.

In addition, and to the extent that there is a demand for PETs, data controllers may gain a competitive advantage through PETs. The assumption is that good privacy protection can serve as a unique selling point as customers flock to the provider with the best PETs. There is little evidence that this is actually happening in the consumer market, but competition as a driver of PETs deployment seems to play an important role in the business-to-business market.

However, data controllers also benefit from the electronic processing of personal data. The main sources of benefit are greater efficiency in carrying out processes electronically; personalising goods and services; and exploiting personal data in the production of new goods and services.

Overall, this means (assuming that PETs deployment is to some degree discretionary) that PETs may involve a trade-off for data controllers: the availability of personal data as an economic resource can create benefits for data controllers, the individuals who supply the data, and, at least in some cases, the wider public.

Using PETs might reduce these benefits. Deploying PETs requires upfront investments in the technology, as well as training and ongoing maintenance. Even though the use of PETs can reduce costs over time, the direct costs of deployment are the most immediate type of costs that has to be weighed against the potential benefits.

---

<sup>1</sup> See Tsai et al. (2007).

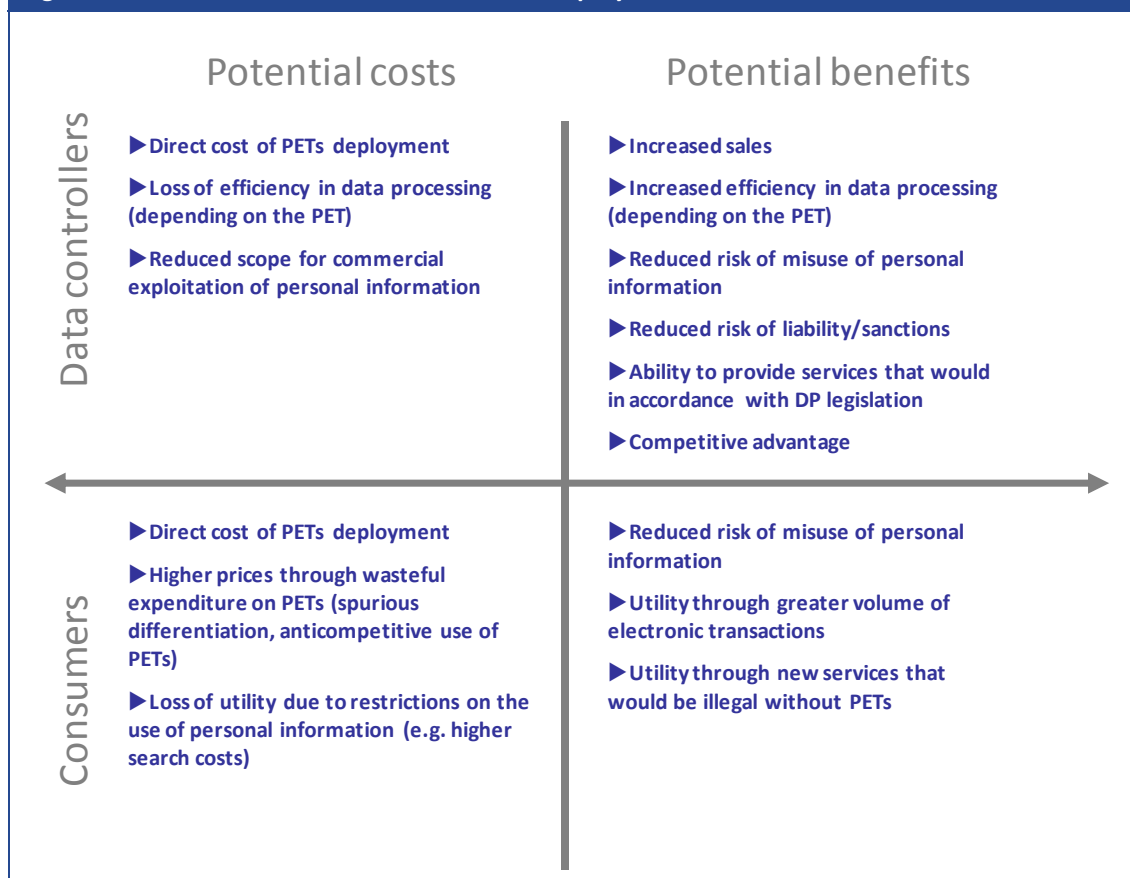
<sup>2</sup> Examples are Hui et al. (2006) and Berendt et al. (2005).

<sup>3</sup> Acquisti et al. (2006) find a cumulative drop in share prices per privacy incident of close to -0.6% on the day following the event, which equates to an average loss of approximately € 7.4 million (\$ 10 million) in market value.

Moreover, since the costs and benefits of PETs are to some extent uncertain, firms might postpone deployment while waiting for more information.

On the basis of the preceding considerations, the potential costs and benefits associated with PETs deployment can be summarised as follows:

**Figure 1: Potential costs and benefits of PETs deployment**



Source: London Economics

### Potential market failures leading to sub-optimal deployment

Market imperfections, which can include asymmetric information, externalities, lack of information sharing about privacy risks and coordination failures, mean that the individually rational decisions of data controllers do not necessarily lead to the optimal level of PETs deployment.

This implies that there may be benefits from PETs deployment which data controllers are currently not realising. To the extent that market failures are an issue in the context of PETs, this points to a potential role for the public sector to help data controllers overcome the barriers holding back PETs deployment.

## **Patterns of technology adoption**

PETs in general are relatively new technologies, and new PETs are constantly being developed. Economic theories of technology adoption suggest that the deployment levels for new technologies are initially low. Deployment rates then pick up as the technologies mature or as information about the technologies spreads among potential users. This leads to an S-shaped deployment rate, which could help to explain why many PETs are currently not widely used.

## **Stakeholders' views**

Data protection authorities, business associations and consumer advocacy groups are in agreement that:

- the risks associated with the use of personal data in electronic form is recognised as serious and growing;
- consumer awareness of these risks is seen as low; and
- PETs are an effective means of protection against these risks.

While data protection authorities see the cost of PETs as an important impediment to their deployment, business associations consider the lack of a political imperative as more important.

Business and consumer organisations emphasise that public bodies are to blame for some of the most notorious cases of data loss in recent years. Business associations also highlight the refusal of consumers to pay for PETs as a reason for low deployment rates.

Business and consumer associations also stress the international dimension of the risks to privacy, arguing that, when it comes to data protection provisions, the system is only as strong as the weakest link in the chain, which might be a jurisdiction outside the European Union.

A disconnect is evident in the views of data protection authorities on the role of individuals' response to PETs as a driver of deployment rates:

- on the one hand, they tend to state that both overall adoption rates and consumer awareness of PETs are low;
- on the other hand, they claim that one of the main benefits associated with the wider deployment of PETs would be an increase in consumer trust.

Overall, many of the representative bodies with a remit that incorporates PETs are convinced of the need for PETs, but benefits are often asserted rather than demonstrated with evidence.

## **Case Studies**

The six detailed case studies presented in the study illustrate the diversity of PETs and the way their benefits are dependent on the circumstances of their deployment.

The case studies underline the fact that individuals do indeed face substantial threats to their privacy from a number of sources. Personal data ranging from movement patterns to medical histories and genetic information is customarily collected and stored by data controllers across a

wide range of industries, from nightclub operators and insurers to mobile phone operators and pharmaceutical companies.

In practice, individuals often have little choice over whether to disclose personal data or not as not doing so would result in considerable inconvenience or prevent them from using certain services altogether.

This means there is a clear need for PETs across a wide range of applications. The examples presented in the present study show that most PETs are composite technologies that use simple security measures (encryption, access management) in conjunction with other mechanisms to enhance overall privacy.

Among the case studies, some types of PETs appear more widespread than others:

- Data minimisation is a very important aspect of PETs that is realised to varying degrees in the technologies we analysed.
- In contrast, mechanisms to obtain consumer consent seem play a relatively minor role.

PETs are application-specific. While some have been designed to fit a narrow purpose, many others can be used in a broader range of applications. Which type is more likely to be used by data controllers is a priori unclear.

PETs do not have to be complex. In 2 of the cases we analyse, the PET simply suppresses the collection of sensitive personal data by the data controller. (Note that 'complexity' here refers to the concept of the PET, not the technical details of its implementation.)

It also appears that simple PETs, which do not reduce the functionality of the application they are used with, face no opposition from data controllers.

However, our case studies illustrate clearly that data controllers are often reluctant to deploy PETs. The main reasons are:

- a perceived lack of benefits; and
- the potential for diminished usefulness of personal data if PETs are deployed.

An important insight, confirming the views of many stakeholders, is that consumer pressure typically is not an important driver of PETs deployment. Intermediaries such as data protection officers or consumer representatives, on the other hand, can play a very important role in incentivising PETs deployment.

The case studies provide strong evidence that the role of the public sector is very important: a lack of enforcement of existing privacy rules and/or inadequate sanctions for infringements appears to depress deployment rates in many cases. The requirements for consent and proportional data use in particular appear insufficiently enforced.

The case studies also suggest that data controllers in some areas may not be using the best available technology to ensure individuals' privacy is protected. The need to comply with privacy legislation is often the most effective driver of PETs deployment.

There is a lot of evidence that the public sector is using a variety of approaches to effectively cooperate with data controllers to increase PETs deployment. This support can range from the endorsement of certain PETs by public bodies to active support of the development of PETs, official certification and pioneering deployment by public bodies. The case studies show that, with the right incentives, data controllers work effectively together with public bodies to spread PETs deployment.

## **Business survey**

The business survey shows that personal data of varying detail is widely held by businesses. This is true for SMEs as well as larger businesses, although larger businesses tend to hold more detailed data.

A majority of the respondents hold detailed personal data on customers. Over 50% of companies with more than 250 employees hold personal data on more than 1,000 individuals. The degree of detail generally increases as the number of records per database increases. It is also evident that certain sectors are more data-intensive than others. Financial services, social services and health-related services, as well as professional and ICT services all report above average data use.

Interestingly, a significant minority of businesses report no benefits from the personal data they hold. Overall, the larger the business, the greater the perceived benefit. The sectors that hold detailed data, such as financial and ICT services also report relatively large benefits. Data on customers are seen as the most beneficial type.

Businesses perceive only a low to medium risk of harm arising from the misuse of personal data (or the threat thereof). However, larger businesses see the risk as significantly greater than SMEs. A small proportion of companies report that these concerns have prevented them from developing new business activities.

The survey provides clear evidence that SMEs judge the benefits of PETs deployment considerably lower than non-SMEs. Partly, this is likely to reflect the fact that SMEs have less need for PETs owing to their less intensive data use. On the other hand, the survey provides evidence that they are less informed about PETs, which might bias their perceptions on their usefulness.

When considering businesses' awareness of PETs, one observes that this depends largely on the type of technology in question. Filters and blockers are very widely used (83% of respondents report using them), and the use of encryption tools (49%) and evidence erasers (53%) is also widespread. Information tools and administrative tools, on the other hand, are less well known, especially by SMEs. This is potentially problematic as some core PETs, such as P3P, fall into these categories.

The survey shows that the level of information businesses have about PETs affects their perception of benefits. The more businesses know about PETs, the greater they judge the net benefits of deployment.

This can be interpreted as evidence of an evolutionary learning process. As technologies become more mature, information about their usefulness spreads. The relatively widespread use of filters and blockers would suggest that these are more mature technologies than some of the other categories of PETs. A further implication is that there might be a role for public bodies to increase



awareness about technologies that are proven to enhance privacy, but have not yet found wide acceptance in the market.

That PETs are seen as effective by a large majority of businesses suggests that businesses could be won over if they have adequate information. In general, the more experience businesses have with PETs, the greater the reported perception of their effectiveness.

High costs and consumer acceptance of the status quo are cited as the most important factors limiting PETs deployment by larger businesses. For SMEs the fact that they do not consider PETs as applicable to their business is the most important barrier.

## Options for public-private cooperation

The evidence suggests that the public sector has a very important role to play in assisting data controllers if the benefits of PETs are to be realised. Four main areas in which public sector initiatives can complement the efforts of private data controllers to enhance privacy can be identified:

- setting and enforcing privacy standards;
- supporting PETs development through direct or indirect funding;
- providing credentials and official endorsements; and
- promoting PETs through information campaigns and ongoing contact with data controllers

A more speculative role for cooperation between the public and the private sector based on theoretical considerations is in the coordination of investments in PETs, which might increase the overall effectiveness of deployment.

Providing information about PETs to data controllers continues to be an important task for public bodies such as national data protection authorities. The business survey showed that awareness of state-of-the-art PETs is still low, especially among SMEs. Concerns about costs and doubts about the applicability of PETs, again frequently observed among SMEs, are other areas that could be effectively addressed by information campaigns.

Regarding the function of the public sector, it is important to consider its role in setting an example of good practice in upholding privacy standards. A number of respondents to the business survey were sceptical about the role of public sector in promoting PETs because of a perception that public bodies are among the main culprits when it comes to failures to protect personal data and ensure user privacy.

## Conclusions

The benefits of PETs are technology-specific on the one hand and application-specific on the other.

There exists a wide variety of PETs, comprising many different approaches to enhancing individuals' privacy. The costs and benefits thus vary across technologies. While some PETs involve virtually no additional costs compared with the privacy-invasive status quo, others require a substantial financial investment from data controllers.

It is important to note that the benefits of the same PET can differ across applications. Factors such as whether the PET is deployed by a large or a small business, whether the data controller has to adjust its business model to deploy the PET or whether the data controller operates in a market where consumer demand is sensitive to PETs deployment all affect the benefits that may be derived from PETs.

The complexity of the issue of economic benefits makes it impossible to quantify the economy-wide benefits to data controllers of PETs deployment. Rather, the evidence suggests that the net economic benefit of PETs deployment needs to be assessed on a case-by-case basis.

There is little evidence that the demand by individuals for greater privacy is driving PETs deployment. The reasons for this include the uncertainties surrounding the risk of disclosure of personal data, a lack of knowledge about PETs, and behavioural biases that prevent individuals from acting in accordance with their stated preference for greater privacy.

Data controllers, on the other hand, can derive a variety of benefits from holding and using personal data, including the personalisation of goods and services, data mining, etc. To the extent that PETs limit the ability of data controllers to use personal data, this acts as a disincentive for deployment.

In particular, data controllers often favour mere data protection to protect themselves against the adverse consequences of data loss over data minimisation or consent mechanisms which can impede the use of personal data.

However, the demand for PETs deployment is much more an important driver in the business-to-business market as well as in settings where individuals are represented by intermediaries that articulate privacy concerns towards data controllers.

Even in cases where PETs deployment is potentially beneficial for data controllers, deployment rate may still be low. The uncertainty of some of the costs and benefits of PETs also explains why firms might rationally postpone the deployment of PETs while waiting for more information, in order not to limit their future choices.

In addition, there are certain market failures, such as the existence of externalities in PETs deployment, which lead to sub-optimal deployment rates.

Finally, as already noted theories of technology adoption suggest that the adoption rates of PETs may follow an S-shaped pattern, which means that current, low deployment rates could pick up quickly in the future as the technologies mature and become better known.

The evidence considered in this study suggests that there is a role for the public sector in helping data controller realise the benefits of PETs. This can take various forms. The most effective appear to be official endorsements of PETs, including through pioneering deployment and official certification schemes, and direct support for the development of PETs, through subsidies to researchers (e.g. the European Framework Programmes).

SMEs are using fewer PETs, and are less convinced of the benefits of PETs, than larger businesses. At the same time, SMEs often store personal data from which they derive no economic benefit.

However, SMEs also use less personal data, which suggests that a proportional response to promoting the use of PETs by SMEs will be required.



# 1 Introduction

This section introduces the terms of reference for this study and outlines in broad terms the approach to undertaking the analysis.

## 1.1 Terms of reference

London Economics were commissioned by EC DG Justice, Freedom and Security in June 2009 to undertake an analysis of the economic benefits associated with Privacy Enhancing Technologies (PETs).

The protection of personal data is an established objective of the European legal framework.<sup>4</sup> As part of this framework, Article 17 of the Data Protection Directive enshrines the obligation of data controllers to implement “appropriate technical and organisational measures” and to ensure a level of security appropriate to the nature of the data and the risks of processing it. The European Commission considers that wider use of PETs would improve privacy protection as well as help data controllers comply with data protection rules.

The central question addressed by the study is whether the deployment of PETs results in economic benefits to the deployer (data controller), with special attention being paid to the situation of SME data controllers.

Further issues to be investigated include:

- the effectiveness of PETs;
- whether/ how the impact of PETs can be measured; and
- whether cooperation/joint action such as Public Private Partnerships of data controllers with national authorities or international organisations would enhance economic benefits.

The study is concerned with the assessment of the *economic* benefits of PETs. While this task requires an understanding of the technologies in question, a technical evaluation of these technologies is not part of the study.

Equally, it is important to stress that the focus of this study is limited to (micro)economic benefits, i.e. the incentives that data controllers have to deploy PETs. The study is not directly concerned with the wider benefits of PETs for the economy as a whole or society in a broader sense. Nor does

---

<sup>4</sup> The seminal provisions are:

- Article 8 of the Charter of Fundamental Rights of the European Union establishing the right to the protection of personal data as a fundamental right;
- Directive 95/46/EC of 24th October 1995 concerning the protection of natural persons in respect of the processing of personal data and the free movement of such data (the Data Protection Directive);
- Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); and
- Regulation (EC) 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

the study address other important aspects of the PETs deployment decision, such as the policy environment, questions about the consistency and adequacy of existing legislation at EU level and in the Member States. The role of data protection authorities and other enforcement bodies, the adequacy of current enforcement levels, available sanctions, etc. will be discussed only in the context of stakeholders' perceptions of these issues.

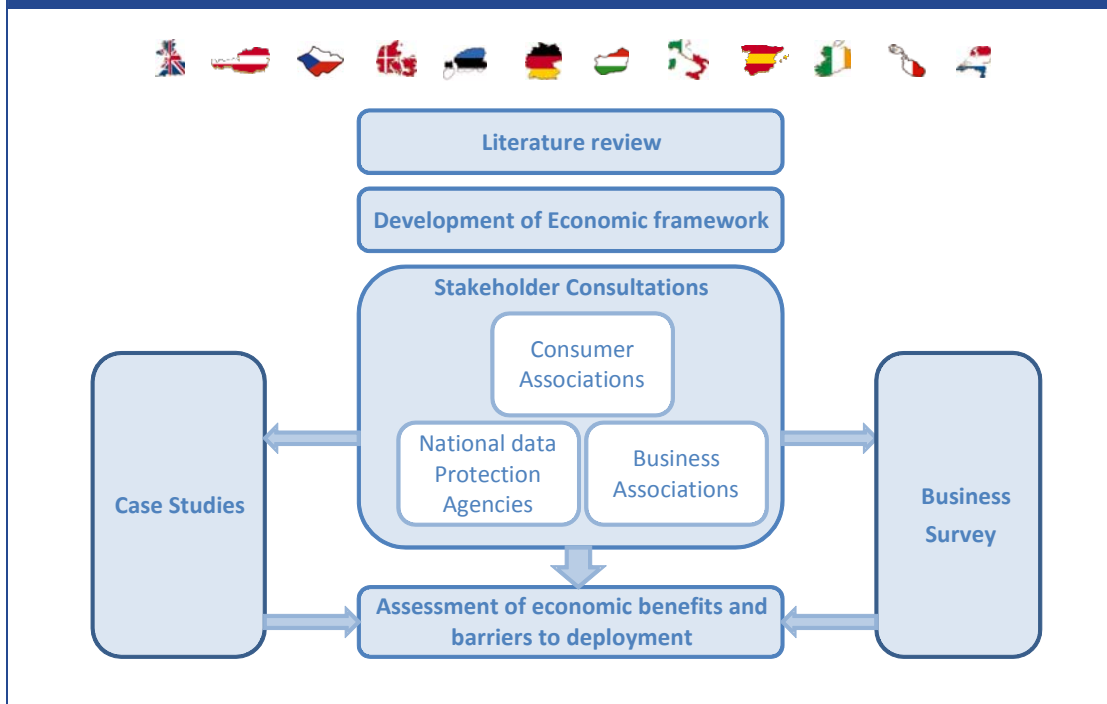
The report is structured as follows:

- A brief outline of the approach taken in this study is provided in the remainder of the present section.
- In Section 2, we introduce the definition of PETs and provide an overview of the 'PETs universe', i.e. the types of technologies that fall under the definition.
- Section 3 contains a review of the academic and policy related literature and sets out the economic context for the deployment decision faced by data controllers.
- In Section 4, we present the findings of the stakeholder consultation exercise with national data protection authorities, consumer and business associations across 12 EU member States.
- In Section 5, we provide six detailed case studies highlighting some of the central issues around the deployment of PETs by public and private sector organisations in the EU.
- Section 6 contains the analysis of the business survey that supplies information on the perceptions and use of PETs by businesses in the different Member States.
- Section 7 summarises our findings regarding the potential for cooperation between the private sector and public bodies to further the deployment of PETs.
- Finally, overall conclusions and recommendations are provided in Section 8.

### 1.2 Approach

In this sub-section, we provide information on the methodological approach adopted for answering the research questions described above. (See Figure 2 for a summary overview).

Figure 2: Methodological approach for considering the economic benefits of PETs deployment



Source: London Economics

### 1.2.1 Literature review

To provide a rounded assessment of the economic benefits associated with the deployment of PETs, London Economics undertook a detailed literature review to gain a deeper understanding of the following fundamental issues:

- whether the lack of privacy enhancing technologies results in overuse of unprotected information by data receivers and underuse of e-based transactions and information provision by individuals who are worried about the lack of protection of their information; and
- the benefits and costs that would arise as a result of the implementation of the PETs.

### 1.2.2 Economic framework

Integrating the analysis of the information collected as part of the literature review, Section 3 sets out the economic framework for the analysis of the benefits of PETs and the incentives for data controllers to deploy them. In particular, we consider:

- how the risk that personal information might be misused affects the value of PETs for consumers and data controllers;
- the benefits from using personal information that might be affected by PETs;
- the behavioural biases that affect the demand for PETs;
- the effect of PETs on competition; and
- the PETs deployment rate seen through the lens of theories of technology adoption/diffusion.

We derive a matrix of costs and benefits that can be used to identify the factors that govern PETs deployment in our case studies.

### 1.2.3 Consultation exercise

London Economics also undertook a detailed stakeholder consultation exercise across 12 EC Member States. This consultation exercise provided information on:

- the specific issues relating to the risks to privacy and the protection of personal information with online activity;
- the current view in relation to the deployment of PETs;
- the current economic benefits and costs associated with the deployment of PETs; and
- the barriers associated with the deployment of PETs.

During the consultation exercise, we contacted officials and/or representatives from the national data protection offices, business associations and consumer associations in 12 EC Member States. (See Table 1 below.)

The consultation exercise involved an electronic survey in July 2009 followed by a range of follow-up activities during August and September 2009 to boost participation in the consultation. The survey questionnaire is presented in 0 and contains a number of both closed response and open response questions. Twelve national data protection authorities, as well as five business associations and eight consumer associations participated in the consultation process. Full details of the responses and findings from the stakeholder consultation exercise are presented in Section 4 of this report.

| Table 1: Consultation with national data protection authorities, business associations and consumer associations |                                                                     |                                                                             |                                                               |
|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------|
| Country                                                                                                          | Authority                                                           | Business association                                                        | Consumer association                                          |
|  Czech Republic               | Office for Personal Data Protection                                 | -                                                                           | SOS – Sdružení obrany spotřebitelů, o.s.                      |
|  Denmark                      | DATATILSYNET - The Danish Data Protection Authority                 | The Trade association DI ITEK within The Confederation of Danish Industries | The Danish Consumer Council                                   |
|  Germany                      | Federal Commissioner for Data Protection and Freedom of Information | Bundesvereinigung der Deutschen Arbeitgeberverbände                         | 1. Stiftung Warentest<br>2. Werbraucherzentrale Bundesverband |
|  Estonia                      | Estonian Data Protection Inspectorate                               | -                                                                           | -                                                             |



|                                                                                                    |                                                                       |                                                                                                                       |                                                         |
|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
|  Spain            | Data Protection Authority                                             | AECM (Asociación Española de Comercio Electrónico y Marketing Relacional)                                             | OCU (Organización de Consumidores y Usuarios)           |
|  Ireland          | Office of the Data Protection Commissioner                            | -                                                                                                                     | -                                                       |
|  Italy            | Garante per la Protezione dei Dati Personali                          | Confindustria                                                                                                         | Altroconsumo                                            |
|  Hungary          | Office of Commissioner for Data Protection and Freedom of Information | 1. Confederation of Hungarian Employers and Industrialists (CHEI)<br>2. The Theodor Puskas Foundation (TPF) and ENISA | National Association for Consumer Protection in Hungary |
|  Malta            | Office of the Data Protection Commissioner Malta                      | -                                                                                                                     | -                                                       |
|  Netherlands     | Data Protection Authority                                             | -                                                                                                                     | -                                                       |
|  Austria        | Data Protection Commission                                            | -                                                                                                                     | Arbeiterkammer (AK Wien)                                |
|  United Kingdom | Information Commissioner's Office                                     | -                                                                                                                     | ConsumerFocus                                           |

Source: London Economics

### 1.2.4 Case studies

To complement the literature review, the development of the economic framework and the stakeholder consultation, London Economics gathered information from a number of public and private sector organisations to illustrate the deployment of different types of PETs. We focused on the same Member States as those represented in the stakeholder consultation and gathered information on the costs and benefits to the PETs deployer associated with the technology. The analysis comprised two stages:

- an initial stage, in which a wide range of different PETs was identified and portrayed, with a view to covering a suitably wide range of example from different Member States and different applications; and
- a second stage, in which six case studies, that were judged to provide the most valuable insights into the issues at hand, were analysed in greater detail.

The case studies illustrate the context of PETs deployment and the economic and non economic benefits that might accrue from their deployment according to the economic framework

developed in Section 3. The 20 case studies from stage one are included in Annex 3, whereas the six detailed case studies are presented in Section 5.

### 1.2.5 Business survey

We have also undertaken a large scale survey of businesses (containing open and closed response questions) to better understand:

- the extent to which business collect and store personal data;
- the benefits associated with that information;
- the risks to the business associated with the storage and transmission of the data;
- the potential costs and benefits associated with the deployment of PETs; as well as,
- information on the extent to which businesses are aware of and use alternative types of PETs.

Finally we asked respondents to provide some additional information in relation to the barriers and challenges associated with the deployment of PETs, as well as information on what public sector organisations might do to assist with the wider deployment of PETs.

The survey was administered online in the same 12 Member States as for the consultation exercise. The results are presented in Section 6.

### 1.2.6 Options for cooperation/joint action

The final section brings together the evidence on how cooperation between public sector bodies and data controllers in the private sector can help to enhance the benefits that data controllers derive from PETs. It summarises the findings of the previous sections and discusses the theoretical arguments as well as the empirical evidence from the case studies, the stakeholder consultations and the business survey.

## 2 PETs: definition and technical overview

### 2.1 Definition

This section reviews the definitions and classifications of PETs that have been applied by international bodies such as the European Commission, national data protection commissioners and academic researchers in the study of privacy enhancing technologies. The literature on this issue has focused on topics within computer science and law with comparatively little work having been undertaken on the economics of PETs. The challenge that this study faces, therefore, is to characterise privacy enhancing technologies in a way that permits the analysis of the economic benefits of PETs.

Privacy-enhancing technologies, or PETs, have no universally agreed definition, but existing definitions normally reflect the consensus that, to qualify as PETs, technologies have to reduce the risk of contravening privacy principles and legislation, minimise the amount of personal data being held, and/or give individuals control over information about them that is being held.<sup>5</sup>

The European Commission in its *Communication to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)* describes a PET 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.”<sup>6</sup>

Our understanding of PETs is based on this latter definition, which will be used implicitly throughout this report. While this clearly delineates the space PETs inhabit, it represents a broad definition that encompasses a large array of technologies and processes, as well as systems combining the two. It is important to think of PETs not just as pieces of software or hardware that can be mixed-and-matched, but as integrated privacy systems.

However, this means that applying the concept of “PETs” to specific technologies is not always straightforward. Specifically, it is important to stress that not all information security technologies are PETs. As the pioneering 1995 report on PETs by the Ontario data commissioner and the Dutch *Registarietkamer*<sup>7</sup> explains:

*“When organizations are asked what measures they have in place to protect privacy, they usually point to their efforts at keeping information secure. While the use of security measures to prevent unauthorized access to personal data is a very important component of privacy, it does not equal privacy protection. The latter is a much broader concept which starts with the questioning of the initial collection of the information to ensure there is a good reason for doing so and that its uses will be restricted to legitimate ones that the data subject has been advised of. Once the data have*

---

<sup>5</sup> For examples of current definitions see “Privacy by Design – An Overview of Privacy Enhancing Technologies”. Enterprise Privacy Group, 26th November 2008. Available at: <http://tinyurl.com/ykwjyjjw>.

<sup>6</sup> COM(2007) 228 final.

<sup>7</sup> Information and Privacy Commissioner, Ontario (Canada) and Registratiekamer (Netherlands), *Privacy-Enhancing Technologies: The Path to Anonymity* (Volume I), 1st August 1995. Available at: <http://tinyurl.com/yenjgns>.

*been collected, security and confidentiality become paramount. Effective security and confidentiality will depend on the implementation of measures to create a secure environment.”*

On the other hand, certain common information security technologies ostensibly fit the PET definition adopted above; encryption tools, access security tools, role-based authorisation, etc. certainly help in “preventing unnecessary and/or undesired processing of personal data”.

Moreover, such security technologies often form an integral part of more complex PETs: for example, it is easy to envisage a technology that reduces the amount of personal data required to perform a certain function and then uses encryption when transmitting the personal information that is still needed.<sup>8</sup>

However, information security technologies are not ‘pure’ PETs, as they can be used in ways that are actually privacy-invasive. Any unnecessary or unwanted collection of personal data remains an invasion of privacy, even if access to that information is well-protected.<sup>9</sup>

In this sense information security technologies often just mitigate the risk of privacy-invasive technologies. But, even then, they might in fact be harmful to privacy by engendering a false sense of security. Equally, it is conceivable that certain data security measures create new privacy risks: for example, a log of people accessing database containing personal data arguably helps preventing undesired processing, but creates a whole new database with information on individuals that constitute a breach of privacy. Overall, while information security is important and necessary in its own right, ‘proper’ PETs have to be seen as holistic solutions to the privacy problem, not technological add-ons.

## 2.2 Classification

The discussion above shows that PET is a complex concept. The line between “true PETs” and data security measures is blurred, if not in the mind of computer scientists working in the area, then certainly in the minds of consumers and practitioners in businesses and data protection authorities.

The variety of PETs and the apparent fuzziness of the concept, pose a twofold challenge for the present study:

- First, it is clear that looking at the benefits of “PETs” in an abstract manner is unlikely to be informative. Too great are the disparities between different technologies (and possibly different applications) in terms of their economic implications.
- Secondly, with respect to the large survey component of our study, it seemed – as a practical matter – difficult to communicate what the concept of PETs entails to respondents who were, in the vast majority of cases, not technical experts.

---

<sup>8</sup> An example of such a complex PET is the PriPAYD concept developed by Troncoso et al. (2007).

<sup>9</sup> See also Cranor (2003) and <http://tinyurl.com/ykwjyjjw> as above.

Both difficulties pointed to a need to further break down the concept of PETs to make it both tractable from an analytical perspective and accessible to parties, above all data controllers, who are not familiar with the discourse among experts and policymakers going back to the seminal papers on the issue in the 1990s.<sup>10</sup>

A useful classification of PETs needs to recognise that there exist disparate technologies, at different stages of development, ranging from state-of-the-art concepts not yet commercially available to long-established technologies threatened by obsolescence. In the context of our study, it is also important to note that most PETs in use today are at the lower end of the spectrum (information access management, encryption, pseudonymisation). An appropriate classification thus needs to include both high-end, pure PETs and data security technologies in a PET role (e.g., encryption technologies to prevent unnecessary/ undesired processing of personal data).

Several classifications for PETs have been developed. None has gained universal acceptance, reflecting differences in the underlying assumptions about the meaning of privacy<sup>11</sup>, the definition of PETs and the purpose of the classification (e.g., technical characteristics, legal aspects).

Typically, the classification systems follow a functional paradigm. The European Project on the Future of Identity in the Information Society (FIDIS) divides PETs into ‘opacity tools’ and ‘transparency tools’. The system is summarised by Fritsch (2007) as follows:

---

<sup>10</sup> See The Enterprise Privacy Group (2008).

<sup>11</sup> A narrow definition of privacy, e.g. privacy as concealment of information (Posner, 1980) is likely to lead to a different classification than the wider definition offered by Scoglio (1994), or Sweeney (2002), i.e. privacy as freedom to develop or ability to control one’s own space.

| Table 2: FIDIS (2007) PETs classification |                                                                                                                             |                                                                                                         |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
|                                           | Transparency tools                                                                                                          | Opacity tools                                                                                           |
| Definition                                | Tools that show clearly to a person what personal data is being processed, how it is processed and by whom it is processed. | Tools that hide a person's identity or her/his relationship to data as it is processed by someone else. |
| Non-technical example                     | Legal rights to be informed about data processing;<br><br>Privacy audits.                                                   | Pseudonymous access to online services;<br><br>Election secrecy.                                        |
| Technical example                         | Database audit interfaces;<br><br>Audit Agents;<br><br>Log files.                                                           | MixMaster anonymous e-mail;<br><br>TOR anonymising web surfing;<br><br>Pseudonyms.                      |

Note: additional information about individual PETs is given in Section 2.3 below.

Source: Fritsch (2007) based on FIDIS (2007)

A more detailed classification that uses a very similar approach is provided by The META Group (2005). The META Group classification uses a different terminology ('privacy protection' instead of opacity and 'privacy management' instead of transparency) and contains a more finely grained break-down of PETs, further classifying PETs in terms of aim (curative or informative) and function (unobservability, unlinkability and anonymity). A high-level overview of the META classification is shown in the table below.

**Table 3: META GROUP (2005) PETs classification**

|                           |                                  |
|---------------------------|----------------------------------|
| <b>Privacy protection</b> | Pseudonymiser Tools              |
|                           | Anonymiser Products and Services |
|                           | Encryption Tools                 |
|                           | Filters and Blockers             |
|                           | Track and evidence erasers       |
| <b>Privacy management</b> | Informational tools              |
|                           | Administrative Tools             |

*Source: Fritsch (2007) based on META Group (2005)*

The European Commission has not adopted a specific classification system for PETs. Rather, in its PETs Communication<sup>12</sup>, it provides a list of examples to illustrate its definition of PETs that includes technologies for the automatic anonymisation of data after a certain lapse of time, encryption tools, cookie-cutters and the Platform for Privacy Preferences (P3P). We used this list together with the more detailed META Group (2005) classification to establish the list of PETs used in our business survey (see the questionnaire in 0).

Jiang et al. (2002) provide a functional classification of PETs into preventive, avoiding and detecting technologies. This approach was also used by Acquisti (2002), whose study is an example of an exploratory analysis of differential economic effects of different types of PETs.

The ‘PET-Staircase’, proposed by Koorn et al. (2004)<sup>13</sup> and shown in the figure below, sorts PETs into four categories:

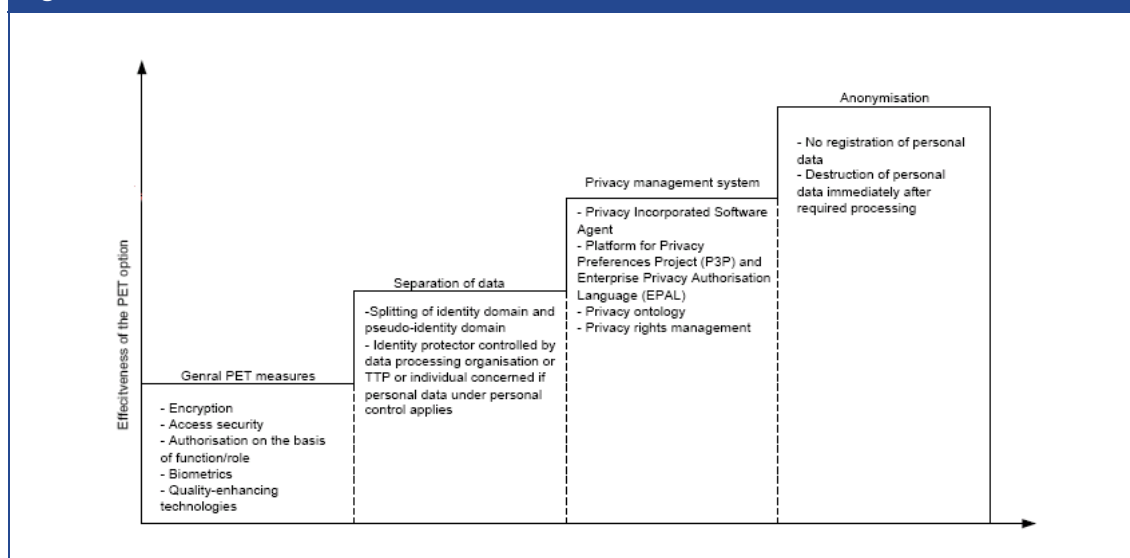
- 1) general PET controls;
- 2) separation of data;
- 3) privacy management systems;
- 4) anonymisation.

<sup>12</sup> COM(2007) 228 final, see above.

<sup>13</sup> See also Borking, J. (2009), “Why adopting of Privacy Enhancing Technologies (PETs) takes so much time”. Presentation at the EC DG Justice Workshop on the Economic Benefits of PETs, Brussels, 12 November 2009. Available at: <http://tinyurl.com/ybrtk4w>.

They are ranked according to their effectiveness (although effectiveness is likely to depend also on the specific application, and is moreover constantly changing with technological developments, with certain forms of de-identification (k-anonymity<sup>14</sup>) becoming obsolete). The 'staircase' is not intended as a model of technology adoption or the technological evolution of PETs. There is no automatic process by which data controllers who deploy general PET controls progress to using more effective PETs. Nor does the ranking effectiveness represent a judgement on the desirability of certain PETs. The suitability of the different PET options depends on the individual situation of the data controller.

**Figure 3: The 'PET-Staircase'**



Source: Koorn et al. (2004)

Clarke (2007) offers a classification based on functional characteristics with a view to legal/practical issues of privacy protection ('savage PETs', for example are likely to be illegal in certain applications).

14 In a k-anonymized dataset, each record is indistinguishable from at least k-1 other records with respect to certain "identifying" attributes. See Machanavajjhala et al. (2007).



**Table 4: Clarke's (2007) PETs classification**

| Category           | Examples                                                                    |
|--------------------|-----------------------------------------------------------------------------|
| Pseudo-PETs        | privacy seals, P3P                                                          |
| Counter-Technology | counter one specific privacy threat, e.g. SSL encryption or spyware removal |
| Savage PETs        | provide untraceable anonymity                                               |
| Gentle PETs        | pseudonymity tools balanced with accountability and identity management.    |

Source: Fritsch (2007) based on Clarke (2007)

Finally, an interesting classification has been suggested to us by Yoram Hacoen, Head of the Law, Information and Technology Authority of Israel (ILITA). It is compelling in its simplicity and puts the spotlight on the role PETs play in the way personal data is processed in real-world applications. According to this classification, PETs can be divided into technologies that are used **before** any personal data is used ('pre-usage') and technologies that safeguard privacy **while** personal data is being processed. The following table shows the approach:

**Table 5: PETs classification after Hacoen (2009)**

|                |                                        |
|----------------|----------------------------------------|
| Pre-usage PETs | data minimisation                      |
|                | Anonymisation                          |
|                | limitation of use                      |
|                | e-consent mechanism                    |
| Usage PETs     | data quality                           |
|                | verification                           |
|                | encryption                             |
|                | watermarking, tagging, sticky policies |
|                | usage logging                          |

Source: London Economics based on Hacoen (2009)

A priori, the usefulness of the different classifications (presented above) for the purpose of economic analysis is unclear. While functional elements are indispensable for classifying PETs, the available classifications do not allow a straightforward matching to the economic characteristics of certain technologies. Since the tentative approach by Acquisti (2002) no progress has been made towards achieving such a classification. The fact that the economic effects depend to a large

degree on the specific context in which PETs are applied, rather than any inherent characteristics, makes a comprehensive 'economic' classification elusive for the time being.

The following section will look in greater technical detail at the different types of available PETs. For the purpose of this section, no detailed classification is needed, but, as a starting point, we use the distinction between privacy management and privacy protection (analogous to the FIDIS classification).

## 2.3 Technical overview

This sub-section provides a short introduction to the different technologies that are subsumed under the PET label. It illustrates the fact that PETs are a mix of technologies at different stages of maturity. It should be noted that some of the technologies we mention are, at the time of writing, already seen by experts as obsolete in the face of advanced threats. Also, many PETs never make it past the concept stage.<sup>15</sup>

However, many PETs developed in academic research since 2002 are innovative. The low uptake at present may be explained by the S-curve pattern of the rate of new technology adoption observed by, among others, Griliches (1957), Mansfield (1968) and Rogers (1995), which suggests that there is a time delay between innovation and the adoption of technology by users.

Goldeberg (2007) lists a number of general properties of technologies that are required for PETs to be useful:

- **usability** (users have to be able to use a PET and want to use it given any difficulties/costs);
- **deployability** (everyday users must be able to obtain and benefit from a PET, requiring compatibility with preferred operating systems, web browsers, etc.);
- **effectiveness** (a PET has to work and provide the benefits it promises); and
- **robustness** (a useful system needs to maintain as much protection as possible).

Since our report is concerned with incentives for deployment by data controllers, usefulness is clearly a crucial consideration. The perceived lack of usefulness of some of the PETs that have been developed over recent years suggests that the research agenda on PETs and the needs of businesses and other data controllers sometimes diverge.

As outlined above, we divide PETs by function into privacy management and privacy protection tools. To illustrate the varying complexity of PETs, we use a further sub-division between stand-alone technologies and more complex 'PET systems', in which privacy considerations are embedded into entire processes and applications.

The section is not an enumeration of all available PETs, but rather an overview of some of the milestones in PET development. Our main source on PETs up to 2007 is Acquisti et al. (2007), the standard textbook on PETs. More recent developments were identified with the help of experts

---

<sup>15</sup> See Goldeberg (2007).

during and following the Workshop on the Economic Benefits of PETs<sup>16</sup> hosted by the European Commission's DG Justice, Freedom and Security on 12 November 2009.

### 2.3.1 PETs for privacy protection

In this sub-section we review some PETs for privacy *protection*. The section is split into two parts. The first part examines a number of stand-alone technologies for privacy protection, whilst the second part reviews broader concepts, processes and systems for privacy protection.

#### ***Stand-alone technologies for privacy protection***

In this sub-section we review seven individual technologies for privacy protection:

- 1) technologies for protection of the identities of senders/receivers of e-mail;
- 2) technologies for protection of identity when accessing interactive Internet services;
- 3) technologies for protection of the content of Internet conversations;
- 4) technologies for enabling private payments;
- 5) technologies for proof of authorisation without revealing private information (privacy credentials);
- 6) technologies for off-line information systems; and
- 7) privacy technologies for RFID systems.

#### **1. Systems to protect the identities of senders/receivers of e-mail**

A number of systems to protect the identities of senders/receivers of e-mail are described by Goldberg (2007):<sup>17</sup>

**Type-0 Remailers:** Type-0 remailers are the oldest and simplest systems for e-mail anonymity. The message goes from the sender to the *remailer*, who strips the identity of the sender and *re-mails* the message to the recipient. A pseudonym is assigned to the sender which is recorded.

**Type-I Remailers:** Type-I remailers are based on the same principle, but with a number of improvements, such as: 'chaining' (using a chain of multiple, independent remailers), encryption and 'mixing' (incoming messages to a remailer are batched together and randomly reordered before they are sent out).

**Type-II Remailers:** Type-II remailers (or *Mixmaster* remailers) address problems with type-I remailers, specifically their susceptibility to size *correlation attacks* and *reply attacks*.<sup>18</sup> In order to defeat size correlation attacks, Type-II remailers divide all messages into several fixed-sized

---

<sup>16</sup> For further details see: <http://tinyurl.com/ycwqyfr>.

<sup>17</sup> Goldberg in Acquisti et al. (2007), pp. 3-18.

<sup>18</sup> In size correlation attacks, attackers attempt to match the messages sent by a certain remailer to the messages that it receives by matching the sizes of the messages. In reply attacks, attackers make a copy of a message received by a remailer and send the same remailer multiple copies of this message. The attackers then observe which outgoing message from the remailer is repeated many times.

packages which are sent separately through the network of remailers. More complex techniques are used to resist reply attacks. Type-II remailers were state-of-the-art in 2002.

**Type-III Remailers:** By 2007, a design had been proposed for Type-III remailers (or *Mixminion* remailers). Improvements include a better system for handling replies to anonymous messages and, among other things, improved protection against reply attacks. However, at the time of writing, only a beta (test) version of the technology was available.

## 2. Systems to protect identity when accessing interactive Internet services

Techniques employed for e-mail security are not appropriate for interactive services because of the time delay they create. However, a number of technologies have been developed to enhance privacy for interactive services:<sup>19</sup>

**PipeNet:** In 1995, an anonymity system for low latency<sup>20</sup> traffic called PipeNet was presented by Wei Dai.<sup>21</sup> The system emphasised security above everything else and worked by shutting down the whole system if any anomaly was detected. However, this is clearly impractical and PipeNet is not used in practice.

**Anonymizer.com:** Anonymizer.com is one of only a few commercially successful anonymity technology providers. Anonymizer.com provides a simple, low cost system along the lines of the type-0 remailers.

**Onion Routing:** Onion Routing was developed by the US Naval Research Lab. It was the first PipeNet like system to be widely available. Its use was (primarily) for anonymising web traffic, and also to allow users to anonymously connect to any Transmission Control Protocol (TCP)/IP server on the Internet. Analogous to remailers, a path is created through several *Onion Routers* around the Internet. Unlike remailers, the path is 'long-lived': data is anonymously delivered and replies are returned along the path. After the communication is complete the path is torn down. The original Onion Routing network was a *proof-of-concept*, and it later evolved into the Tor network (below).

**The Freedom Network:** The Freedom Network was a commercial venture based on the PipeNet system and incorporating some ideas from the Onion Routing project. The Freedom Network allows users to set up a persistent pseudonym to use when communicating online, meaning they can maintain separate online personas (this feature is referred to as a *pseudonymity service* - Onion Routing did not provide this service). However, the costs of maintaining the system were prohibitive as operators were needed all over the world to run *Anonymous Internet Proxies* (AIP nodes). The number of paying users did not support the network, which had to be shut down.

**Java Anon Proxy:** Java Anon Proxy (JAP) is a technical project of the University of Dresden. It is one of the few PETs that existed in 2002 and was still in use in 2007. JAP is web-only (unlike PipeNet)

---

<sup>19</sup> See Goldberg (2007) for more details.

<sup>20</sup> Latency is a measure of time delay experienced in a system.

<sup>21</sup> See <http://weidai.com/pipenet.txt>.

and uses the techniques of type II remailers (web requests and replies are divided into fixed-sized chunks and sent through a series of mix nodes, each of which collects a batch of these chunks and encrypts/decrypts them as appropriate, reorders them, and sends them to the next mix node).

**Tor:** Tor is the next generation of the Onion Routing project and, according to the Goldberg (2007), is the most successful interactive anonymity tool: hundreds of thousands of users send about 8 terabytes of data per day through hundreds of Tor nodes. It shares some of the characteristics of the Onion Routing project: anonymisation of TCP/IP protocols, requires users' Internet applications to be configured, etc. Unlike the Freedom network, all the nodes are run by volunteers and the software is free and open-source. However, one of its most notable drawbacks is that it reduces the speed of web browsers. In addition to protecting users, Tor also protects the privacy of providers of TCP/IP-based services: somewhere in the world, a user runs a web server which can only be accessed through Tor, and Tor protects the identities of the user and the provider of the service.

### 3. Technologies that protect the content of Internet conversations

Participants in Internet communication using e-mail or instant messaging may wish to keep the content of their conversations (which might entail sensitive personal data) private, rather than their own identity. Technologies which target this issue are described by Goldberg (2007):

**PGP and Compatible Systems:** Pretty Good Privacy's (PGP) fundamental purpose is to encrypt or digitally sign e-mail. Users install PGP-compatible software and use it to encrypt e-mail before sending it. Some e-mail programs have incorporated PGP support. PGP has been available in some form for more than 25 years.

**SSL and TLS:** Secure Sockets Layer (SSL),<sup>22</sup> renamed Transport Layer Security (TLS) in later versions, is a protocol developed by Netscape (the US computer services company) to transmit private documents via the Internet using a cryptographic system. According to Goldberg (2007), SSL protocol and TLS, were the most widely used PETs in 2007. Every major web browser comes with in-built support for these technologies and their use is largely invisible to the user, so no special installation or configuration needs to be done by the user.

**Off-the-Record Messaging:** Off-the-Record (OTR) messaging (first released in 2004) protects the content of instant messaging communication. Senders are assured that only the recipient will be able to read it and the recipient will be assured that the message came from the sender and has not been modified en route. Parties to conversations can provide no *proof* of what is said, so third parties must accept the content on trust. OTR encryption must be handled automatically in some way. The most preferable method is for OTR to be built into the user's instant messaging client, as this means that (like SSL/TLS) the user does not have to install or configure anything special.

### 4. Technologies for enabling private payments

According to Goldberg (2007), there were still no serious electronic cash services by 2007 and this is identified as an important gap in the set of available PETs. Chaum (1983) proved the viability of

---

<sup>22</sup> <http://www.webopedia.com/TERM/S/SSL.html>

electronic cash, but to our knowledge so far there has been no uptake by the market. Consequently, there exist many centralised records of everything purchased online and databases of payment records including credit card numbers which may be stolen by fraudsters and identity thieves.

Making a system widely accepted and interoperable with real money is difficult. Goldberg (2007) mentions that PayPal may be in the best position to provide privacy-friendly payments online as it already has the infrastructure and a large user base and could easily set up an interface between electronic cash and the rest of the financial system.

## 5. Technologies for proof of authorisation without revealing private information (privacy credentials)

Privacy credentials allow users to prove they are authorised to access certain information/use certain services etc. without revealing personal data such as their full identities. Hence, storage of personal information is prevented. In contrast to PETs that withhold identity and provide untraceable anonymity (sometimes called ‘savage PETs’, see Clarke, 2007), credential systems rely on a trusted body that acts as the repository of the true identity. Service providers can access only information that is directly relevant to them, i.e. whether an individual is entitled to receive a certain service. For example, minors might be barred from buying certain services online. The service provider can then use the credential system to verify only that the person requesting the service is not under age, without acquiring any further personal data.

Trust in the credential system is essential for this setup to work. Unsurprisingly, this means that governments are taking on the role of central identity controller. An example is the eID function of the planned new national identity cards<sup>23</sup> in Germany. In the proposed systems, service providers who want to use the official credential system will have to apply to a government agency, which then issues a certificate that specifies which personal data (i.e., which subset of the data stored on the electronic ID card, which includes name, address, age, etc.) the provider will be able to access.

A private-sector credential scheme called Open Identity Exchange (OIX) has recently been announced by PayPal, Google and Equifax, VeriSign, Verizon, CA and Booz Allen Hamilton. The non-profit initiative is being supported by the US government and allows the participating organisations to issue digital identity credentials that will be accepted for privacy-protected registration and login at US government websites, such as the National Institute of Health (NIH). It is envisaged that users will eventually be able to access not only various government services but also private e-commerce services with their OIX credentials.<sup>24</sup>

Another example of a credential product at an advanced development stage is the U-Prove technology, which was acquired by Microsoft in March 2008.<sup>25</sup>

## 6. Technologies for off-line information systems

PETs are not confined to the online environment only. They have also been developed for off-line information systems. For example, Van Blarckom (1998) developed a hospital information system which separates individuals’ identification data from their other personal data (such as diagnostic and treatment details) by creating two separate domains for these different types of information in the database.

Patient numbers from the ‘identity domain’ are encrypted and these encrypted numbers are used as the patient numbers in the second domain where other personal information is kept. The encrypted patient numbers can be decrypted using the ‘identity protector’ so that the link can be

---

<sup>23</sup> See <http://tinyurl.com/yfb8m6u> (in German).

<sup>24</sup> See <http://tinyurl.com/yb9qxpl>.

<sup>25</sup> <http://www.credentica.com/>

made with the identity domain. In this way, only authorised individuals can make the connection between the two domains.

## 7. Privacy technologies for RFID systems

Radio-frequency identification (RFID) is a widely used technology for identification and tracking of products, animals or people using radio waves. RFID technology is implemented through the use of *tags* which are attached to products. The tags emit radio waves from which they can be uniquely identified. RFID has the potential to revolutionise industry through applications such as supply chain management, animal identification and transport logistics. However, certain features of the technology lead to a range of potential privacy threats:

- *Product information leakage:* Without a security mechanism, unauthorised readers can obtain a tag's unique electronic code. The reader can find out the product type and manufacture. Essentially, the technology can give 'x-ray vision' of the items carried by individuals, information which, for example, may be exploited by thieves.
- *Association between tags and owners:* Tags allow the identification of products, but the unique IDs can be associated with the owners (for example at checkouts). This information may be exploited by organisations or governments causing privacy threats. Further, individuals may not be aware of the presence of a tag on their possessions or their association with it.
- *Tracking of individuals:* There is a possibility that individuals can be tracked based on their possessions. An individual's movements and location may be monitored. In addition, there is a risk that individuals may be 'profiled' by linking information on their possessions with other personal information.
- *Privacy threats to companies:* Companies' privacy may be compromised as a result of the application of RFID, for example when tags are used in supply chains.

Privacy issues arising from the use of RFID are addressed via a number of technological solutions:

**Out-of-tag privacy mechanisms:** Out-of-tag privacy mechanisms prevent ID disclosure without modifying the tags' other specifications (read rate, storage capacity, etc.). There are two approaches in this category:

- *Faraday cage:* This approach blocks output from a tag so preventing communication with readers. This is done by shielding the tag against unauthorised reading with some form of conducting material, such as water or metal. The effectiveness of the approach depends on the transmission frequency of the tag. In some countries (for example the USA), ePassports use this shielding method by embedding fibres in the covers of passports so that they cannot be detected until they are physically opened.
- *Active jamming:* This approach works by broadcasting a signal which prevents unauthorised readers from identifying or accessing RFID tags. An example is the *blocker tag*, where a tag identifies itself as all possible tags, so preventing unauthorised readers from knowing its true identity.



**Tags with cryptographic circuits:** In some cases, tags are equipped with cryptographic circuits which (for example) encrypt the IDs of the tags. The drawback is that this attribute of a tag comes at the expense of some other specification, such as size/weight, cost, storage capacity, etc.

### ***Concepts, processes and systems for privacy protection***

In this sub-section, we review two concepts, processes and systems for privacy protection:

1. cryptographic obfuscation; and
2. random data perturbation.

#### **1. Cryptographic obfuscation**

In many cases, maintaining the privacy of individual records is not the objective of the PET. Instead, the aim is to control *how* individual records are accessed. In a typical application of *cryptographic obfuscation* for access control and data privacy, a database owner wishes to distribute a database to potential users, but wants to obfuscate the database so that only queries that are permitted by the owner's privacy policy are allowed. This can be achieved through cryptographic obfuscation, which restricts *how* records are accessed ensuring that only certain queries can be evaluated.

Narayanan and Shmatikov (2007) describe three general situations where access control is the objective (rather than the confidentiality of individual records):

- users should not be able to execute queries which return all the information in the database;
- some records should not be accessible unless users enter a password; and
- users should have to describe precisely what they are looking for before access is granted.

Three practical examples are:

- *Credit bureaus:* Employees of credit bureaus must have access to individuals' records to make necessary updates, but the bureau must not be able to compile a list of consumers' information to sell to third parties.
- *Online directories:* If someone knows the name of an individual they can look up their contact details, but at the same time spammers cannot indiscriminately harvest information in the directory.
- *Outsourcing of technical support:* If a company outsources its technical support, the support staff need to have access to individual records in the database.

In each scenario, the database must have a built-in access control mechanism, which enforces the database owner's privacy policy. Narayanan and Shmatikov (2007) note that it is very challenging to enforce such access control policies. They envisage a solution based on cryptographic

obfuscation,<sup>26</sup> which transforms a database so that queries which are not explicitly permitted by the owner's access control policy are *computationally infeasible*.

In their approach, the owner of the database defines a set of queries which are permitted for the user. The database is then obfuscated so that only this set of queries can be evaluated on the database, and evaluating any query outside the set is computationally infeasible.

The goal is to limit users to a certain set of queries, and it is up to the database owner to decide what these queries should be. Cryptographic obfuscation provides database owners with a mechanism for enforcing their desired policy.

Using this approach, the access control policy becomes an inseparable part of the database which can then be publically released, while the owner can be sure that users are accessing it only via queries which comply with the access policy.

The drawback to this approach is that only certain types of queries can be obfuscated in this way, so not every access control policy can be imposed using the approach.<sup>27</sup> Further, for some types of queries obfuscation has significant performance and storage costs.

However, in many situations cryptographic obfuscation is an efficient and *provably secure* way to ensure data access control. The approach works, for example, in securing directories against address harvesting: an obfuscated directory can have the property that it is easy to look up a name and company or name/address pair, but queries such as "retrieve all names in the directory" are not computationally feasible.<sup>28</sup>

## 2. Random data perturbation

The random data perturbation technique has been widely used for preserving the privacy of individual records when statistical databases are disclosed. The technique adds random noise to confidential numerical records, meaning that true values are not revealed when databases are shared or publically released, whilst the statistical properties of databases are preserved. The owner of a database provides values  $u_i + v$ , where  $u_i$  is the original data and  $v$  is a random value drawn from a certain distribution.

Narayanan and Shmatikov (2007) note that this is the conventional solution to the so called *census problem*: how to sanitise a database such that the privacy of individuals in the database is respected, whilst at the same time the database still allows statistical estimation of the characteristics of the population. According to Su et al. (2007), the technique has also recently been applied to preserving privacy in data mining.<sup>29</sup>

---

<sup>26</sup> According to Narayanan and Shmatikov, Lynn et al. (2004) made one of the first observations that cryptographic obfuscation may be used for access control.

<sup>27</sup> See Narayanan and Shmatikov for more detail on the mechanics of obfuscation for access control.

<sup>28</sup> Narayanan and Shmatikov go on to extend the discussion of obfuscation to more complex group privacy policies.

<sup>29</sup> As explained by Su et al., data mining is an analytic process for exploring data in search of patterns or systematic relationships between variables, and then examining new sets of data in an attempt to validate the findings.

### 2.3.2 PETs for privacy management

In this sub-section we review some PETs for privacy *management*. Like the last sub-section, this sub-section has two parts: the first examines standalone technologies for privacy management, whereas the second reviews some broader concepts, processes and systems for privacy management.

#### ***Stand-alone technologies for privacy management***

In this sub-section we review two stand-alone technologies for privacy management:

1. technologies for preventing phishing attacks; and
2. technology for transparency of prior transactions (PRIME Data Track).

##### **1. Technologies for preventing phishing attacks**

Anti-Phishing tools aim to prevent *phishing attacks*, where users are directed to malicious websites which often appear to be a common site (such as a bank or eBay), but which are in fact run by the attacker. Users are usually invited to visit the site to address some issue (with their account for example). When they do so, the attacker captures their login name and password. There are a number of tools available to alert users that websites are in fact phishing sites. Often these appear as a tool bar in the web browser which turns a certain colour if the site is *probably* a phishing site. Different tools use different methods to determine whether sites are genuine.

##### **2. Technology for transparency of prior transactions (PRIME Data Track)**

In order to allow individuals to properly manage their digital privacy it is important to enable them to know what information is known about them and by whom. This need is addressed by “Data Track”, one of the main components of the EU-funded project PRIME. Data Track is a history function of all online transactions, storing for the user information on which personal data has been disclosed to whom. Thus, Data Track provides transparency to users of their online transactions and also enables them to later question data controllers over whether they really treated their personal information as promised. The technology is not yet in use.

#### ***Concepts, processes and systems for privacy management***

In this sub-section we describe four concepts, processes and systems for privacy management:

1. Enterprise privacy policies
2. Languages for writing enterprise privacy policies
3. Privacy metrics
4. HCI technology for privacy-enhancing identity management

### 1. Enterprise privacy policies

Enterprise privacy policies define the purposes, conditions and obligations under which personal information is collected and can be accessed. They formalise the privacy rules of enterprises. According to Backes and Dürmuth (2007), enterprise privacy policies:

- define who can access collected data;
- define the purposes for which collected data can be accessed;
- define the way in which collected data can be accessed; and
- impose obligations on organisations using the data.

Examples of the obligations on organisations using the data include obligations to send notice to data subjects when their information is accessed, or obligations to delete data within a certain time limit. Privacy policies may also set out rules on the collection of personal data (although this is not mentioned by Backes and Dürmuth).<sup>30</sup>

In some cases, enterprise privacy policies are *verified* to, for example, confirm that they fulfil regulatory requirements or adhere to self-regulatory standards. This can be done internally or by external auditors such as TRUSTe or Sentillion.<sup>31</sup> In some cases, multiple policies are combined with the intention of collectively refining them. For example, some enterprises take all applicable regulations and combine them into one minimum policy.

The development of “*sticky policies*” is another component of the EU funded project PRIME. Once an online transaction has been completed by a user these policies ‘stick’ to the data which has been disclosed. Hence, sticky policies enforce the rules on how data may be processed even after the data has been disclosed and left the user’s area.

### 2. Languages for writing enterprise privacy policies

IBM’s EPAL is a formal language for writing enterprise privacy policies to govern data handling practices in IT systems according to fine-grained positive and negative authorization rights. An ‘EPAL policy’ defines:

- Hierarchies of:
  - data-categories - categories of data that are handled differently from a privacy perspective;
  - user-categories - entities (users/groups) that use collected data; and
  - purposes - intended uses of the data.

---

<sup>30</sup> Early examples of this concept, which has now become widespread, are described by Fischer-Hübner (2002), Karjoth et al. (2002) and Karjoth and Schunter (2002).

<sup>31</sup> Online respectively at: [www.truste.com](http://www.truste.com) and [www.sentillion.com](http://www.sentillion.com).

- Sets of:
  - actions - how the data is used (e.g. disclose vs. read);
  - obligations - actions that must be taken (e.g. delete after 30 days or get consent); and
  - conditions - Boolean expressions to evaluate the context (e.g. “the user-category must be an adult” or “the user-category must be the primary care physician of the data-subject”).

Using these components, privacy rules are formulated allowing or denying actions by user-categories on data-categories, for certain purposes and under certain conditions, while fulfilling obligations.

To accommodate general rules and exceptions, EPAL rules are sorted by descending precedence (e.g. a rule about an employee can be inserted before a rule about a department in order to implement an exception).<sup>32</sup>

Refinement of an EPAL policy (meaning adding more details to it) may be done in reaction to changes to regulations or as a result of entering new sectors or markets.

For the purposes of standardisation across enterprises, IBM has proposed EPAL as an *XML specification*, which has been submitted to the World Wide Web Consortium for Standardisation.

### 3. Privacy metrics

*Privacy metrics* measure privacy disclosure in some quantitative way, and are necessary in situations where absolute privacy is not a practical solution. As explained by Wang and Jajodia (2007), privacy metrics have two aspects:

- *Uncertainty* of the values of personal data (i.e. published data lacks certainty as to the actual value of some piece of information for an individual).
- *Indistinguishability* of one individual from the rest (i.e. from the published data the value of some piece of information for an individual cannot be distinguished as *higher* (or lower) than the value for the rest).

For example, the level of an individual’s salary may be revealed as between two values, and this would provide *uncertainty*. However, if it is also revealed that all other salaries are definitely less (i.e. in totally different ranges), then the individual’s privacy may still be violated, as *indistinguishability* is not provided.

From this example, we see that uncertainty does not imply indistinguishability. Likewise, indistinguishability does not ensure uncertainty (saying that a group have a given salary provides indistinguishability, but no uncertainty).<sup>33</sup>

---

<sup>32</sup> For more details on EPAL, see the EPAL technical specification (<http://tinyurl.com/ycavz9q>), or Acquisti et al. (2007).

#### 4. HCI technology for privacy-enhancing identity management

An important issue in privacy management is ensuring that individuals retain control of their personal information. Tools for enforcing user control are provided by privacy-enhancing identity systems, such as human-computer interaction (HCI) technologies. Examples of such HCI technologies are those being researched in the EU FP6 project 'PRIME'.

Fischer-Hübner et al. (2007) present a number of alternative user interface (UI) 'paradigms' for identity management that have been designed and tested as part of the PRIME HCI research:

- Role-centred paradigm
- Relationship-centred paradigm
- TownMap-based paradigm

In the *role-centred paradigm*, users' control over the disclosure of data is mainly undertaken through "roles" described above the function. Within a role, users set different disclosure preferences for different types of data. Users must then choose the role they will be acting under when they contact service providers.

In the *relationship-centred paradigm*, different privacy preferences are defined for different communication partners. Identity management controls are integrated as for the role-centred paradigm, but in addition the ordinary bookmarks have roles attached to them. By default, a predefined role based on transactional pseudonyms (that is, a new pseudonym is created for each transaction) called "Anonymous" is activated.

In the *TownMap-based paradigm*, roles are replaced by 'areas' with default privacy settings, namely the Neighbourhood, the Public area and the Work area.

##### 2.3.3 Summary of PETs reviewed in this section

Table 6 overleaf summarises the PETs reviewed in this section. As in the sub-sections above, the PETs are divided into PETs for privacy protection and PETs for privacy management, and within these two categories stand-alone technologies are separated from concepts, processes and systems.

---

<sup>33</sup> In a formally defined setting (which is not reproduced here), Wang and Jajodia (2007) outline basic ideas to check whether a set of query results satisfy uncertainty and indistinguishability metrics.

---

**Table 6: Summary of PETs reviewed**

| <b>PETs for privacy protection</b>                                                                  |                                                                                                                |
|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Stand-alone technologies</b>                                                                     | <b>Examples</b>                                                                                                |
| Technologies for protecting of the identities of senders/receivers of e-mail                        | Remailers, types 0-III.                                                                                        |
| Technologies for protecting of identity when accessing interactive Internet services                | PipeNet,<br>Anonymizer.com,<br>Onion Routing,<br>The Freedom Network,<br>Java Anon Proxy,<br>Tor.              |
| Technologies for protecting of the content of Internet conversations                                | PGP and Compatible Systems,<br>SSL and TLS,<br>Off-the-Record Messaging.                                       |
| Technologies for enabling private payments                                                          | None (according to Goldberg, referring to electronic cash).                                                    |
| Technologies for proof of authorisation without revealing private information (privacy credentials) | eID, OIX, U-prove                                                                                              |
| Technologies for offline information systems                                                        | Van Blarckom's hospital information system                                                                     |
| Privacy technologies for RFID systems                                                               | Out-of-tag mechanisms,<br>Tags with cryptographic circuits.                                                    |
| <b>Concepts, processes and systems</b>                                                              | <b>Examples</b>                                                                                                |
| Cryptographic obfuscation                                                                           | n.a. <sup>1</sup>                                                                                              |
| Random data perturbation                                                                            | Privacy Integrated Queries (PINQ) <sup>2</sup>                                                                 |
| Privacy friendly pay-as-you-drive insurance                                                         | PriPAYD                                                                                                        |
| <b>PETs for privacy management</b>                                                                  |                                                                                                                |
| <b>Standalone technologies</b>                                                                      | <b>Examples</b>                                                                                                |
| Technologies for preventing phishing attacks                                                        | eBay's Account Guard,<br>Google's Safe Browsing toolbar,<br>Cloudmark Anti-Fraud Toolbar,<br>Numerous others.  |
| Technology for transparency of prior transactions                                                   | PRIME Data Track                                                                                               |
| <b>Concepts, processes and systems</b>                                                              | <b>Examples</b>                                                                                                |
| Privacy metrics                                                                                     | Uncertainty measures,<br>Indistinguishability measures.                                                        |
| Languages for writing enterprise privacy policies                                                   | EPAL                                                                                                           |
| Enterprise privacy policies                                                                         | EPAL policies                                                                                                  |
| HCI technology for privacy-enhancing identity management                                            | PRIME HCI technologies,<br>Role-centred paradigm,<br>Relationship-centred paradigm,<br>TownMap-based paradigm. |

Note: 1. See Narayanan and Shmatikov (2007) for more in-depth discussion of these techniques, and Su et al. (2007) for more discussion on the use of these techniques specifically for privacy in data mining and document clustering. 2. <http://tinyurl.com/2687wod>. See Su et al. (2007) for more in-depth discussion of techniques of this kind.

**Source:** *London Economics*

## 2.4 Summary

This section showed that PETs is a complex concept that comprises a broad range of individual technologies. Data security technologies are PETs if they are used to enhance privacy, but it should be noted that they can be used in inherently privacy-invasive application, in which case they cannot properly be counted as PETs. It is also important to stress that PETs are not limited to pieces of software or hardware, but comprise procedures and management systems as well. Data minimisation and consent mechanism are an important part of PETs, and PETs often combine these elements with data protection tools into an integrated privacy system.

The section also highlighted that PETs are constantly evolving. New technologies, originating in publicly funded research programmes such as PRIME, in universities and in private sector R&D continue to come to the market. This evolution means that technologies exist at different stages of maturity, from designs and concepts to mature technologies in widespread use and older technologies that are being rendered obsolete by changes in the threat environment.

A variety of different classifications of PETs has been proposed. Mostly, these are based on technological characteristics. A classification according to economic characteristics remains elusive and may be impossible because of the context-specific nature of the economic effect of PETs. User-centric classifications, such as the ones proposed by FIDIS (2007) and Hacoen (2009), are the most useful classifications in the context of this study. Still, the complexity of the PETs concept, the diversity of the technologies and the difficulty in making a clear distinction between PETs and 'mere' data protection tools suggest in interactions with data controllers and other stakeholders, the use of more specific terminology ('data protection tools', 'data minimisation tools', 'consent mechanisms', etc.) may be advisable.



## 3 PETs deployment: context and issues

This chapter takes a detailed look at the factors that determine whether data controllers deploy PETs. It is based on economic theory as well as empirical evidence. Separate sub-sections describe the determining factors from a range of angles. The section is structured as follows:

- Sub-section 3.1 introduces the question of PETs deployment and describes the analytical approach.
- Sub-section 3.2 considers the role of individuals in shaping data controllers' PETs deployment decision.
- Sub-section 3.3 looks at the issues from the perspective of data controllers, considering incentives and disincentives for deployment as well as factors that might hold back deployment levels even if it is economically beneficial.
- Sub-section 3.4 discusses the role of PETs in competition.
- Sub-section 3.5 introduces a general model of technology adoption that suggests PETs deployment rates may change naturally over time.

### 3.1 Outline of the economic approach

The protection of personal data is an important policy objective for the European Union. Article 8 of the Charter of Fundamental Rights of the European Union enshrines the right to the protection of personal data. The Charter further specifies that:

- “personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law” and that
- “everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified”.

These fundamental rights form the basis of the legal framework in which PETs are deployed. The Data Protection Directive of 1995<sup>34</sup> provides for the implementation of these rights with respect to the processing of personal data in the European Union. The Directive requires Member States to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, in order to ensure the free flow of personal data in the Community. The Directive outlines the core principles for the protection of personal data:

- transparency;
- proportionality; and
- data minimisation.

---

<sup>34</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

This means that informed consent is required for any use of personal data and that only data that is strictly necessary for carrying out a certain function may be collected and processed. Moreover, individuals must be informed about any processing of their personal data and the purpose of such processing at the time of collection and be able to verify the accuracy of any personal data being held. Even voluntary disclosure of personal information on the part of individuals does not absolve data controllers from the obligation to collect and use the information only in accordance with the existing privacy and data protection legislation.

With respect to the processing of personal data by institutions of the European Union (or by Member States when carrying out activities which fall within the scope of Union law), the Treaty on the Functioning of the European Union (TFEU) gave responsibility for implementing the protection of personal data to the European Parliament and the Council, which resulted in the passing of Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.<sup>35</sup>

The legislation underpinning the protection of personal data in the European Union is currently undergoing a review in which a more explicit role for “privacy by design” and PETs more broadly is being considered. This is in consequence of the fact that PETs have a potentially crucial role to play in ensuring that users of information technology conform to the standard of protection of personal data envisaged in the EU legislation.

In particular, deploying the appropriate PETs allows data controllers to use personal data in situations where they could not have done so without PETs. For example, this applies in cases where individuals (or organisations) would not disclose personal data if they data controller did not deploy appropriate PETs.<sup>36</sup> Some PETs minimise or eliminate the need for personal data altogether, so that businesses can provide a service that would normally require personal data without the PETs.<sup>37</sup>

Thus, there is a category of cases where data controllers *must* use PETs if they want to carry out activities that involve personal data. Not deploying PETs means not offering the service. Thus, the economic calculus for data controllers becomes a matter of subtracting the cost of PETs (both direct and indirect) from the benefit they derive from the activities in question.

Alternatively, there is a second category of cases in which a service can be provided with PETs or without PETs. For example, data controllers may have a choice about the data-intensity of the service they offer: either, the service is offered in a way that involves the use of personal data, in

---

<sup>35</sup> In the specific field of police and judicial cooperation in criminal matters, the protection of personal data is further regulated by the Council Framework Decision 2008/977/JHA of 27 November 2008.

<sup>36</sup> A salient example is a business-to-business transactions in which personal data constitutes a business secret for one of the parties, e.g., a company that outsources certain processing tasks involving its customer database to another company.

<sup>37</sup> An example of such a PET is presented in Section 5.3.

which case PETs are required, or, there is an alternative way of providing the same service without using personal data.<sup>38</sup>

A lack of strict enforcement or a generous interpretation of existing data protection rules might also give rise to a situation in which businesses can choose between deploying and not deploying PETs (or between different PETs offering different levels of privacy protection). Note that this requires that individuals are prepared to disclose personal data to data controllers that do not deploy PETs.

In the cases in the second category, the deployment decision involves a more complex trade-off that involves the cost of PETs, their effectiveness, the level of risk to privacy, the demand response to PETs, etc. This is the situation our study is mainly concerned with.

In both categories of cases it should be noted that the need for/attractiveness of PETs – whether compulsory or chosen voluntarily – change over time with the evolution of threats to privacy and technologies to mitigate them. For example, recent years have seen the emergence of algorithms that are able to extract personal information from datasets that would have been considered securely anonymised only a few years ago.<sup>39</sup>

At the same time, innovations in PETs allow businesses and governments to offer services that used to rely extensively of the processing of personal data in ways that are less privacy-invasive without losing substantial functionality.<sup>40</sup> An implication of the latter point is that a new PET could alter what is a ‘proportional’ use of personal data in a certain application: if the PET makes it possible to provide a service with more privacy, then arguably all providers of the same service without the PET are suddenly using personal data excessively.

From an economic perspective, assessing the value of PETs for businesses and consumers – which is what drives deployment – requires an assessment of the associated costs and benefits. In this section we use simple economic principles to characterise the factors that determine the deployment decision. We look at the issue from the perspective of both consumers and businesses, in recognition that their interests can, in certain circumstances, conflict.

The discussion here will be kept general. Many PETs are technologies that make carrying out activities that rely in some form on the processing of personal data more costly or prevent it altogether. Only a subset of PETs can claim to be ‘positive-sum’ in the sense that they allow the delivery of services as well as or better than would be the case without them. Such PETs often follow the ‘privacy by design’ paradigm, where privacy considerations are integrated from the start with the business model as well the systems and processes of the organisation. The implication is that the cost-benefit calculation is likely to depend strongly on the specific PET in question. Where certain security technologies are used merely as add-ons to make existing applications more

<sup>38</sup> An example is the choice between Customer Relationship Management (CRM) and Vendor Relationship Management (VRM), which fulfil the same function, but where only the former approach requires detailed personal data. A company may thus either opt for CRM and install the appropriate PETs, or choose VRM and have no need for PETs at all. Our understanding is that both models are legal under current European privacy rules.

<sup>39</sup> A prominent example is the de-anonymisation of the Netflix Prize database described in Shmatikov and Narayanan (2008).

<sup>40</sup> An example is the concept described by Troncoso et al. (2007) of a PET that reduces the data requirement of pay-as-you-drive insurance. (See Section 5.3.)

secure, the costs of implementation and the potential for loss of functionality are likely to be higher, and benefits more limited, than if integrated PETs are designed for a specific application. It has to be stressed that the former (non-integrated) type of PET is currently much more widely used than the latter.

The principles of economic assessment remain the same for all types of PETs, but the way in which different factors (demand response to PETs, effectiveness/ efficiency, behavioural biases, network effects etc.) interact will depend on the specific technologies and the context in which they are used. Such differences between specific types of PETs are thus primarily an empirical matter.

The costs and benefits of PETs are inextricably tied up with the costs and benefits of making personal information available in an electronic format. PETs can, in various ways, increase or decrease those costs and benefits. For example, a PET that hinders the exploitation of personal data for an economically beneficial purpose reduces or even eliminates an economic benefit. A different PET might enable an economic benefit by facilitating the limited use of personal information where this information would not have been available at all had it not been for the PET – either because it would not be lawful to collect it or because individuals would not supply it.

Equally, on the cost side, PETs can lower the cost of online activities for individuals (and businesses) by reducing the risk of data loss, while at the same time increasing the cost for data controllers that have to invest in PETs. In this section, we identify the main mechanisms that determine these costs and benefits, i.e. the drivers of PETs, both from individuals' and from data controllers' point of view. In particular, we consider:

- individuals' demand for PETs and its determinants, including the risk of privacy breaches, individuals' risk perceptions and actual behaviour, and awareness of PETs;
- factors influencing the deployment decision, including the value of personal data for data controllers, the role of PETs in competition, and barriers to effective deployment; and
- theories of technology adoption that might apply to PETs.

This section will provide a structure for understanding the microeconomic incentives that govern PET adoption by businesses and consumers. An overall evaluation of the importance of these factors is a matter for empirical research that goes beyond the scope of this project, although we provide a detailed analysis of specific PETs in Section 5.

## **3.2 Individuals' demand for PETs**

We first look at the demand for PETs from the perspective of individuals. This is determined primarily by the risk involved in the disclosure of personal data, as well as by the awareness of PETs and views about their efficacy.

### **3.2.1 Risk of data loss**

The disclosure of personal data carries certain risks. We concentrate here on the likelihood of incurring tangible economic losses; however, it should be noted that less tangible factors, such as the unease engendered by the loss of control over personal information that, once disclosed, might be used in unforeseen ways are potentially also important drivers of the demand for PETs by individuals.

The economic loss most commonly associated with the misuse of personal information is the financial loss resulting from identity fraud, e.g., in the form of credit card fraud or theft from online bank accounts. In addition, economic loss can take more subtle forms, for example, where an individual's job application is turned down due to the disclosure of unfavourable personal information to a potential employer.<sup>41</sup> The issue of who is liable for such losses (the individual or the data controller) will to a large extent determine where the demand for PETs originates. We assume that, at the moment, consumers bear a significant part of the losses due to privacy breaches. Even where legal liability rests with data controllers, which is often the case, individuals typically still incur significant costs, either directly or through inconvenience, difficult restitution processes, etc.

If consumers have perfect information about the possible losses associated with disclosure of personal information (including the intangible costs of privacy invasion) and the likelihood of such losses when engaging in online activities, we expect them to take all this information into account and demand the amount of the services in question that is optimal under the circumstances.

In this situation, PETs that lower risk reduce the cost for consumers and will thus, all else equal, lead to an increase in demand for online transactions. This is one of the mechanisms invoked by data protection authorities as a justification for calling for increased PET deployment. Weak demand for PETs can then be explained in two ways:

- either individuals currently feel adequately secure; or
- individuals do not understand the risks that sharing personal data exposes them to.<sup>42</sup>

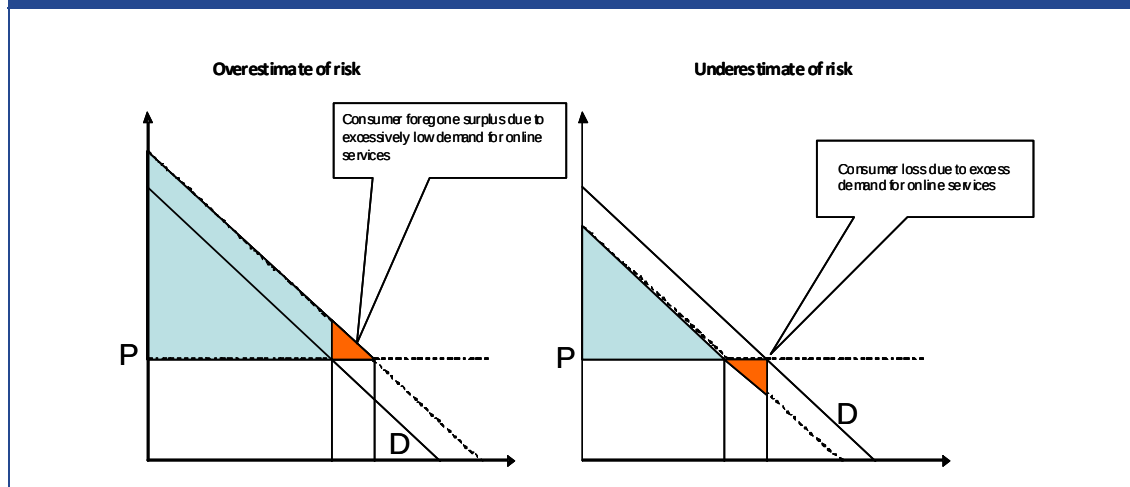
The question is whether consumers misjudge the level of risk. Risks can be perceived either as lower, or higher, than they really are. In each case, there are consequences for the demand for services that require the disclosure of personal data and the demand for PETs. If consumers overestimate the risk, they will demand fewer online services than would be optimal, while at the same time demanding too much privacy protection. If the true risk is higher than consumers think, it's the reverse: the demand for online services is too high and the demand for PETs is too low.

Figure 4 shows the consequences of false risk expectations on the part of consumers. The panel on the left of Figure 4 shows the consequences of overestimating the risk associated with online transactions: consumer surplus under the correct demand conditions, i.e., the demand that would prevail if consumers' risk assessment were accurate, is the large shaded region on the left. A lower level of demand (the inner demand curve) leads to a loss in surplus equivalent to the triangle at the right edge of the surplus area. Conversely, the right-hand panel shows the consequences of underestimating the risk: here, consumers' demand is too high given the price (which implicitly includes losses due to data theft), so that the triangle below the price curve represents the loss to consumers. The deployment of PETs can help to move the demand to a level where the allocation is efficient.

<sup>41</sup> From an economic point of view it is possible, however, to see such involuntary disclosure as welfare-enhancing, to the extent that it reveals genuinely information that is relevant for the hiring decision.

<sup>42</sup> See Acquisti (2004).

Figure 4: The consequences of misjudging the risk of misuse



Source: London Economics

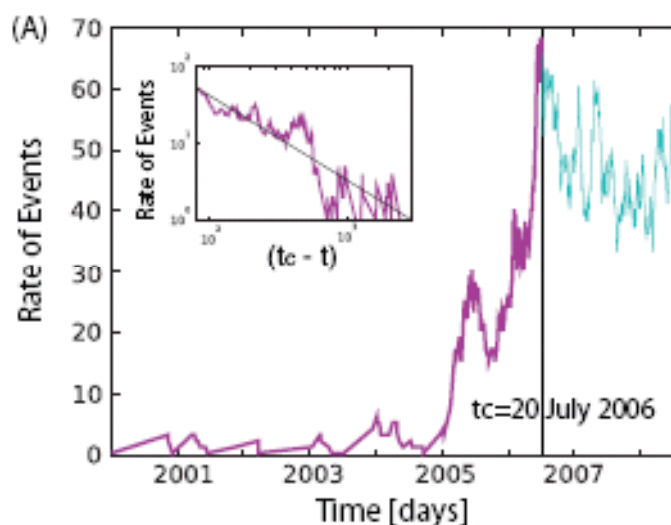
An added difficulty faced by individuals (and data controllers) is that the true risk is difficult to quantify, as it requires knowledge of variables ranging from the number of transactions or processes that involve the disclosure of personal information, as well the number of incidents of data loss or misuse and the amount of financial and other losses incurred as a result.

### 3.2.2 Evidence on the risk of data loss

Empirically, the risk is difficult to measure, principally due to a lack of good data. A recent attempt by Maillart and Sornette (2009) to quantify the risk, based on 956 events of data loss documented by the Open Security Foundation<sup>43</sup>, shows a rapid increase in the incidence of data loss, which might have reached a plateau in 2006, although the average size of loss events continues to increase.

<sup>43</sup> See <http://datalossdb.org/>. The coverage is international, although the preponderance of incidents is in the United States.

Figure 5: Rate of identity loss events (2000-2008)



Note: The rate of ID loss events in sliding windows of fifty days is plotted as a function of time, revealing the existence of two successive regimes: (i) explosive growth culminating in July 2006 and (ii) stable rate thereafter. The inset shows a non-parametric test suggesting that the first regime was characterized by a faster-than-exponential growth.

Source: Maillart and Sornette (2009)

An obligation to notify data breaches would make risk assessment more accurate, and could form the basis for rational consumer decision-making about privacy risks due to disclosure of personal data.<sup>44</sup> This would need to include at a minimum the type of data that was compromised, the number of records, the proportion of compromised records out of the total records of the same type, and the direct loss (e.g. money stolen from bank accounts) that resulted from the breach.

Further, it is important to quantify the size of the potential economic loss to consumers. Again, no reliable figures are available. A possible approach to estimating direct monetary losses is to use the market price of stolen personal data. Assuming the underground market in personal data is competitive; the prices should reflect the risk-adjusted marginal benefit of personal data to criminals, which is equal to the direct loss suffered by individuals (although the loss might ultimately be borne by data controllers, depending on liability). An overview of prices paid for personal data on underground economy servers is shown in Table 7. The table shows that bank account credentials commands the highest prices, indicating that they are the data items most likely to result in financial losses when stolen.

<sup>44</sup> However, see Romanosky et al. (2008). The authors find that state-level disclosure laws in the United States have only a very weak effect on the incidence of data loss.

**Table 7: Prices for personal data sold via underground economy servers (2008)**

| Rank | Item                     | Percentage of incidents* | Price range        |
|------|--------------------------|--------------------------|--------------------|
| 1    | Credit card information  | 49.2%                    | \$0.06-\$30        |
| 2    | Bank account credentials | 29.2%                    | \$10-\$1,000       |
| 3    | E-mail accounts          | 7.7%                     | \$0.10-\$100       |
| 4    | E-mail addresses         | 7.7%                     | \$0.33/MB-\$100/MB |
| 5    | Full identities          | 6.2%                     | \$0.70-\$60        |

Note: \* percentage of observed incidents of personal data items for sale on websites and Internet Relay Chat (IRC) channels.

**Credit card information:** includes credit card number and expiry date. It may also contain the cardholder name, Credit Verification Value 2 (CVV2) number, PIN, billing address, phone number, and company name (for a corporate card). CVV2 is a three or four-digit number on the credit card and used for card-not-present transactions such as Internet or phone purchases. This was created to add an extra layer of security for credit cards and to verify that the person completing the transaction was in fact, in possession of the card.

**Bank account credentials:** may consist of name, bank account number (including transit and branch number), address, and phone number. Online banking logins and passwords are often sold as a separate item.

**E-mail accounts:** includes user ID, e-mail address, password. In addition, the account may contain personal information such as addresses, other account information, and e-mail addresses in the contact list.

**E-mail addresses:** consists of lists of e-mail addresses used for spam or phishing activities. The e-mail addresses can be harvested from hacking databases, public sites on the Internet, or from stolen e-mail accounts. The sizes of lists sold can range from 1 MB to 150 MB.

**Full identities:** may consist of name, address, date of birth, phone number, and government-issued number. It may also include extras such as driver's license number, mother's maiden name, e-mail address, or "secret" questions/answers for password recovery.

Source: *Symantec Global Internet Security Threat Report, Volume XIV (2009)*

Another approach to quantification of the risk is to determine individual's willingness to pay for protection, e.g. through experiments. For example, Hann et al. (2002) collected the results from experiments in which people trade-off personal data for monetary rewards to map individuals' willingness to pay for privacy. They show that the disallowance of secondary uses of personal data is worth approximately € 30 (\$ 40) and € 37 (\$ 50) to people. Although the validity of these figures depends on the accuracy of individuals' risk perception, the advantage of this approach is that it can measure individuals' valuation of intangible losses resulting from the loss of personal data.

Another factor that needs to be taken into account to assess the extent of the risk for individuals is how much of their personal data is being held by data controllers, both in terms of the type of records that are being kept (as Table 7 suggests, losses will be different for different types of personal data) and in terms of the number of different data controllers that hold such records.

Clearly, the amount of personal data held by data controllers is going to differ widely across individuals. For example, our stakeholder consultation revealed particular concerns about the volume of personal data disclosed by young people (see Section 4). An attempt to measure the type of data held by various institutions on the 'average' citizen was undertaken for Austria by a labour/consumer association (AK Wien) in 2009. The results are shown in Table 8 overleaf. The table shows the type of personal data collected by various public and private sector organisations and the probability that such data is being held.

While the situation is likely to differ to some degree across Member States, we consider Table 8 to represent a good approximation of the 'data tracks' individuals leave in their everyday lives. One important insight from Table 8 is that data controllers in the public sector collect markedly more pieces of personal information than those in the private sector. This is particularly striking when it



comes to data on personal circumstances, living conditions and personal history, data that is likely to be considered especially sensitive by many consumers.

Information on personal habits and preferences, on the other hand, is collected primarily by the private sector, for which such information is of obvious commercial value. Other personal information, for example income data, credit history, and bank details, are collected by public and private bodies in approximately equal measure.

One implication is that a 'one size fits all' approach to PETs deployment is unlikely to be practical. Different types of organisations have different needs when it comes to PETs, depending on the sensitivity and the volume of personal data they control. Moreover, public expectations about data security are likely to be different for different institutions, which changes the latter's incentives for investing in PETs.

Table 8: Overview of data tracks of the average Austrian citizen

|                     | Institution/Organisation                                                | Public Sector |               |                          |              |                                      |                 |                  |            |                  |                    | Private Sector |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|---------------------|-------------------------------------------------------------------------|---------------|---------------|--------------------------|--------------|--------------------------------------|-----------------|------------------|------------|------------------|--------------------|----------------|----------------------------|----------------------------|-----------------|-------------------|--------------|-----------------|----------------------|----------------------|---------------------------|------------------------|---------------|
|                     |                                                                         | Registration  | Land Registry | Municipal administration | Police/court | Federal Armed forces/ Social Service | Tax authorities | Social insurance | Health/GDA | Education system | Statistics Austria | Employer       | Financial Service provider | Telecommunications provide | Religious group | Private insurance | Radio, Media | Societies/clubs | Loyalty card/profile | Credit Rating Agency | Internet Service Provider | Mailing list publisher | Internet shop |
| Standard basic data | Name                                                                    |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Gender                                                                  |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Extended basic      | Title                                                                   |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Postal address                                                          |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| data                | Phone number (fixed phone, mobile)                                      |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Phone number (phone card)                                               |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Private cv data     | Fax number                                                              |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | email address                                                           |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Private life        | ZMR-number                                                              |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Date of birth                                                           |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Insurance           | Place of birth                                                          |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Marital status                                                          |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Body                | Nationality                                                             |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Occupation                                                              |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Financial data      | Work place                                                              |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Number of children                                                      |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Assets              | Education                                                               |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Religious beliefs                                                       |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Contacts            | Family members                                                          |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Size of accommodation                                                   |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Habits              | Flatmates                                                               |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Neighbours                                                              |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Delinquency         | Social security number                                                  |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Insurance details (life-, health and car insurance)                     |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Dynamic data        | Health history                                                          |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Biometrics (DNA, retina scans, photo, fingerprints)                     |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Private cv data     | Bankdata/creditcard                                                     |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Income                                                                  |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Assets              | Expenditures                                                            |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Creditworthiness                                                        |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Contacts            | Taxes paid                                                              |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Real estate                                                             |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Delinquency         | Other assets                                                            |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Criminal record (saved by police)                                       |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Habits              | Business contacts(point in time, frequency, duration, medium, location) |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Private contacts(point in time, frequency, duration, medium, location)  |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Delinquency         | Dynamic data                                                            |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Leisure activities                                                      |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Contacts            | Shopping behaviour                                                      |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     | Visited webpages & personal preferences                                 |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
| Habits              | Political attitude and interests                                        |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |
|                     |                                                                         |               |               |                          |              |                                      |                 |                  |            |                  |                    |                |                            |                            |                 |                   |              |                 |                      |                      |                           |                        |               |

Legend:

■ Data is highly likely to be registered and/or saved  
■ Data is not very likely to be registered or saved.  
empty cell= Data are very unlikely to be saved

Source: AK Wien (2009), available at: [http://wien.arbeiterkammer.at/bilder/d89/Erhebung\\_Datenschutz.pdf](http://wien.arbeiterkammer.at/bilder/d89/Erhebung_Datenschutz.pdf) (in German)

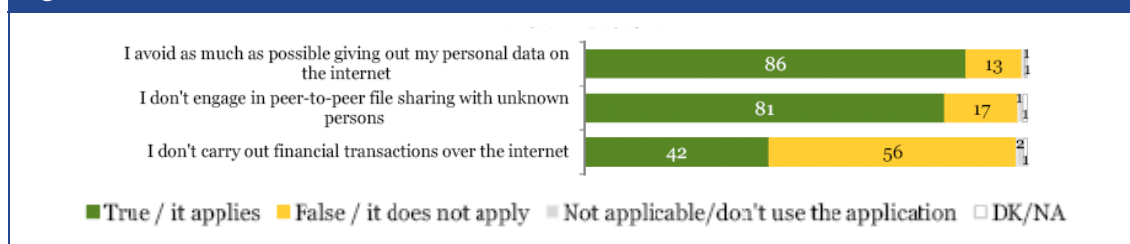
### 3.2.3 Evidence on individuals' risk perception

Risk perception of individuals (and the degree of their risk aversion) is at the heart of the issue of PETs deployment: if the disclosure of personal information is seen as fraught with risk, and if PETs are seen as effective in mitigating the perceived risk, consumer demand for PETs should increase.

There is a considerable body of survey evidence suggesting that a more comprehensive deployment of PETs could lead to an expansion of demand. However, increasing the level of PETs investment is only socially optimal if the risk perception is accurate. It is important to emphasise that the risk that personal data is compromised is real, serious, and – by many accounts – growing inexorably. There is no doubt that the consequences can be very serious, ranging from stress and anxiety to financial damage through theft and fraud and in some cases even to job-loss and wrongful imprisonment.<sup>45</sup>

Opinion surveys regularly find high levels of consumer concern about online privacy. The 2009 Eurobarometer Survey 'Confidence in the Information Society' shows that 90% of consumers in the EU are aware of privacy violations like leakage or abuse of personal information sent on the Internet. Almost as high (86%) is the proportion of people who claim they are reluctant to give out personal information on the Internet (Figure 6).

**Figure 6: Consumer risk aversion**

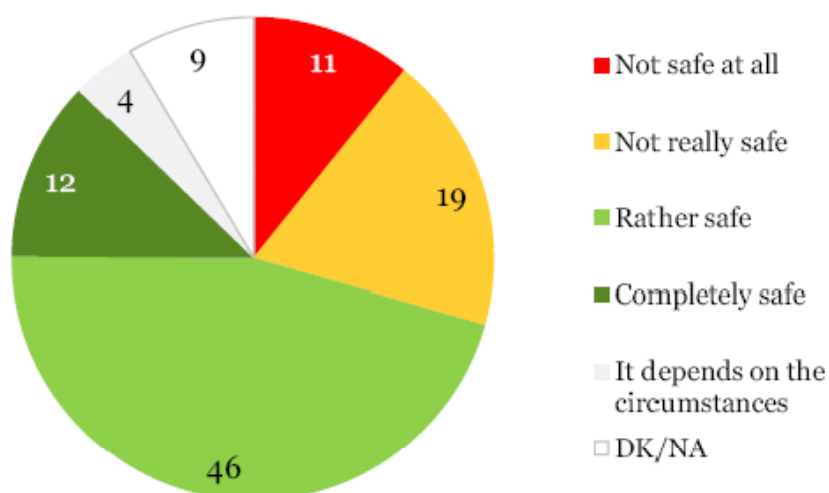


Note: Base: all respondents, % of EU27.

Source: Flash Eurobarometer No 250 – Confidence in the Information Society (May 2009)

At the same time, according to the survey, only 5% of people have experienced misuse of their personal information after disclosure on the Internet. Overall, 30% of users have significant doubts about the security of online transactions (i.e. they see transactions over the Internet as 'not safe at all' or 'not completely safe'; see Figure 7).

<sup>45</sup> See Syverson (2003).

**Figure 7: Perceived security of transactions over the Internet**

Note: Question: How safe do you feel when you carry out transactions over the Internet? Base: all respondents, % of EU27.

Source: Flash EB No 250 – Confidence in the Information Society (May 2009)

The Eurobarometer survey also found that a substantial minority (42%) of European citizens report that they do not carry out financial transactions over the Internet as a precaution against data loss and the ensuing risk of economic loss (Figure 6). However, it should be noted that the absence of widespread PETs deployment has not prevented the e-commerce market from growing quickly in the past.

Similarly, the 2008 Eurobarometer Survey on EU citizens' perceptions of data protection shows that data protection is an issue for the majority of people, with close to two-thirds of respondents (63%) concerned about whether organisations handle their personal data appropriately. More specifically, in relation to online data transmission, 82% of people felt that using the Internet to transfer personal data was not secure; with only 15% of people feeling that they trusted Internet data security.

It is important to note that people's perceptions differ across Member States. At the time of the study, in Austria and Germany, for example, around two-thirds of people claimed to be "very concerned" about how data controllers handle personal data, while only 38% of people in the United Kingdom, 20% of people in Estonia and 8% of people in the Netherlands expressed a similar level of concern. Overall, however, concern about the security of personal data in the European Union can be described as high.

### 3.2.4 Perceptions vs. actual behaviour

In contrast to the evidence presented in the previous sub-section, which shows considerable levels of consumer concern about the protection of personal data, a number of data protection authorities voice concerns that people are careless with their personal data (see Section 4). This suggests that individuals' actions in relation to privacy may be quite contrary to the evidence

presented above. Such a discrepancy between reported views and actual behaviour has been observed by a number of studies within behavioural and experimental economics.

This experimental economics approach has an advantage over survey evidence because it relies on people's real-world decisions (or decisions similar to those they would face in real-world settings) rather than their opinions alone.

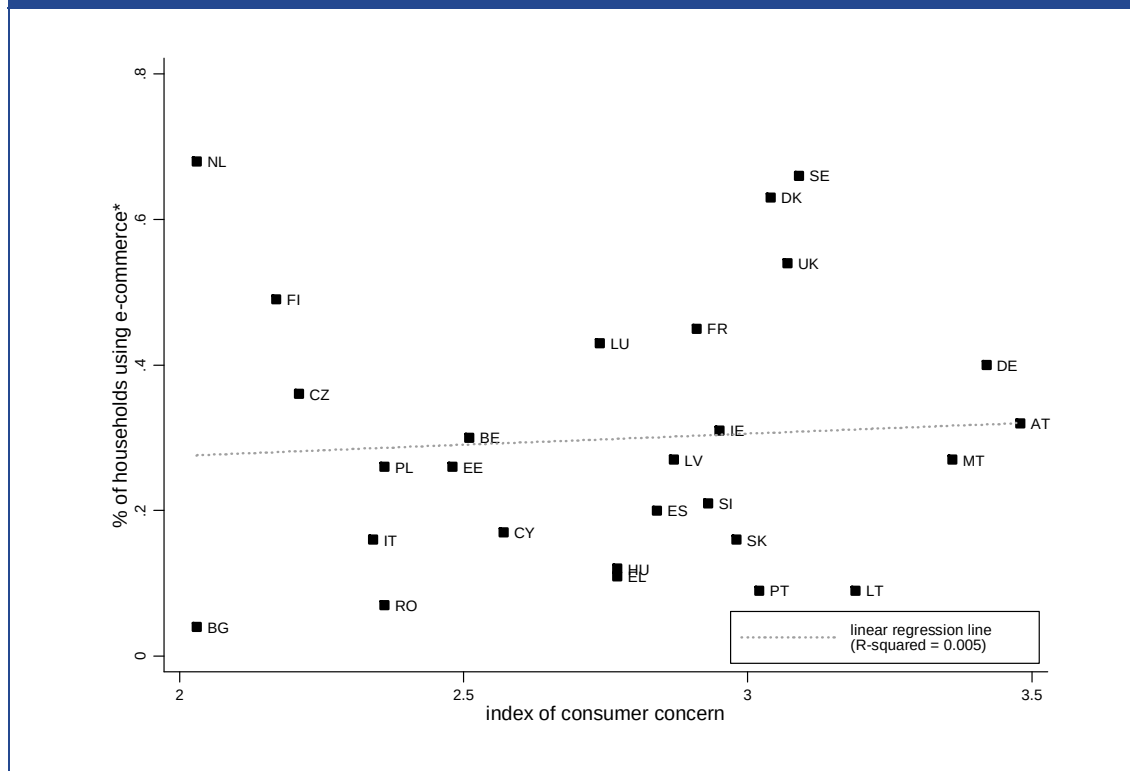
Examples of experiments in which behavioural biases, that is, systematic deviations from the behaviour that would be expected if individuals were completely rational in their actions, have been identified with regard to privacy choices include the following:

- Hui et al. (2006) use a field experiment to test whether people are willing to disclose personal data for small monetary rewards. In a laboratory setting, the authors find that people are willing to provide companies with more personal data on websites that are designed in slightly more appealing ways.
- Berendt et al. (2005) find that people are more willing to provide their home address to online retailers when faced with a virtual shopping assistant (as one might find in conventional stores).
- Earp and Baumer (2003) find that reputation is important, with 415 respondents participating in a study where the respondents, who were shown the web pages of more well-known websites, provided far more personally identifiable information (e.g. phone numbers, home addresses, e-mail addresses, etc.).

Various reasons why people exhibit “behavioural biases” in relation to their privacy choices have been identified in the literature:

- The costs of a privacy violation (e.g., receiving direct marketing e-mails sometime in the future) are considered remote compared to the benefits that might be experienced by making an online decision today (e.g., receiving a discount on a product for signing on to a direct marketing e-mail list).
- The lack of an established link between an action to relinquish one's privacy and the consequences. For example, it is not always clear how third parties get hold of personal data. This lack of feedback prevents individuals from learning to be careful about their privacy in the future.
- The difficulty of truly identifying the benefits associated with privacy. While individuals can easily decide between two meals in a restaurant, they are less able to make choices between, say, small monetary rewards and the experience of privacy.

In order to explore the relationship between individuals' perceptions and actual behaviour, we looked at the correlation between reported concerns about privacy and usage of e-commerce in the EU. Figure 8 shows the correlation between the percentage of households reporting having bought goods or services over the Internet in the last 12 months and an index of the level of concern about privacy risks. The figure suggests no clear relationship exists between the two: high levels of concern do not appear to be linked with low reported participation in e-commerce.

**Figure 8: E-commerce transactions and consumer concern in the EU (2008)**

Note: \* = 'e-participation' in Table 9: % of respondents answering 'yes' to the question: "Please tell me if you have purchased any goods or services in the last 12 months via the internet (website, email, etc.)" (QC1.1.).

Source: *Flash Eurobarometer No. 225 (2008) Data Protection in the European Union*

To validate the conclusions drawn from Figure 8, we estimated econometrically a cross-section model relating e-commerce usage to consumer concern while controlling for the level of Internet access in each country, measured by the percentage of households with broadband Internet connections as reported by Eurostat. The estimated results of this regression analysis are shown below. The estimated coefficient on the "concern" variable is negative, but very small and statistically not very significant. The availability of the Internet, as measured by broadband access, appears to be the major driver of e-commerce activities: the strong positive relationship between the two variables is again shown in Figure 9.

Overall, the conclusion is warranted that consumers may often not act in accordance with their reported concerns when it comes to disclosing personal data.

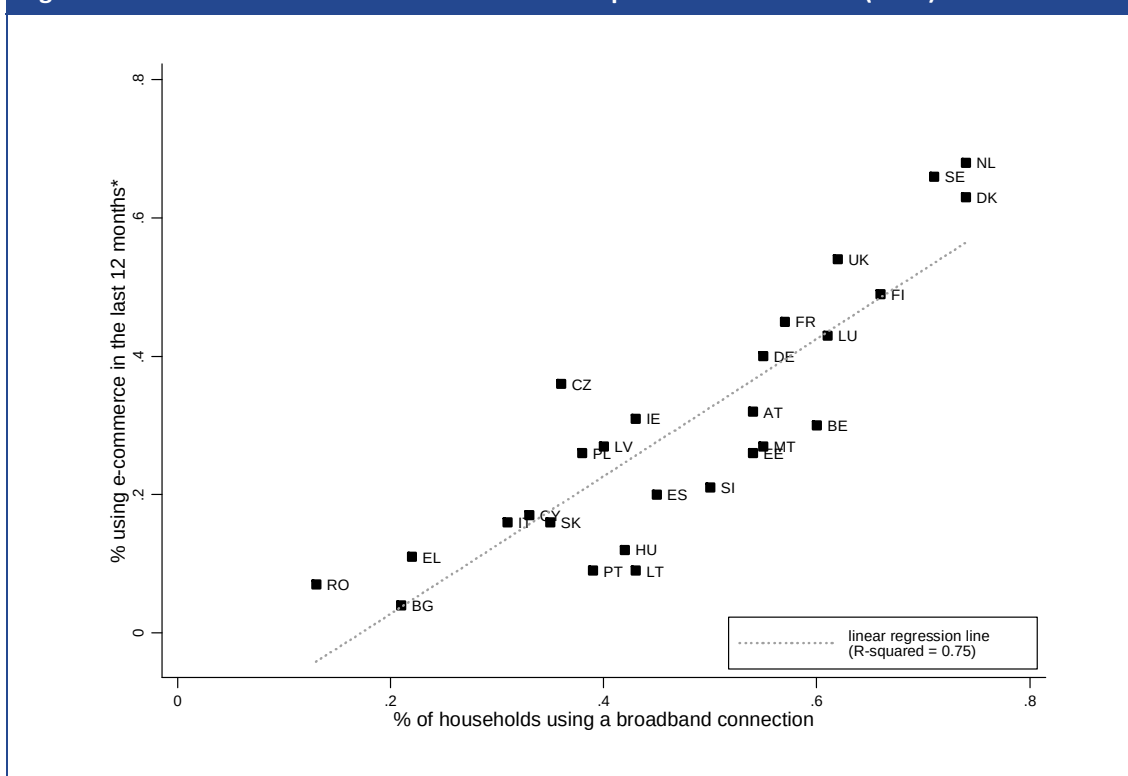
**Table 9: Determinants of e-commerce participation in the EU: regression results**

| <b>e_participation (dependent variable)</b> |                    |                       |          |                 |
|---------------------------------------------|--------------------|-----------------------|----------|-----------------|
| <b>explanatory variables</b>                | <b>coefficient</b> | <b>standard error</b> | <b>t</b> | <b>P&gt; t </b> |
| broadband                                   | 1.04               | 0.11                  | 9.12     | 0.00            |
| concern                                     | -0.07              | 0.04                  | -1.65    | 0.11            |
| constant                                    | 0.01               | 0.12                  | -0.24    | 0.26            |

$R^2 = 0.78$  (goodness of fit), no. of observations = 27

Note: 'e-participation' = % of respondents having purchased goods or services over the Internet in the last 12 months; 'broadband' = % of households with broadband Internet connection; 'concern' = index of consumer concern about privacy protection by data controllers (1 'not at all concerned' – 5 'very concerned').

Source: Eurostat, 2008 Eurobarometer survey (available at <http://www.eubusiness.com/topics/consumer/ecommerce-eu-guide/>, Flash Eurobarometer No. 225 (2008) Data Protection in the European Union

**Figure 9: E-commerce transactions and broadband penetration in the EU (2008)**

Note: \* = 'e-participation' in Table 9: % of respondents answering 'yes' to the question: "Please tell me if you have purchased any goods or services in the last 12 months, in (OUR COUNTRY) or elsewhere in any of the following ways (MULTIPLE ANSWERS POSSIBLE)? Via the internet (website, email, etc.)" (QC1.1.).

Source: Eurostat, 2008 Eurobarometer survey (available at <http://www.eubusiness.com/topics/consumer/ecommerce-eu-guide/>)

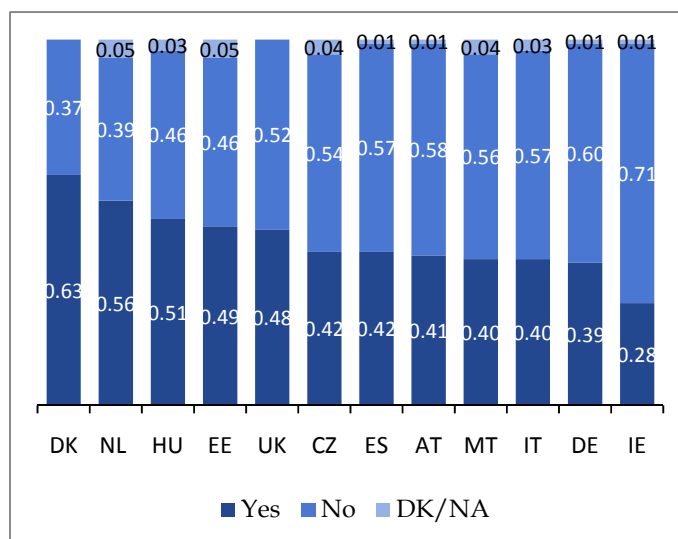
### 3.2.5 Awareness of PETs by individuals

A further factor determining the demand for PETs deployment is the level of awareness of the available technologies and their effectiveness. The Eurobarometer Survey (2008) collected information on individuals' awareness of technologies such as PETs that limit the collection of personal data and showed that a slight majority were unaware of them, while more than two-fifths of people that were aware of them did not use them. Therefore, only approximately one-

tenth of people use technologies that limit the collection of personal data when transmitting information online.

The results show considerable variation across Member States. As shown in Figure 10, in Denmark over 60% of people were aware of technological means with which they could improve data security while in Ireland less than 30% of people had this awareness. However, the survey does not provide information on whether differences in awareness might be caused by the differences in the availability of PETs across European markets.

**Figure 10: Awareness of tools or technologies improving data security**



Note: Have you heard of tools or technologies limiting the collection of personal data from your computer?  
%, Base: who use the Internet/computer, by country.

Source: Flash Eurobarometer No. 225 – Data Protection (2008)

Interestingly, a large proportion (43%) of people who were aware of tools or technologies limiting the collection of personal data chose not to use them, with over one-third of respondents (36%) stating they “wouldn’t know how to use them” or “wouldn’t know how to install them on the computer”.<sup>46</sup> This points to usability as an important factor in raising PETs deployment.<sup>47</sup>

The combined evidence presented above suggests a role for data controllers and public agencies in protecting individuals’ personal data. Most people are concerned about their privacy but are susceptible to behavioural biases that expose them to privacy risks and are unaware of technological means or other channels through which they can protect themselves.

It should be recognised that the evidence is not clear-cut: the willingness to trade-off privacy for small monetary rewards reported in the experimental literature, the apparent willingness of many individuals to engage in online transaction despite reported concerns, and the lack of knowledge

<sup>46</sup> Flash Eurobarometer No 225 – Data Protection (2008).

<sup>47</sup> See Dingledine and Mathewson (2005).



about PETs and data security tools may stem from the fact that people's valuation of privacy is in fact often lower than they report. Given the uncertainty about the risks arising from the disclosure of personal data, which interpretation is the most accurate cannot be decided in the absence of much more detailed empirical research.

### 3.3 Data controllers' deployment decision

After the discussion of individual's demand for PETs, in this sub-section we turn to the deployment decision of data controllers. In part, the deployment decision faced by data controllers resembles the decision by individuals on whether to disclose personal data. However, since data controllers often use personal data to carry out their activities, the trade-off between costs (direct or through a loss in functionality) and benefits of PETs protection, including the effect on competition, becomes important.

#### 3.3.1 Risk of data loss

Whether or to what extent data controllers should offer services that require personal data, and whether they should adopt PETs (here we are considering the case where deployment is discretionary), is in part subject to the same utility calculus that is faced by individuals. The loss of personal data, which in the case of data controllers, can relate to staff, customers, suppliers or other parties (e.g. research subjects) may result in economic losses. These losses can be direct as they are in the case of individuals, e.g. theft and fraud. They can also be indirect, e.g. in the form of official sanctions or private lawsuits following a privacy breach, or in the form of the loss of trust of customers or business partners, resulting in reduced demand for their products and services.

The European Data Protection Directive (Art. 23) clearly specifies that liability for damage as a result of an unlawful processing of personal data normally rests with the data controller, who would thus seem to have a particular strong interest in mitigating the risk of legal sanctions and damages claims.

However, the effect on demand is potentially the most important consideration faced by data controllers. In the worst-case scenario, consumers can threaten to withdraw from transactions involving personal data altogether out of fear of data loss. This might be due to a general feeling of insecurity, rather than concrete fears of economic damage resulting from any particular transaction. This has potentially large costs for businesses and government agencies that derive great efficiencies from carrying out processes electronically. Where there is evidence that a lack of PETs is preventing such efficiencies from being realised, data controllers have a strong incentive to invest in PETs.<sup>48</sup> In the same vein, one of the strongest arguments for PETs is that providing better security would lead to an overall growth in the demand for electronic transactions.

The discussion shows that certain aspects of data controllers' deployment decision mirror the situation of individuals. Specifically, data controllers face the same risk of data loss. However, the deployment decision for data controllers is made more complicated by the fact that they may also want/require personal data to carry out their day-to-day business.

---

<sup>48</sup> Of course, consumers also gain from electronic transactions, but the effect is likely to be stronger for businesses and governments due to economies of scale.

### 3.3.2 Usefulness of personal data

Despite the risks discussed above, to understand the incentives data controllers face when making decisions about PETs deployment, it is important to recognise that the disclosure of personal information to a data controller can be a source of benefit to the data controller and individuals. This is because personal information is a valuable economic resource.

#### ***Benefits of digitisation***

Companies and governments collect and store large amounts of personal information that are used in a variety of applications. Partly, the benefits stem from the use of information technology to carry out the normal tasks of an organisation in a more efficient manner. Many e-government applications, electronic billing, customer feedback facilities, etc. fall into this category. Both data controllers and consumers benefit through the greater efficiency (savings on time, postage, paper, etc.) that electronic processing allows, although the benefits for larger organisations may be greater due to economies of scale.

#### ***Personalised services***

A second type of benefit is the targeting and personalisation of goods and services. This is an extension of what businesses have always done: sending birthday cards to loyal customers, targeting advertising at people who have made purchases in the past, tailoring offers based on observed customer characteristics, etc. Electronic storage and processing of personal information has markedly increased the scope and sophistication of these kinds of activities. Benefits for companies consist of increased sales and customer loyalty, while consumers benefit from lower search costs (e.g. tailored offers from online retailers based on past purchases) and higher utility from personalised goods and services.

#### **Price discrimination**

A special case of personalisation is price discrimination. Price discrimination characterises a set of practices used by firms aimed at using personal data (e.g. on preferences or purchasing histories) to understand consumers' willingness to pay for their goods and services; and then charging consumers different, sometimes personalised, prices on this basis in order to achieve larger overall profits.

Note that a priori there is nothing sinister about this. A typical example of price discrimination is the differentiation between peak and off-peak hours for transportation services, where some individuals (such as business travellers), who place a high value on travelling at certain times, spend more than leisure travellers, who care more about cheap fares than specific travel times. In this example, the preferred travel time is all a company needs to price discriminate. In other applications, more detailed personal data may be required. Private sector data controllers therefore may have a preference not to have restrictions placed on their collection of personal data and not to deploy PETs that keep personally identifiable information on consumers hidden from them.

The conclusions of the existing literature (e.g. Calzolari and Pavan, 2001; Acquisti and Varian, 2005; and Taylor, 2004) are ambiguous on the issue of whether price discrimination has a positive

or negative impact on society as a whole. In simple terms, for some consumers, sharing personal data may be costly because it may allow firms to determine that they would be willing to pay more for a service they are using than they are currently being charged.

However, other consumers that were not purchasing these goods before potentially benefit as a result of firms using personal data to lower the prices they are offered.<sup>49</sup> The net effect is ambiguous. It is an empirical matter to determine whether conditions are such that restricting firms' access to personal data has positive or negative consequences (on a market by market basis).

However, note that the existence of potential benefits of price discrimination for certain types of consumers does not mean that indiscriminate disclosure of personal data is economically desirable. PETs (such as privacy-enhancing identity management systems or credentials) can be used to disclose only the information necessary to realise the benefits of price discrimination. It is important to stress that certain PETs are flexible in the amount of personal data they permit users to reveal and can be configured to some appropriate application-specific level.

Acquisti (2008) considers each of three standard forms of price discrimination and their compatibility with privacy-enhancing identity management systems.

- First degree price discrimination requires firms to be able to estimate the maximum willingness to pay for a good or service for each consumer (such as a doctor in a small town determining on a case-by-case basis call-out charges based on the nature of the property of the patient).
- Second degree price discrimination involves consumers voluntarily choosing different price-quantity combinations of goods and services (such as the purchase of a plane ticket and selecting whether to stay over on Saturday night and thus self-selecting as a business or leisure traveller).
- Third degree price discrimination involves price-setting on the basis of group characteristics (cinema tickets for students and pensioners).

In the case of first and third degree price discrimination, prices can be calculated on the basis of relevant consumer data (e.g. a purchasing history) and linked to the consumer's pseudo-identity via an identity management system, while keeping personal data such as name and address private. Even when the consumer is transacting with the firm, a number of PETs/data security tools such as anonymous/ pseudonymous payments systems (see Chaum, 1985; and Low et al., 1994, respectively) and browsing and messaging technologies can be used to minimise the amount of personal data shared. Although the risk of re-identification remains, given sufficient levels of traffic and trail analysis (see, for example, Narayan and Shmatikov, 2008), these technologies help to make it costly (perhaps prohibitively so) for violations of privacy to take place.

In the case of second degree price discrimination personal data is not necessarily used (as the firm is providing a menu of choices for the consumer to choose from) so privacy-enhancing identity management systems are not required.

---

<sup>49</sup> An added complication is that firms may use personal data to improve the products and services they offer (Varian, 1996).

The only issue that data controllers may face when deploying these PETs is that, once the PETs are in place, demands may be placed on them protect increasingly more personal data, in effect, prohibiting price discrimination. In other words, this type of uncertainty (e.g. the future state of privacy law) means that a business might limit its future choice set by investing in PETs (for further details, see the discussion of the PETs deployment decision as a *real option* in sub-section 3.3.3).

### ***Personal data as a productive resource***

A further type of benefit stems from the use of personal information as a raw material, which data controllers use to create new products, services and business methods. It is here that information technology holds the greatest promise, even though the use of personal information as an input in business innovation is again nothing fundamentally new and can be seen as a step in the evolution of market research methods. Benefits in this third category can overlap with the personalisation benefits described above, but are distinguishable by their greater innovative potential.

A wide variety of applications are made possible by the processing of personal information. Examples include social networking sites on the Internet, sophisticated market analysis using data collected through store cards, online market places and payment systems, and applications in medical and social research. The range of examples shows that the benefits for consumers and data controllers are multi-faceted, and potentially far-reaching.

### **Externalities, long-term and network effects**

It is important to stress that the benefits that can be derived from exploiting personal data (including anonymised data that is vulnerable to advanced de-anonymisation attacks) can exceed the direct benefits to consumers and data controllers. A straightforward example is the use of personal information in epidemiology, where disclosure of medical details can lead to better protection for everyone, including people who did not disclose any personal information themselves.

Moreover, in some applications, benefits increase with the volume of personal information that is available. Examples are electronic exchanges and social networking sites, whose service becomes more valuable with the number of users. Each act of disclosure increases the value of the service for every participant.

In addition, there are longer-term effects: if personal information is used as an input, limiting its use may compromise the future development of certain applications, place constraints on innovation and restrict the growth of the market for electronic services. All these examples suggest that restrictions on the use of personal data have costs that are not necessarily taken into consideration by data controllers and individuals when making decisions about the use or disclosure of personal data and the deployment of PETs that might limit their usefulness. This may suggest a role for public sector intervention to promote the use of PETs that are effective in protecting privacy, while at the same time allowing the socially beneficial exploitation of personal data.

### **Personal data as a tradable commodity**

Electronic storage and transmission transform personal information into a tradable good.<sup>50</sup> This potentially increases the usefulness of personal information as a productive resource, as the party that collects the data might not always be the one that can make the best use of it. Tradability – given the consent conditions stipulated by existing data protection legislation are met – thus has the potential to increase the efficiency of production processes that use personal information as an input.

A situation can be conceived in which the deployment of strong PETs that eliminate the need for personal data by data controllers who are not themselves interested in exploiting the personal data leads to losses for third-party data users who used to buy personal data from the data controllers. Note that this loss is independent of any benefits the original data controllers derive from the PETs.

However, it is equally conceivable that the deployment of adequate PETs increases the benefits described above. For example, consent mechanisms that allow the trade in personal data to take place more transparently (and to the benefits of the individuals whose data is being traded) may lead to a much more competitive and efficient market in personal information. Thus, it is important to understand the consequences of different types of PETs for the trade in personal data.

### **Proportionality**

The preceding discussion shows that not all PETs are compatible with a thriving market for personal data, which is an important part of the digital economy. Personal data as an input has many benefits and focusing narrowly on PETs that limit or eliminate the use of personal data may be economically inefficient in some cases. In such circumstances, the emphasis should be on PETs that allow the benefits to be achieved in as privacy-friendly a manner as possible. In other words, proportionality is important when assessing the economic benefits of PETs

The issue can be illustrated by using the example of statistical databases based on personal information. For many applications, such databases do not need to contain personal data as such. Anonymised data is typically sufficient. Data mining and statistical processing of the databases can thus be carried out without invasion of privacy.

However, recent advances in de-anonymisation techniques<sup>51</sup> mean that such processing can no longer be considered privacy-neutral in the case of conventionally anonymised or de-identified datasets (k-anonymity<sup>52</sup>,  $\ell$ -diversity<sup>53</sup>).

<sup>50</sup> Of course, personal information can in principle be traded irrespective of the way it is stored, although the assumption that the volume of such transaction is minuscule compared with what can be done using electronic data processing appears plausible.

<sup>51</sup> See Shmatikov (2008).

<sup>52</sup> See footnote 14 on p. 11.

<sup>53</sup> The concept of “ $\ell$ -diversity” refers to the distribution of target values within a group of records that share the same quasi-identifier in a de-identified dataset. If a group of k different records share the same quasi-identifier, an attacker cannot identify the individual

But, while PETs for secure anonymisation exist<sup>54</sup>, these have been shown to reduce the utility of the data for (non-privacy-invasive) data mining purposes.<sup>55</sup> The question then is whether deploying these PETs is a proportional response to the threat level. Here, it has to be considered that some complex threats that are discussed in the computer science literature might be very unlikely in practice.<sup>56</sup>

### 3.3.3 PET deployment as a real option

On a more abstract level, deployment is determined by the value firms place on PETs under conditions of uncertainty. This can be understood by looking at the deployment decision in a real-option framework.

The real options model focuses on firms' deployment decisions as any other investment choice under uncertainty, as discussed by Stoneman (2001) and Dixit and Pindyck (1994). The key insight of this model is that it highlights the fact that even if the benefits for data controllers of adopting PETs are higher than the costs, a data controller may still decide against adoption. There are several reasons for why this is the case.

- Firstly, due to uncertainty, it is unclear what the future stream of benefits of adopting PETs might be. If the benefits exceed the costs today, it is not certain that this will be the case next year. The firm may therefore choose to delay deployment until it is clearer that benefits outweigh costs.
- Secondly, investments into some PET involve some amount of “sunk costs”, i.e., costs that are un-recoverable or costly to reverse. For instance, the configuration of PETs for the specific uses of an organisation is costly as is training employees to use the PET; and these costs cannot be recovered if the technology is to be sold in some secondary market. This feature of PETs also implies that there is a value to delaying deployment, for instance, due to the likely introduction of a superior technology in the future.

### 3.3.4 Potential supply-side market failure

Even in situations where PETs are unambiguously beneficial, it is possible that deployment levels will be sub-optimal or ineffective. A variety of barriers to the effective deployment of PETs have been identified in the economic literature on information security. These fall into two categories:

- hidden action problems (moral hazard); and
- externalities.

This sub-section synthesises the theoretical explanations and empirical evidence on barriers identified in prior research.

---

based on the quasi-identifier. But if the value of interest (e.g. the individual's tax status) is the same for everyone in the group, the use of quasi-identifiers does not conceal any individual's value from attackers.

<sup>54</sup> E.g. *differential privacy*, see Dwork (2006).

<sup>55</sup> See Shmatikov and Brickell (2008), Machanavajjhala et al. (2008) and Alexander et al. (2010).

<sup>56</sup> Machanavajjhala et al. (2008).

### **Hidden action problems**

Hidden action or moral hazard is a special case of information asymmetry and occurs in situations where one party in a transaction has more information than another. Specifically, the party that is insulated from risk generally has more information about its actions and intentions than the party paying for the negative consequences of the risk. More broadly, hidden action occurs when the party with more information about its actions or intentions has a tendency or incentive to behave inappropriately from the perspective of the party with less information.

For example, if consumers are not well-informed about privacy risks and PETs, data controllers may be able to offer a sub-optimal level of protection without fear of being driven out of the market by better products. If privacy violations occur, a data controller can attribute this to advances privacy-invasive technologies and perhaps even charge its customers extra to put PETs in place (Feigenbaum et al., 2002).

It is difficult for individuals to overcome the problem of asymmetric information when it comes to choosing between data controllers. Edelman (2006), for example, showed that a sample of websites approved by security rating agencies in fact offered worse privacy protection than a random sample of websites. This is because the privacy-invasive websites seeking to violate individual privacy are more likely to seek out a rating agency to provide a rubber stamp of approval.

### **Externalities**

Externalities arise when one party's actions have consequences for others that are not reflected in the costs incurred by the party producing the externalities. Certain PETs, such as remailers (see Section 2.3.1) exhibit network externalities because the level of privacy users enjoy depends on the number of other users of the PET.

Another important externality in the context of PETs arises from 'logical diversity'. Put simply, this means the greater the variety of available PETs, the less likely is any one attack to succeed. On the other hand, if the set of available PETs do not possess logical diversity, then data thieves may be able to swiftly compromise large volumes of personal data with a given attack strategy.<sup>57</sup>

On the data controllers' side, high-profile privacy breaches may tarnish the reputation of a whole sector, even if some data controllers in the sector offer very high standards of privacy protection. The overall level of security in a system can depend on the "sum of all investments", the "weakest link" or the "best shot". Grossklags et al. (2008) explore investment levels in PETs under these different assumptions. While they make some specific assumptions, their results are still instructive.

- If PET effectiveness depends on the weakest link or the sum of all investments, then a large homogenous population of firms (e.g. a large number of SMEs) will typically under-invest in information security.

---

<sup>57</sup> See Anderson et al. (2009) on the dangers of limiting the logical diversity of PETs.

- If a diverse range of firms exist however, such as a few big firms among SMEs, the incentive might be large enough for big firms to take a leadership role – i.e. they benefit from such a large proportion of PET investments made that any additional benefits other firms receive are inconsequential to investment decisions.
- In situations where the overall level of information security is dependent on the “best shot” then there is relatively little need to coordinate firms over PET investments.

How the investment decisions of individual data controllers affect the overall level of PETs deployment determines the appropriate policy response. With regard to some privacy enhancing technologies, data controllers can independently and successfully deploy PETs. With regard to others, data controllers may need to be encouraged to adopt PETs via technological leadership, subsidies, coordination or other public or private actions.

### 3.4 PETs and competition

This sub-section is about the role PETs might play in inter-firm rivalry. It is looking at the issue of demand responses to PETs from the point of view of individual data controllers. Previously, we stressed the effect of PETs on demand for the services of data controllers in general, whereas here we are concerned with the benefit data controllers may achieve *at the expense of their competitors*.

#### 3.4.1 PETs as an aspect of quality competition

If consumers care about privacy protection, PETs can give businesses a competitive advantage: in theory, at least some consumers are likely to switch their custom to businesses that can credibly claim to offer better protection than their rivals. PETs are one way to support this claim. The competitive advantages PETs confer are frequently invoked by data protection authorities and could represent a strong driver of increased PETs deployment.

Despite the importance of reputation, relatively little reliable empirical work has been undertaken to measure its value in the context of privacy. This is partly because it is difficult to measure the value of an intangible asset such as reputation. But, it is also difficult to obtain good quality data on the costs of reputation loss (e.g. through privacy breaches) since firms may be unwilling or unable to quantify their losses.

However, event studies avoid the problem of lack of data by focusing on the stock price reactions to privacy breaches at listed companies. The methodology controls for market trends and volatility, without relying on self-reported loss data provided by firms, to precisely identify the cost of a privacy incident on the market value of a firm.

This places a monetary value on privacy incidents that embodies market participants’ expectations of the financial losses, capturing both the effect of reputation loss as well other consequences for firm value, such as the effect of sanctions or fines.



### 3.4.2 Evidence on reputation loss due to data security breaches

A study conducted by Acquisti, Friedman and Telang (2006) estimated the market reaction to the following types of privacy incidents:

- poor security practices;
- hacker attacks;
- insider attacks;
- computer or data thefts;
- loss of data or equipment; and
- other incidents such as the illegal sale or handling of individual data.

It found a moderately negative, statistically significant cumulative drop in share prices per privacy incident of close to -0.6% on the day following the event, which equates to an average loss of approximately € 7.4 million (\$ 10 million) in market value. Interestingly, the results shows that the largest drops in share prices on the day of the event are experienced by retail companies. The authors argue that this can be explained by the ease with which consumers can switch to another retailer, compared with greater reluctance to switch financial companies, for example. Moreover, the negative effects were greater in cases where there was evidence of the involvement of a malicious actor (data theft).

More generally, one observes that the size of the market reaction identified in Acquisti, Friedman and Telang (2006) is within an order of magnitude of other similar announcements made by firms, giving a sense of the economic value of reputation and the cost of sanctions. These (Jarrell and Peltzman, 1985; Chatterjee et al., 2001; Im et al., 2001; Dos Santos et al., 1993; Hendricks and Singhal, 1997) are also shown in Table 10 overleaf.

There is some evidence that security breaches involving personal data are more damaging to companies than other security breaches: Campbell et al. (2003) find that security breaches in which personal data was accessed had a significant impact on a company's stock market valuation, while the effect of incidents that did not involve personal data was insignificant. Among privacy breaches, those that involve financial data tend to result in larger share price reactions as might be expected given the value of the information.

While the losses described in Table 10 appear to be small, often reverting to zero within a few days of an announcement, one must be aware of the assumptions on which event studies proceed – namely the effectiveness with which firms' fundamental valuations are reflected through market reactions to news – and therefore one must be cautious about drawing strong conclusions regarding the importance to data controllers of reputational effects following privacy incidents.

In deciding whether to deploy PETs, data controllers weigh up the benefits that the PETs may yield as a result of an improved reputation for privacy protection against their costs.

**Table 10: Summary of event studies**

| Classification of event study                                                 | Authors                                                     | Time period | Number of events | Compound share-price reaction (%) |
|-------------------------------------------------------------------------------|-------------------------------------------------------------|-------------|------------------|-----------------------------------|
| Impact of data breaches on share price                                        | Acquisti, A., Friedman, A., and Telang, R. (2006)           | 2000-2005   | 79               | -0.58                             |
| Impact of vulnerability disclosures                                           | Telang, R. and Wattal, S. (2004)                            | 1999-2004   | 146              | -0.65                             |
| Impact of security breaches on firms<br>(personal data accessed)              | Campbell, K., Gordon, L.A., Loeb, M. P. and Zhou, L. (2003) | 1995-2000   | 11               | -5.4                              |
| Impact of security breaches on firms<br>(all security breaches)               | Campbell, K., Gordon, L.A., Loeb, M. P. and Zhou, L. (2003) | 1995-2000   | 43               | -1.9*                             |
| Impact of security breaches on firms                                          | Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004)        | 1998-2000   | 66               | -2.1                              |
| Impact of security breaches on firms                                          | Hovav, A. and D'Arcy, J. (2003)                             | 1998-2002   | 23               | Not significant                   |
| <b>Comparison results: effect of announcements with impact on share price</b> |                                                             |             |                  |                                   |
| Impact of auto recall announcements                                           | Jarrell, G. and Peltzman, S. (1985)                         | 1967-1981   | 116              | -0.81                             |
| Impact of auto recall announcements                                           | Davidson, W. L. III and Worrell, D. L. (1992)               | 1968-1987   | 133              | -0.68                             |
| Impact of IT investment announcements                                         | Chatterjee, D., Richardson, V. J. and Zmud, R. W. (2001)    | 1987-1998   | 96               | 1.16                              |
| Impact of IT investment announcements                                         | Im, K. S., Dow, K. E. and Grover, V. (2001)                 | 1981-1996   | 238              | Not significant                   |
| Impact of IT investment announcements                                         | Dos Santos, B. L., Peffers, K. and Mauer, D. C. (1993)      | 1981-1988   | 97               | Not significant                   |
| Impact of winning a quality award                                             | Hendricks, K. B. and Singhal, V.R. (1997)                   | 1985-1991   | 0                | 0.59                              |

Note: \*not significant at the 10% level.

Source: Acquisti et al. (2006)

### 3.4.3 Potential downsides of PETs as a quality signal

A necessary precondition for a beneficial deployment of PETs in a competitive setting is that the PETs are effective (i.e. they protect personal data from misuse) as well as efficient (i.e. they are the cheapest means of achieving a given level of protection). If consumers' knowledge about PETs is limited, there is a danger that a business might not deploy the best PETs, expecting that consumers will be content in the knowledge that at least some PET is used. This could also mean that data controllers may be tempted to deploy legacy PETs with higher 'brand recognition' instead of cutting-edge-but-obscure PETs that offer better protection. While the level of privacy protection in this situation is likely to be better than if no PETs were used, it might be sub-optimal.

In particular cases, PETs may be used as a tool for foreclosure. In cases where incumbents use proprietary PETs that come to be seen as benchmarks of protection quality by consumers, this could place competitors using other (potentially cheaper and more effective) PETs at a disadvantage. This is particularly relevant in situations where PETs are integrated into business processes, so that it is difficult to switch between different PETs.

The fact individuals cannot easily measure the efficiency of specific PETs means that the use of PETs in the competitive process thus might not result in the optimal level of deployment or the selection of the most efficient PETs. However, it should be noted that the effects described above are purely theoretical at this stage. We have not seen any evidence that the anti-competitive use of PETs is currently an issue for data controllers.

### 3.4.4 Strategic PETs deployment

Another interesting aspect of competition using PETs is the interaction between technology and legislation. PETs that reduce the need for personal data have the potential to change what is considered 'proportional' data use. A new PET could thus in theory render a whole class of applications/business models illegal at a stroke. By being the first to deploy such a 'paradigm-shifting' PET, a data company may gain a competitive advantage, as it can force competitors to incur adjustments in order to fulfil their obligations under data protection legislation. Note that this mechanism creates an incentive for companies to deploy the best PETs available at all times. Again, this argument is theoretical only at present. We have seen no evidence that such a strategy is being considered by data controllers.

### 3.4.5 Competition in the business-to-business market

So far, we have discussed competition in the consumer market, where data controllers interact directly with individuals and where personal data is exchanged between individuals and data controllers. However, PETs might have a much larger role to play in the business-to-business market. The difficulties that constrain the demand for PETs from individuals have been discussed above. It is reasonable to assume that data controllers are, on average, better informed about the risks associated with holding personal data and more technically competent than individuals, so that the constraints are less severe. Most importantly, personal data in the hand of businesses, especially if the latter derive value from them, take on the characteristics of valuable assets, which data controllers have a strong incentive to protect.

Many business models involve the outsourcing of certain data storage and processing tasks to specialist providers. Given the value of the data, it is important from a business perspective that these secondary data controllers keep the data secure. If such data are stolen, this represents not only a breach of the privacy of the individuals whose data is being compromised; it also presents a direct loss to the primary data controller (for example, competitors may use the stolen data to target a rival's customers). Because of this, some of the data protection experts we interviewed regard the demand for PETs from other data controllers as more effective in driving deployment than demand from individuals. Moreover, assuming a higher sophistication of businesses when it comes to choosing providers based on the PETs they use, the potential downsides of PETs as quality signals mentioned above are reduced.

### 3.5 Patterns of technology adoption

Apart from the factors that determine the deployment decision of individual firms, there are more fundamental explanations as to why deployment levels of new technologies can be low, at least temporarily, despite their apparent usefulness. This is an important consideration in the PET context, as with modern information technologies more generally, the current situation is subject to continuous change.

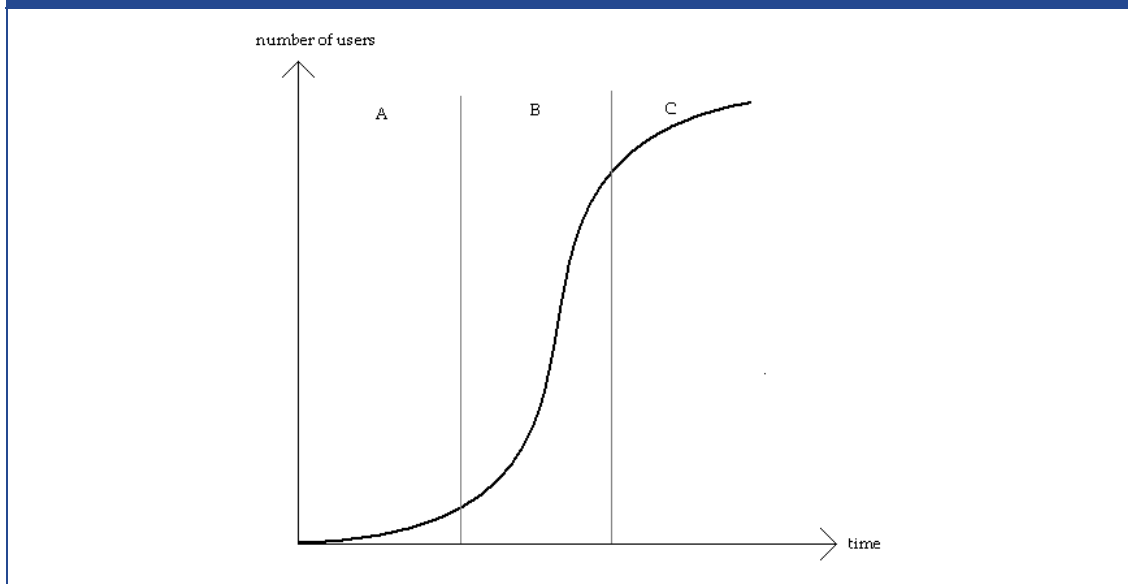
#### 3.5.1 The S-curve

The evolution of new technologies often follows an S-curve pattern when the number of users of the new technology is tracked over time. This observation has been made in areas as diverse as the coal, iron, steel, brewing and railroad industries, as well as information and communication technologies (see Griliches, 1957; Mansfield, 1968; and Rogers, 1995 for seminal studies).

Given the frequency with which S-curves describe the take-up of new technologies, it is useful to analyse the determinants of this shape in order to determine whether they provide any insights into the pattern of PET deployment by data controllers, and SMEs in particular.

Figure 11 below shows a typical S-curve. The rate of increase of the number of users of a new technology is initially slow, before rising at an increasing rate and then reaching a plateau.

Figure 11: The 'S-curve'



Source: London Economics

Perhaps the most interesting feature of this shape is the initial region, A, in which the number of users of the technology remains small for a long period of time. This is because it gives rise to the following question: if a new technology really is a significant improvement over existing technologies, why do some firms shift over to it more slowly than other firms?

### 3.5.2 Models of technology adoption

Theoretically, there exist two key rationales for the S-curve: the learning model and the heterogeneity model. The learning model views firms' adoption choices as a result of becoming aware of the new technology. While the heterogeneity model adds that firms' adoption decisions are also based on firm characteristics such as having the skilled workforce to implement the technology and market conditions such as competition levels.

#### *The learning model*

The first is known as the "learning model" and is based on the simple premise that some firms (early adopters) discover the new technology before other firms. Over time, firms that have not adopted the technology discover information about it from early adopters (e.g. via observation) and this leads to progressively more firms adopting the technology per time period. However, eventually the market becomes saturated and the rate of adoption decreases again (Hall and Khan, 2003). This yields an S-curve and does not make any assumptions about firms other than assuming that the timing with which they discover the technology differs. In this model, deployment rates will be higher if:

- technologies are easily learned/knowledge is easily transmitted;
- the presence of early adopters influences the behaviour of other firms, i.e., there are "spillovers"; and

- the new technology is superior to the old technology, and there are no switching costs.

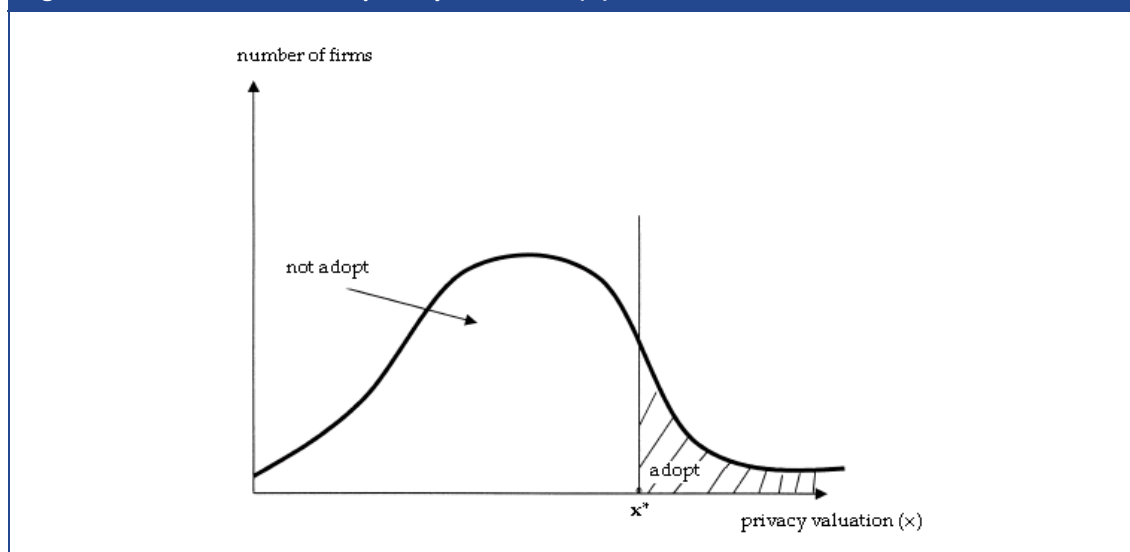
### The heterogeneity model

The second rationale for the S-curve is known as the heterogeneity model. This model is interesting because, rather than assuming all firms value the new technology equally and different adoption times are determined by when data controllers learn about a technology, it explicitly accounts for the possibility that different firms (e.g. large firms versus SMEs) will value the new technology differently.

The heterogeneity model yields an S-curve because of the following line of reasoning: firms have different privacy valuations,  $x$ , which are driven by the profitability of adopting the PET. The higher a data controller estimates the economic benefit of a certain PET, the higher its  $x$ .

These differences in privacy valuations between firms can be expressed as a distribution presented in Figure 12 below. The normal distribution suggests that some firms have very high privacy valuations (such as banks and social networking sites) whereas the majority have lower privacy valuations and a few companies do not consider privacy issues at all.

Figure 12: Distribution of firm privacy valuations ( $x_i$ )



Source: Geroski (2000)

When a technology is first introduced, it will be adopted by all firms who value it highly enough (i.e., those with a valuation  $x > x^*$ ). This is indicated by the shaded region in Figure 12. Adoption rates increase as  $x^*$  shifts to the left, i.e. as the technology becomes more attractive to companies with lower privacy valuations. This might occur because the technology is becoming cheaper over time (e.g. because economies of scale in production) or because the reliability of the technology improves as it becomes more mature, etc. If  $x^*$  falls constantly over time the normal distribution of valuations will yield an S-curve as in Figure 11.

The value of the heterogeneity model is the ability to relate differing technology valuations to firm characteristics. For instance, one might need to examine whether smaller firms are less likely to adopt new a technology because they are:

- less likely to use the technology intensively and therefore do not benefit fully from it (i.e. larger firms benefit from economies of scale);
- more credit-constrained, making it difficult to invest in new technology;
- more risk averse in terms of experimenting with new technologies; and
- less capable (e.g. as they employ less technical staff).

These hypotheses are supported by theoretical work in the area of technology adoption. Nelson and Winter (1982), for instance, show that larger firms are in a better position to appropriate the returns from innovation and do not face the same financial constraints as smaller firms in their adoption decision. Empirically, many studies that have studied other technologies have shown that smaller firms are slower to adopt new technologies.<sup>58</sup> In the context of PETs, there are many good reasons to believe that SMEs are less likely to adopt PETs than their larger counterparts.

### 3.6 Summary

In this chapter we discussed the factors that determine the deployment level of PETs. It shows clearly that the deployment decision is multi-faceted and contingent on external factors (e.g. the legal and regulatory environment, deep-rooted behavioural biases) as well as the real costs and benefits of PETs in specific applications.

A few of the factors apply to both individuals and data controllers. A fundamental driver of PETs deployment is the fear of privacy breaches which result in damage, both economic and intangible. PETs deployment consequently depends on:

- **The level of risk:** this can be derived from statistics on the incidence of data loss and the associated damage. To our knowledge, no convincing overall assessment of the risk associated with disclosure of personal data exists. Snippets of the necessary data (e.g. the number of records lost in data breaches<sup>59</sup>) are available from various sources. However, the risks are application specific: the theft of bank details is likely to be more damaging than the theft of information that can only be exploited after further processing, for example by being combined with other records to perform data mining. And in many instances they are likely to be specific to individuals as well: how much a potential perpetrator of identity fraud can learn about a prospective victim depends on how much personal data that person has disclosed in the past. Moreover, individuals differ in their valuation of the intangible losses associated with the invasion of their privacy.

<sup>58</sup> David (1969), Romeo (1975), Davies (1979), Hannan and McDowell (1984), Levin et al. (1987), Rose and Joskow (1990), Pennings and Harianto (1992), Ingham and Thompson (1993) and Karshenas and Stoneman (1993) all report positive correlations between firm size and the speed of adoption.

<sup>59</sup> Examples can be found here: <http://datalossdb.org/>.

- **The efficacy of PETs in reducing the risk of data loss:** this determines to what extent PETs, including organisational arrangements, greater economy with personal data, etc., reduce the risk of data loss. To an extent, this will vary with different types of PETs. While the most sophisticated PETs aim to minimise the scope for human error by reducing the need for personal data, many of the PETs at the lower end of the spectrum (the most widespread type), can be ineffective against human error. PETs that are designed to inform users about privacy risks, such as P3P, are a special category that protect users only insofar as they are willing to act on the information. In principle, evidence from experiments or observations from case studies can be used to determine the efficacy of PETs.<sup>60</sup>
- **The demand response to increased PETs deployment:** with informed consumers, this is a function of consumers' risk aversion, the risk of data loss, and the efficacy of PETs in reducing it. Again, it can be observed in case studies or experiments. At the moment, the evidence on demand response is weak. Surveys indicate relatively high levels of concern about privacy in online settings and research has shown that consumers are willing to pay a premium for privacy under certain conditions.<sup>61</sup> However, stakeholders that were consulted for the present study attest to a widespread indifference on the part of individuals when it comes to actual buying decisions and there is also evidence from experimental studies that support this view.<sup>62</sup>
- **Awareness of PETs:** PETs will only be used if deployers are aware of them. Survey evidence suggests that awareness is far from universal, although some PETs are much better known than others.
- **The prevailing liability regime:** whether data controllers have an incentive to deploy PETs depends to some extent on who is liable in case data is lost or stolen. Data controller liability increases the attractiveness of PETs, as economies of scale mean that large organisations can expect greater economic benefits.

Using information on the above parameters allows a high-level reproduction of the individually rational decisions on PETs deployment (in situations where deployment is voluntary) based on the expected costs of not deploying PETs. Stakeholders, especially data protection authorities, see these costs (both direct costs due to fraud, as well as lost business and lower growth) as a very important argument for increased investment in PETs.

The prevailing view among data protection authorities is that privacy protection in general and PETs deployment in particular, is often insufficient. One widespread explanation for the insufficient demand is the perceived irrationality of individuals when undertaking transactions that might impact on their privacy.

According to this view, individuals underestimate the risk associated with the disclosure and thus reveal too much personal data. Behavioural economics has identified various *behavioural biases* that can explain this. The most important one relates to the weak link between actions (the

---

<sup>60</sup> See Borking (2009), p.6.

<sup>61</sup> See Tsai et al. (2007).

<sup>62</sup> Examples are Hui et al. (2006) and Berendt et al. (2005).



disclosure of personal data) and consequences (e.g., nuisance mail, fraud, theft, profiling etc.) This lack of feedback also prevents individuals from learning to be careful about their privacy in the future.

Empirical evidence also suggests that the cost of reputation loss (in terms of stock market impact) following incidents of data loss is relatively low and dissipates quickly. A lack of technical literacy and awareness of the value of personal information also contribute to the possibility that risk perceptions are not in tune with the true risk picture. PETs that rely on human input to function, even if they are deployed, may be rendered ineffective if individuals lack the incentives and the knowledge to use them properly. This danger is aggravated by the fact that deep-rooted behavioural patterns are difficult to overcome simply by providing more information. Other PETs, especially those aimed at data minimisation, are effective irrespective of whether individuals' risk perceptions are accurate or not.

In this situation, data controllers can exploit the information asymmetry that exists between them and the individuals who entrust them with their personal data. The second part of this Section therefore focuses on data controllers' incentives to deploy PETs, specifically on the economic benefits of deployment.

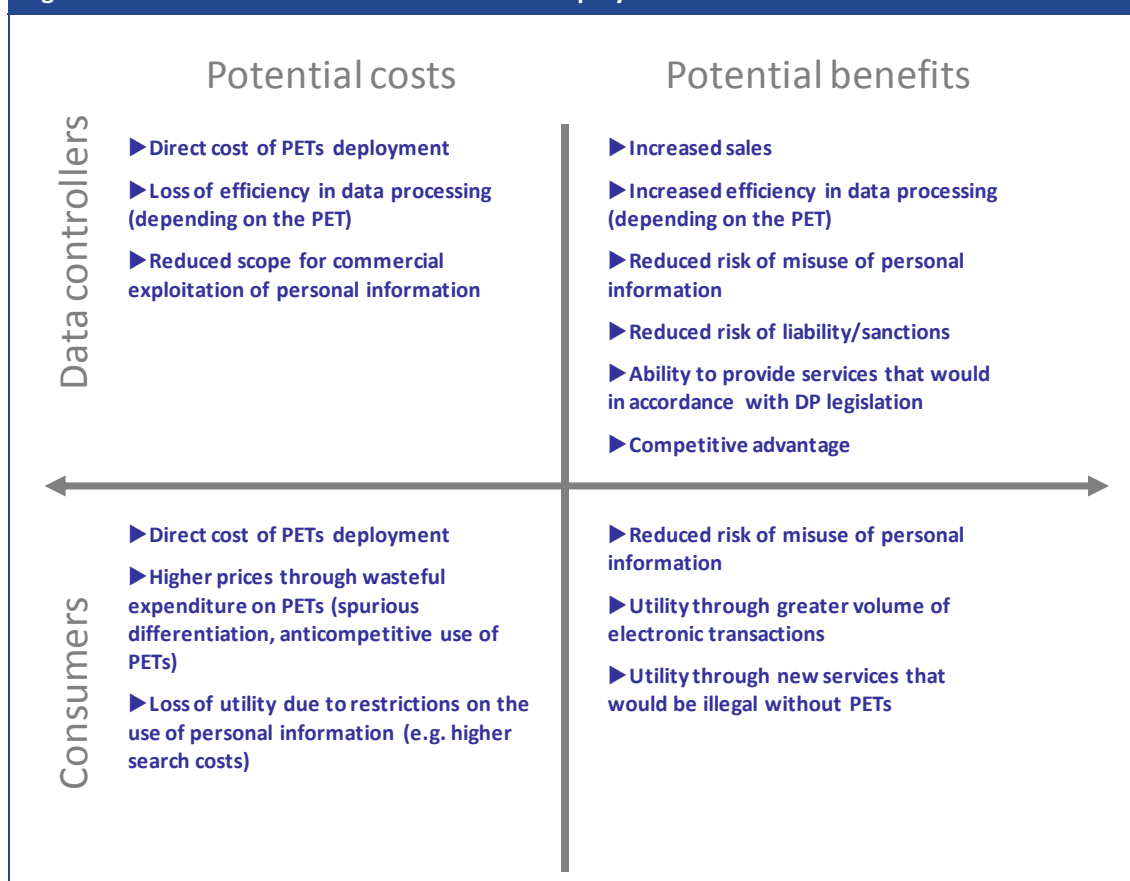
As we have seen, data controllers' deployment decision is determined by many of the same factors that shape the demand by individuals, including the fear of data loss, which in the case of data controllers can involve data on employees, suppliers, customers, etc. However, data controllers also benefit from the electronic processing of personal data. The main sources of benefit are greater efficiency in carrying out processes electronically; personalising goods and services; and exploiting personal data in the production of new goods and services.

A further benefit specific to data controllers is competitive advantage through PETs. The assumption is that good privacy protection can serve as a unique selling point as customers flock to the provider with the best PETs. There is little evidence that this is true in the consumer market, but competition as a driver of PETs deployment seems to play an important role in the business-to-business market.

Overall, this means (assuming that PETs deployment is to some degree discretionary) that PETs may involve a trade-off for data controllers: the availability of personal data as an economic resource can create benefits for data controllers, the individuals who supply the data, and, at least in some cases, the wider public. Using PETs might reduce these benefits. Deploying PETs requires upfront investments in the technology, as well as training and ongoing maintenance. Even though the use of PETs can reduce costs over time, the direct costs of deployment are the most immediate type of costs that has to be weighed against the potential benefits. The cost of PETs to data controllers increases if they make the processing of personal data more difficult, or using them requires a more fundamental redesign of business processes. Finally, a reduction in data controllers' ability to exploit personal data can represent a cost, depending on the value the personal data has for the data controller.

On the basis of the preceding considerations, it is possible to derive a high-level summary of the potential costs and benefits associated with PETs deployment. This is shown in Figure 13 below. A simple comparison of costs and benefits will reveal whether PETs deployment is an economically sensible decision for data controllers and consumers.

Figure 13: Potential costs and benefits of PETs deployment



Source: London Economics

However, it should be remembered that market imperfections (asymmetric information, externalities, lack of information sharing, underinvestment) mean that the individually rational decisions of data controllers do not necessarily lead to the socially optimal level of PETs deployment.

As mentioned previously, the incentive structures are also shaped by the legal framework that governs the use of personal data. In particular, this consists of privacy legislation that prescribes the way in which personal data can be used, which can make the use of PETs compulsory; and of the liability regime that determines which party – data controllers or individuals – is responsible in case of damage as a result of the misuse of personal information.

Finally, it should be remembered that PETs are relatively new technologies. With such technologies, it is to be expected that deployment levels are initially low. Deployment rates then pick up as information about the technologies is disseminated and uncertainty recedes. This leads to an S-shaped deployment rate, which could help to explain that many PETs are currently not used as widely as could be expected when considering their usefulness in the abstract.

From an economic point of view, for the data controllers PETs are not useful *per se*. Their usefulness instead depends on the ways in which they help the production of goods and services,

their effectiveness in averting economic damage, and the competitive advantage they impart. Only if a PET effectively fulfils at least one of these functions, and is the most cost-effective way of doing so, will businesses consider investing in its deployment. Even then, PETs might not be deployed immediately owing to the uncertainty about the benefits of a new technology.<sup>63</sup>

At the same time, the use of personal data by businesses and government is a source of benefits. Only PETs that allow the realisation of these benefits, and whose cost are not so high as to cancel out the incentive to deploy them, will be deployed voluntarily.

It is also important to note that the benefits and costs are unequally distributed between low and high-end PETs. PETs that allow the provision of services in accordance with data protection legislation that could otherwise not be lawfully offered are the most unambiguously beneficial.

Given the partial misalignment of the incentives to deploy PETs between individuals and data controllers, PETs may have a specific role in rebalancing the market for personal data in favour of consumers, who are currently at a disadvantage due to information asymmetries. PETs that provide enhanced transparency about the way data is used (including by whom and for what) and the value of PETs as an economic resource to data controllers can empower consumers vis-à-vis data controllers without diminishing the utility of personal data (from which data controllers and individuals can both benefit).<sup>64</sup>

---

<sup>63</sup> Hall and Khan (2003).

<sup>64</sup> This might lead to an increase in the – often implicit – price that data controllers pay for personal data, but potentially also to more rather than less disclosure (individuals are more likely to ‘sell’ at a higher price). Whether data controllers see this as an incentive to deploy PETs depends on how the benefits from having more data compare with the cost of the PET plus the added cost of the data (assuming the data could have been collected lawfully without it).

## 4 Stakeholders' views

In the late summer of 2009, we carried out a stakeholder consultation exercise across the twelve selected Member States. The consultation sought information on three specific points:

- risks to privacy and the state of data protection;
- the economic and non-economic benefits of PETs; and
- the country-specific empirical evidence, including notable examples and cases, on data protection and PETs.

In this section, we summarise the information we received on the first two points. The information collected on the evidence available in the Member States was used to inform the subsequent parts of the study, in particular by identifying data sources and candidates for detailed case studies.

The responses we received were mostly qualitative in nature, and showed variation in the level of detail, but were very useful in providing an overview of the privacy situation in each Member State and the thinking on PETs by professionals involved in the field.

To gain a deeper understanding of the experiences, attitudes and policies regarding PETs in different Member States, we first canvassed the public bodies charged with overseeing data protection issues in each of the twelve Member States. A semi-structured interview questionnaire<sup>65</sup>, agreed upon between the EC DG Justice, Freedom and Security and London Economics was used to collect information from the relevant stakeholders via either telephone interviews or written responses. We obtained responses from each of the data protection authorities in 12 Member States (see Table 1 on p. 4).

In parallel to the consultation exercise with national data protection authorities, a second consultation exercise was conducted with business and consumer associations to gauge how firms and consumers view the issues of privacy and PETs. A total of thirteen responses were received from stakeholders, comprising eight survey responses from consumer associations and five responses from business associations (see Table 1, as above). The results of the consultation exercise represent the views of respondents from:

- the Czech Republic (consumer association);
- Denmark (consumer and business association);
- Germany (2 consumer associations and business association);
- Spain (consumer and business association);
- Italy (consumer and business association);
- Hungary (consumer and business association);
- Austria (consumer association); and

---

<sup>65</sup> The interview tool is presented in Annex 2.

- the United Kingdom (consumer association).

A further international business association, the association of records and information services management companies (PRISM International), contacted us of their own accord and submitted a statement on behalf of its members.

The following sub-sections present the stakeholders' views on the risks to privacy, including individuals' awareness of the risks associated with disclosing personal data, and the state of data protection and the role of PETs, including economic and non-economic benefits.

## 4.1 Risks to privacy and the state of data protection

### 4.1.1 Perceived risks

National data protection authorities perceive a large increase in the risks to privacy and personal data associated with online activity, with some characterising the risk as growing at a speed commensurate with the take-up rate of new technologies and online services.

The national data protection authorities see the proliferation of social networking sites as one of the main drivers of risk to privacy online. This goes hand-in-hand with an increasing willingness of individuals to disclose personal information online, where it is open to misuse. For instance, the increase in the volume of personal photographs and videos was identified as a specific danger by the data protection authorities in Malta and Austria.

Outright data theft and identity fraud are significant concerns, but the risks are wider and include unauthorised (although not criminal) use of data by businesses.

The Austrian authority specifically identified a propensity on the part of businesses to collect and store large amounts of data without a specific reason. This is made possible by the rapid decline in the cost of electronic data storage and is driven by the realisation that personal data represents an economic resource that might be exploited.

In addition to the scenario of simply storing information, a number of authorities indicated that there is an increasing threat associated with data mining, where the combination of information contained in a number of separate databases can yield detailed profiles of individuals even if the full data is not available in any single database.

The exploitation of personal information by business represents the flipside of a wider trend away from pseudonymous/anonymous online activities, which might be seen as an outcome of the commercialisation of the Internet.

Business and consumer associations expressed the view that the market for personal information is thriving with information having significant value for advertisers and fraudsters alike. With an increase in the capability and capacity to handle and store large volumes of information, particularly electronically, the risks are considered to be ever present.

One problem is that even anonymised information can often be combined with other online information to identify the individual. This issue is especially prevalent when considering social

networking sites. Much of this information is provided by consumers voluntarily; however, there are circumstances where individuals cannot access services without providing information online.

This requirement to provide information results in personal information becoming available to third parties in perpetuity and allows some organisations to potentially screen their customers according to their personal characteristics or perceived risk. There have been concerns that this activity has been prevalent in the financial services and insurance industries in particular.

In relation to the wider economic and non-economic outcomes associated with the increased threat to personal information, the Spanish data protection authority considered that there was a substantial danger that unfettered exploitation of personal data has the potential to undermine consumer confidence in online services, such as e-commerce.

Many of the perceived threats or risks to privacy identified by the national data protection authorities related to the private sector use of information and the increased volume of sensitive information that was being shared electronically. Although public sector data losses are highly publicised and potentially damaging, relatively few authorities mentioned the primary risks to privacy being as a result of data loss – especially in the case of public authorities. However, leakage from public/government databases was specifically mentioned by the Estonian authority, with a lack of technical security measures mentioned as a specific risk only by the German and British authorities (both public and private sector).

Although the majority of the information collected as part of the consultation exercise was qualitative, the survey also included some closed response questions to gauge the perceptions of the national data protection authorities, business associations and consumer associations.

In Figure 14, we present information on the extent to which the various stakeholder groups considered the risks to privacy and the protection of personal data associated with online activity to be increasing. The respondents were asked to consider the extent to which risks associated with online activity were increasing on a scale of 1 to 5, where 1 represented to *no significant extent* and 5 represents to a *very significant extent*. There was little difference in response between the various stakeholder groups but it is interesting to note that all national data protection authorities (bar one) considered risks to be increasing to a significant or very significant extent.

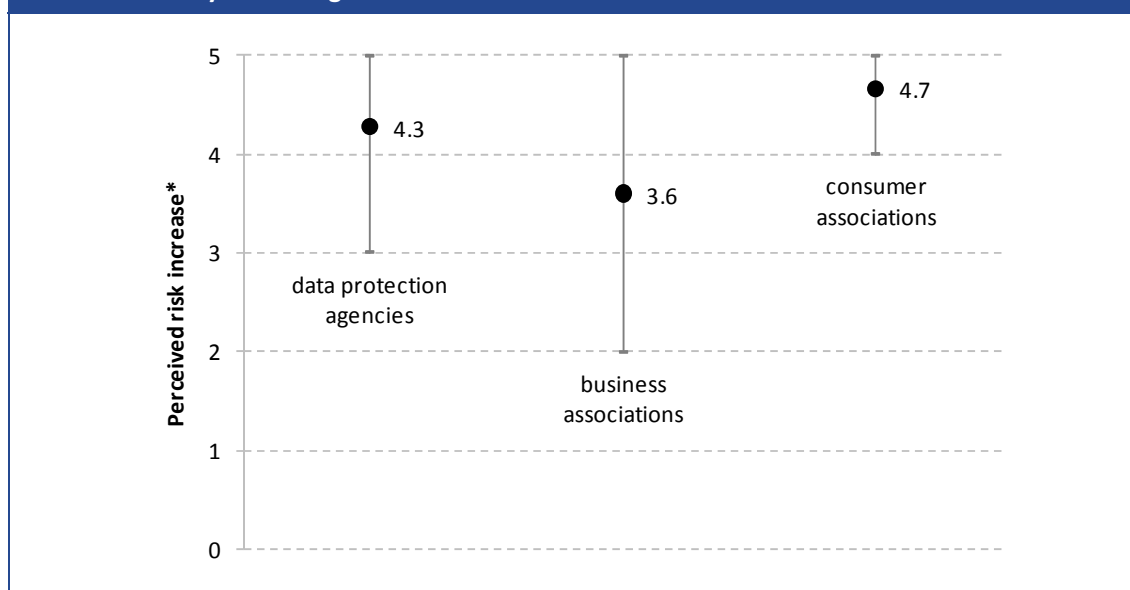
On average, consumer and business association agree that risks are “increasing”. It is interesting to note that of the six consumer associations providing an answer, four perceived the risks to be “increasing significantly”, while the remaining two consumer associations considered the risks to be ‘increasing’. While the business associations also assessed in general that the risks associated with online privacy were increasing, only one of the respondents indicated that they felt the risks to be increasing significantly. Consumer associations were of the opinion that the risks associated with online transmission of information were greater than even national data protection authorities.

More specifically, the types of risks identified by the national consumer and business associations generally involved the following:

- lack of consumer consent and control on how their personal information is used;

- potential secondary use of personal data through data sharing (and without consumer permission);
- identity theft and fraud;
- potential discrimination of consumers that are in some way disadvantaged, e.g., in financial or insurance services;
- people forced to consent to various uses of their data in order to access services (e.g., use of their data for marketing purposes);
- easy export of data to third countries where the data protection laws or enforcement may be weaker;
- use of vast databases particularly in government services which are prone to data breaches and unauthorised cross-sharing of information;
- people not understanding the technologies and the risks associated with them; and
- new developments, such as “cloud computing”, posing additional risks, since the space for personal data and applications may be operated by lots of different sub-contractors.

**Figure 14: Are the risks to privacy and the protection of personal data associated with online activity increasing?**



Note: \* 1 = 'no significant increase' to 5 = 'very significant increase'; mean response (•) and range (I) by stakeholder group across Member States.

Source: London Economics

#### 4.1.2 Consumer awareness

The general view of national data protection authorities is that consumer awareness of the risks surrounding the use of personal information online is increasing, but is still at a relatively low level. The Maltese and Dutch data protection authorities highlighted the important role played by public

bodies in raising awareness, while other authorities mentioned the effect of high-profile incidents in relation to the loss of personal data.

An important issue put forward by the Irish authority is that, while awareness is increasing, consumers in general do not seem to be exercising choice on the basis of privacy concerns. There is a vocal minority that do so. But, until demand responses to privacy risk becomes more prevalent, there will be an inherent lack of incentive for many businesses to place a focus on privacy or to incorporate the protection of personal information into their business models.

However, the Irish data protection authority considers that large multinational businesses take privacy issues very seriously given media interest and the perceived reputational risks associated with data losses or misuse.

A further issue raised by the Netherlands and United Kingdom authorities is the superficial nature of consumers' understanding of the nature of data protection risks. There is concern that consumers worry excessively about identity fraud, which receives a large amount of media attention, rather than other types of misuse.

Business and consumer associations both identified a lack of consumer awareness as an important source of privacy risk. One respondent highlighted that consumers might see exposure to privacy risk as a necessary cost associated with online data transmission. For example, they assign such a low probability to ever being a victim of identity theft that they see the possibility as an acceptable risk to take. This fits in with the view of another respondent that stressed that consumers sometimes transfer their personal information online because access to some online services is contingent on it.

One respondent indicated that general awareness amongst consumers was low. It is a particular issue amongst young people, who appear to be substantially more liberal with the information that they shared online. This respondent suggested this was a simple characteristic of youth, but that there was a role for policy-makers to make young people more aware of the risks associated with online activity.

However, the same respondent indicated that, although consumers signal that they, in some respects, tolerate some degree of uncertainty or risk in relation to the use of the information they provide online, it is also the case that they are not aware that technological solutions were readily available that could be employed to instantaneously eliminate many of the problems associated with the transmission of personal information. One interesting point made by a German consumer association was that

*"businesses see security as a cost rather than a competitive advantage; consumers are often not aware that their data has value and is often used as an 'alternative currency'".*

As such, the respondent indicated that there is no incentive either to introduce additional security, nor is there any incentive to dispel consumer ignorance.

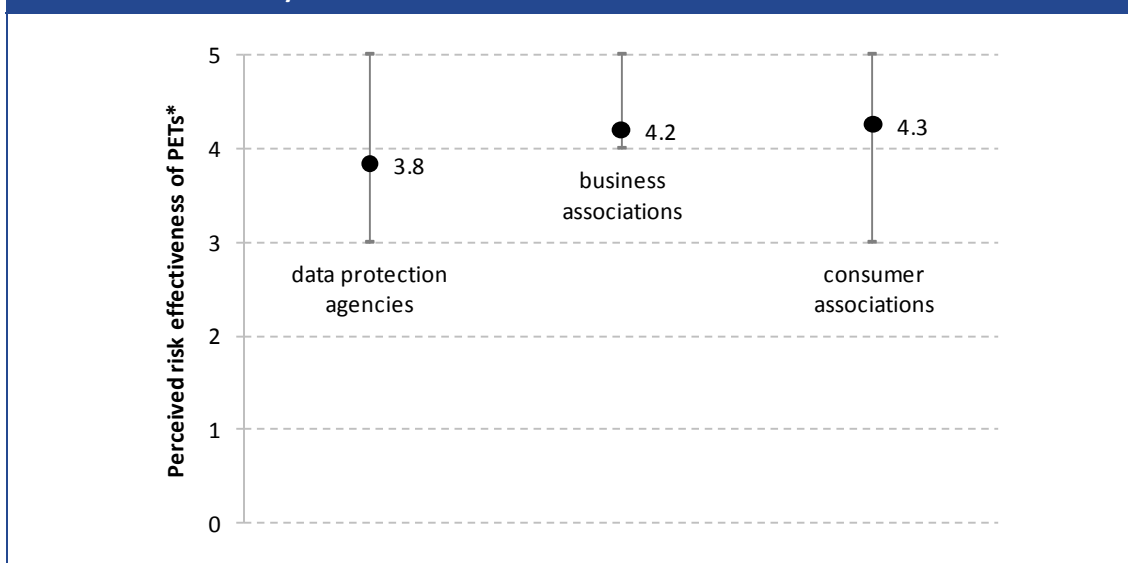


## 4.2 The role of PETs

### 4.2.1 Effectiveness of PETs

Data protection authorities are relatively optimistic about the ability of PETs to reduce the identified risks associated with online activity. In Figure 15, we present information on whether the various stakeholder groups think that the deployment of PETs is an effective means for minimising the risks to privacy and protecting personal data associated with online activity. Again, using a scale from 1 to 5, where 1 implies 'not at all effective' and 5 implies 'very effective', data protection authorities considered the deployment of PETs to be relatively effective (3.83) – though relatively less effective compared to the business and consumer associations.

**Figure 15: Is the deployment of PETs an effective means of minimising the risks associated with online activity?**



Note: \* 1 = 'not at all effective' to 5 = 'very effective'; mean response (•) and range (I) by stakeholder group across Member States.

Source: London Economics

Probably most interestingly, the Austrian Data Protection Authority indicated there is no universal answer in relation to the effectiveness of PETs in reducing online risks to personal information. An important factor for the appropriateness of PETs (and the selection of the appropriate PETs) is the origin of the security threat. Simple PETs such as firewalls might offer a good protection against threats of data theft from outsiders, but might have no effect on threats from personnel working for the data controller. However, PETs that minimise the amount of personal data that is collected, stored and processed by the data controller can offer protection against this kind of insider threat.

Among business and consumer associations, there was general agreement that PETs play an important role in reducing the privacy risks that data providers face. All but one of the business and consumer associations (Czech Republic) responding to this question saw PETs as either "effective" or "highly effective" and there was no difference on average between the consumer and business associations in relation to their perception of the effectiveness of PETs.

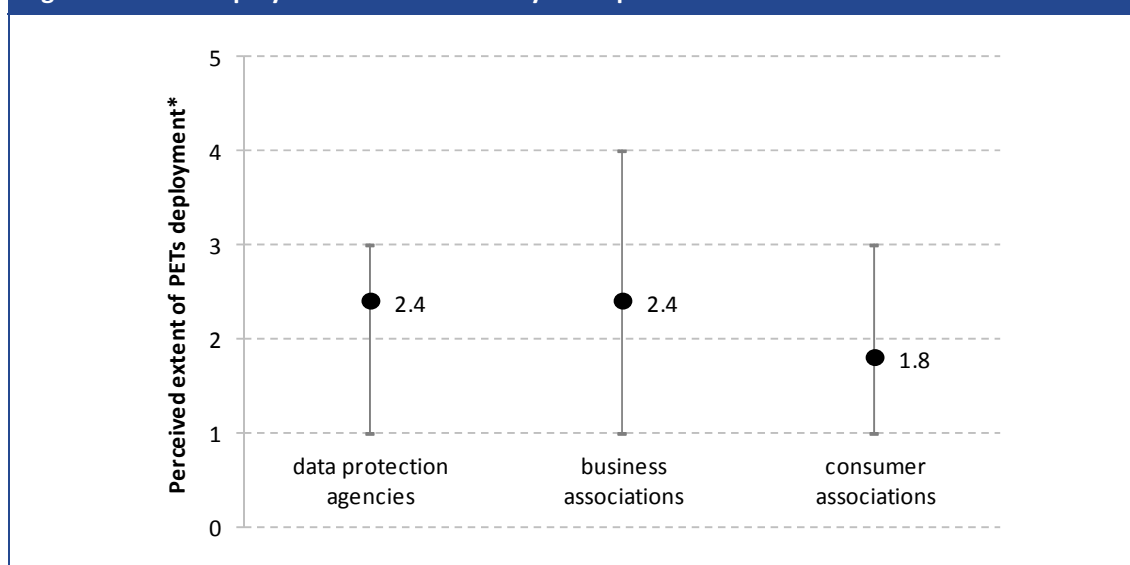
It is interesting to note that both business and consumer associations believe that the effectiveness of PETs is greater than that suggested by the national data protection authorities. This may in part reflect the better understanding of the accelerating risks to privacy that the data protection authorities are becoming increasingly aware of.

However, it is also the case that consumer and business associations consider the deployment of PETs to be much less widespread than national data protection authorities and this difference in views may account for the slightly divergent opinions across stakeholder groups (see Figure 15).

#### 4.2.2 Current level of PETs deployment

From the perspective of stakeholders, the picture is less positive when it comes to estimating the current levels of PET deployment. There was general agreement that privacy enhancing technologies were not widely deployed and the rate at which deployment has grown over the last few years has not been substantial (according to the Danish and Italian business association and the UK, Danish, Italian and Czech consumer associations). This is surprising given the belief that privacy risks have been growing and that PETs are effective at reducing privacy risks (eight out of eleven respondents held these views).

**Figure 16: Is the deployment of PETs currently widespread?**



Note: \* 1 = 'not at all widespread' to 5 = 'very widespread'; mean response (•) and range (I) by stakeholder group across Member States.

Source: London Economics

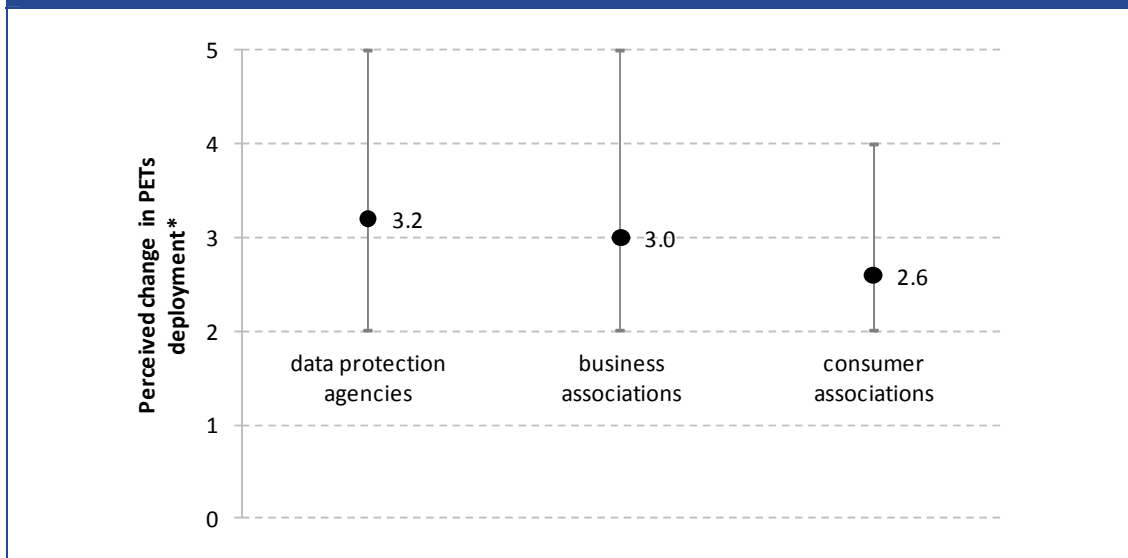
More specifically, the German data protection authority estimates that around 50% of the relevant services and applications are protected by PETs. According to the authorities in the United Kingdom, Malta and Hungary, there are particularly low levels of PET penetration in these three countries.

In Figure 17 below, we present information on the extent to which the stakeholder groups consider whether there has been an increase in the deployment of PETs over the last 5 years. There is no consensus within each group of stakeholders about trends in the rate of PETs adoption.

In particular, the Irish, Estonian and Maltese data protection authorities consider that there has been a relatively extensive increase in the deployment of PETs, while the German, Danish and United Kingdom authorities see no increase.

Consumer associations take the most pessimistic view of the spread of PETs over the last five years, with an average response score of 2.6. Although the picture is relatively inconclusive, on balance, increases in PETs deployment are seen as moderate by stakeholders.

**Figure 17: Has the deployment of PETs changed significantly over the past 5 years?**



Note: \* 1 = 'no significant change' to 5 = 'very significant change'; mean response (•) and range (I) by stakeholder group across Member States.

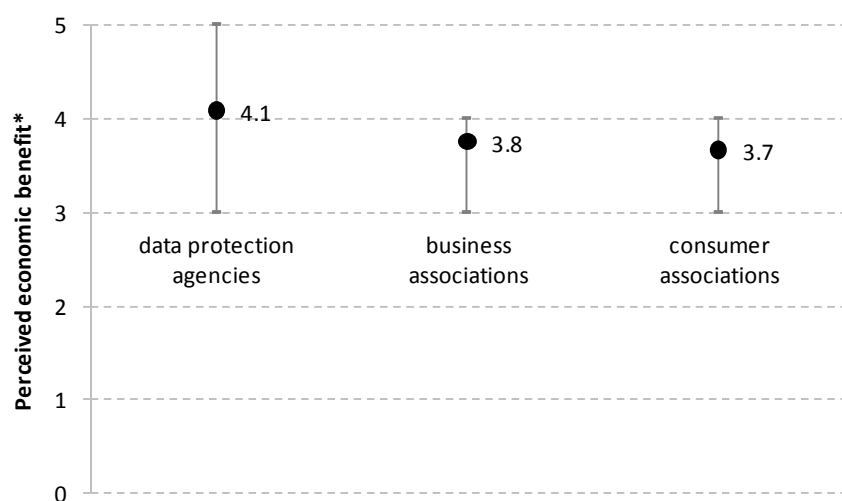
Source: London Economics

### 4.2.3 Economic benefits of PETs

In this sub-section, we consider the assessment of stakeholders of the economic and non-economic benefits that might be associated with the deployment of PETs. As presented in Figure 18, the national data protection authorities view PETs as a source of significant economic and non-economic benefits.

In particular, in relation to the economic benefits to data controllers that might be generated through the further deployment of PETs, most data protection authorities indicated that the economic benefits were very high (Austria, Germany, Malta and Spain) while Ireland, Estonia and Hungary indicated that the economic benefits were high. No national data protection authorities thought that the economic benefits would not be significant.

**Figure 18: To what extent could the deployment of PETs yield economic benefits to data controllers?**



Note: \* 1 = 'very insignificant benefits' to 5 = 'very significant benefits'; mean response (•) and range (I) by stakeholder group across Member States.

Source: London Economics

There was a belief among consumer and business associations that it is possible for data controllers to derive at least “moderate” if not “significant” economic benefits as a result of PET deployment as shown in Figure 18. The principal channel through which data controllers might derive these benefits was identified by stakeholders as “trust”-related or reputational effects.

Compared with the consumer and business associations, national data protection authorities see a slightly higher potential for economic benefits. Three national agencies (Germany, Austria and Malta) see the potential for ‘very significant’ benefits, a view not shared by any business or consumer associations.

A number of respondents also mentioned that they believed that, with the increased deployment of PETs, more customers might shift away from using traditional channels to complete transactions (such as conventional stores), which might result in significant cost savings for businesses. Additionally, security achieved through the use of PETs was identified as a benefit to firms insofar as any costs incurred through data breaches would now be reduced (for example, compliance costs associated with data protection laws would be avoided). One issue that we will consider in a later section relates to the use of sanctions.

There was a belief amongst some stakeholders that, although there may be significant economic and non-economic (or short term and long term) benefits associated with the deployment of PETs, the initial fixed and operating costs act as an immediate disincentive to their deployment. Some respondents indicated the better use of sanctions would act as a deterrent against the misuse of data but might also act a lever or trigger for deployment and realisation of as yet untapped benefits.

The data protection authorities identified a number of specific benefits. Several stress the importance of PETs for corporate image and consumer trust, which contribute to customer loyalty and increased sales. Equally, better control over data stored by an organisation reduces exposure to risk of data loss, with the attendant risk of costly legal disputes, fines and lasting reputational damage.

An interesting point is made by the United Kingdom Information Commissioner's Office in relation to the costs that might be associated with storing personal information: specifically that not storing information reduces the cost that would otherwise be incurred to safeguard it. In a similar vein, the Dutch authority points out that certain simple PETs, like the anonymisation of datasets eliminate the need for more intricate PETs necessary to secure access and transmission of non-anonymised data.

A potentially important benefit identified by the Estonian authority was that better quality of data could be secured through the use of PETs that might have positive knock-on effects on research- and development-based personal data.

On a broader level, a climate of trust and security was seen as beneficial for the further development of online services, including e-government applications. While the authorities maintain that businesses and organisations across the board can benefit from deploying PETs, most see the benefits as concentrated in public sector organisations and large businesses (one authority specifically mentions the finance and telecommunications sector).

An important reason for this is that consumers have higher trust in, or expectations of, these organisations, which consequently have more to lose from data loss or misuse. Moreover, such organisations are more likely to collect, store and use large volumes of personal information, so that the problem for them is more acute.

Finally, organisations might be able to use PETs as a competitive tool, for example by promoting themselves on the basis of data security, which they can do more easily/convincingly than smaller organisations (although as will be discussed in the next section, this was not seen as enough of an incentive for organisations to deploy PETs given the expected costs associated with deployment). In this context, the Hungarian authority raises the point that trust can prevent customers switching to other service providers.

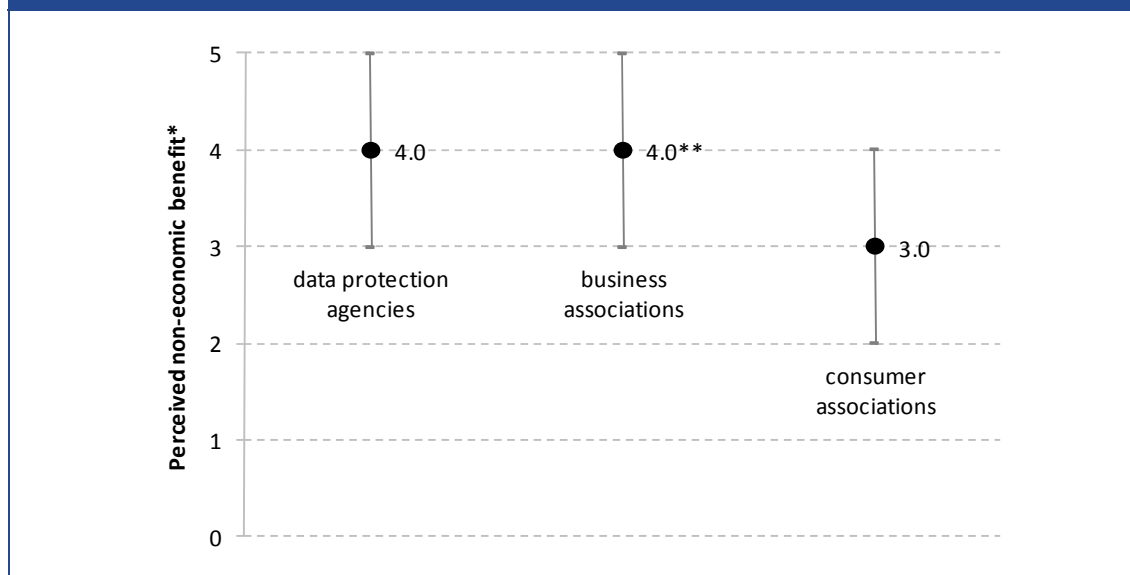
This highlights not only how PET deployment varies by sector, but also that such deployment can have knock-on effects on competition, which need to be taken into account in the assessment of overall costs and benefits.

#### 4.2.4 Non-economic benefits of PETs

Stakeholders were asked to consider the extent of the non-economic benefits that might be associated with the deployment of PETs. On average, all three stakeholder consultation groups assessed the non-economic benefits to be more significant than the economic benefits. In particular, the average rating of the extent of non-economic benefits by the data protection authorities was 4.2 compared to 4.0 for the economic benefits. Similarly, the business associations rated the non-economic benefits to be highly extensive (5.0) compared to a rating of 3.8 in

relation to the economic benefits. Similarly, the consumer associations considered the non-economic benefits to be significant (4.0) compared to a rating of 3.7 for the economic benefits.

**Figure 19: To what extent could the deployment of PETs yield non-economic benefits to data controllers?**



Note: \* 1 = 'very insignificant benefits' to 5 = 'very significant benefits'; mean response (•) and range (I) by stakeholder group across Member States. \*\* Only 2 observations available.

Source: London Economics

In terms of the types of non-economic benefits associated with the deployment of PETs, there was some overlap with the types of economic benefit. In particular, a number of authorities mentioned the reputational gain that might be associated with enhanced privacy protection through the deployment of PETs. They indicated that, although there may be short-term costs with few tangible benefits, the longer-term impact on the business as a result of reputational gains would be significant.

The stakeholder views on non-economic benefits raise an important conceptual issue: non-economic (e.g., enhanced privacy leading to greater consumer confidence in electronic transactions) can over time turn into economic benefits for data controllers (e.g., increased sales). This may suggest that it is crucial to ensure that any discussion around the deployment of PETs adopts a suitably long time frame for the assessment of the associated costs and benefits.

Otherwise, a clear distinction between economic and non-economic costs has far-reaching policy implications, as the weighing-up of economic and non-economic costs and benefits is likely to be contentious.

#### 4.2.5 Factors limiting the deployment of PETs

As discussed in the previous sections, there is some evidence (especially from the UK ICO) indicating that there is a disjoint between the stated preferences of consumers in relation to data protection issues and the actual behaviour of consumers when faced with decisions relating to

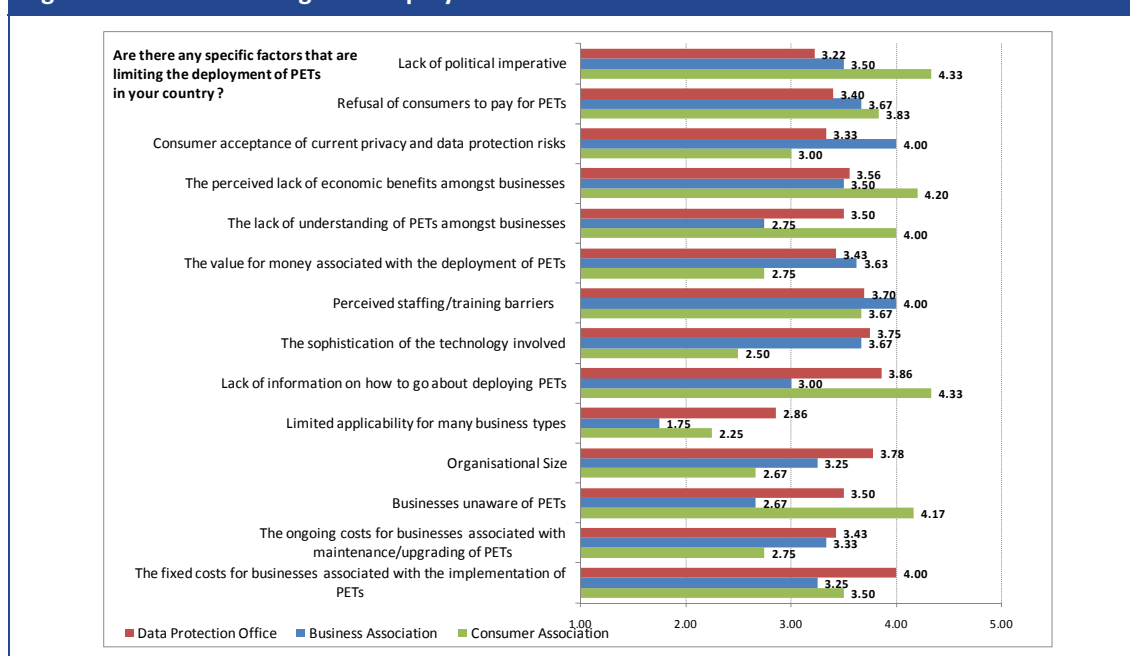
protecting the privacy. The previous section also noted that national data protection authorities, business associations and consumer associations are of the view that, in general, there are significant economic and non-economic benefits associated with the deployment of PETs. The question remains as to what deters businesses from deploying PETs.

In Figure 20, we present some additional information on the factors that limit the deployment of PETs. From the perspective of the national data protection authorities, the chart shows that the fixed costs of PETs are seen by the data protection authorities as the most important factor limiting PETs adoption. This view is not shared by business associations, who instead blame a lack of political imperative, and a lack of organisational know-how.

In addition to the issues in relation to the fixed costs associated with the deployment of PETs, data protection authorities also indicate that a lack of information in relation to how to go about incorporating and deploying PETs into interactions with other businesses and consumers, as well as issues relating to the size (and expertise) of many organisations, limit the deployment of PETs.

Interestingly, there was some significant variation across the national data authorities' perception of the perceived lack of benefits to businesses. In particular, the German and Austrian authorities were of the opinion that the fact that businesses were unaware of the economic benefits associated with the deployment of PETs was a significant barrier to the further deployment of PETs, whereas the Maltese data protection authority indicated that this was not the case.

**Figure 20: Factors limiting PETs deployment**



Source: London Economics

The survey also gathered information from the national data protection authorities on the perceived preference and behaviour of consumers. In particular, when queried whether consumer acceptance of current privacy and data protection risks is acting as a disincentive for firms to deploy PETs, the Estonian and Austrian authorities responded that this was either significant or

highly significant with only the German data protection authority indicating consumer lethargy as being insignificant.

When asked whether the possibility that consumer refusal to pay for PETs to protect personal information acted as a barrier for the further deployment of PETs, the Irish and Maltese authorities indicated that this was not a significant barrier; however, the Spanish, German and Austrian authorities considered this to be a significant or highly significant challenge to overcome.

In general terms, business associations identified staffing and training issues associated with the deployment of PETs (Danish business association and one German consumer association thought these were particularly important) or the perceived technological complexity of deploying PETs (Spanish and Danish business associations); a lack of political imperative (Danish and Hungarian business associations and UK, German and Czech consumer associations); the perceived lack of economic benefits associated with the deployment of PETs (the Danish business association and the UK, Hungarian and German consumer associations).

Consumer associations mentioned that a general lack of awareness of PETs and the availability of information describing exactly how to deploy PETs were significant reasons for the non-adoption of PETs. It is also interesting to note that both consumer and business associations indicated that the refusal of customers to pay for PETs and consumer acceptance of current privacy arrangements were reasons for the non-deployment of PETs by businesses.

### 4.3 Promoting PETs deployment

Data protection authorities acknowledge the difficulty of increasing the deployment of PETs. The Estonian authority highlights the inertia of businesses and believes that PETs will not be deployed if doing so requires specific efforts on the part of businesses. The UK authority makes the point that relying on altruism is ineffective. Businesses will only invest in PETs if they stand to benefit from doing so. The authority acknowledges that this means that deployment will vary from business to business.

The Estonian authority suggests that including PETs in applications by default is the way forward although it is not clear whether they envisage binding (legislative) obligations to include PETs. The Maltese authority takes a gradualist view: PETs should be deployed according to the specific data protection requirements of individual businesses. The implication seems to be that this would increase PETs deployment over time, and would minimise the costs of deployment. Importantly, the initiative for this is assumed to come from businesses themselves.

In contrast, the data protection authority in the Netherlands sees consumer concern as the driving force for PETs deployment. It argues that businesses (especially financial institutions) should take active steps to address consumer concerns and mentions examples of measures that are already being taken (e.g. campaigns to inform customers about the threat of *phishing* attacks and the use of secure connections).

The views of the data protection authorities in our sample highlight the fundamental disagreement about the causes of the unanimously perceived lack of deployment, and the resulting differences in policy approaches to PETs. Essentially, three stances can be distinguished depending on who is seen as the driving force behind PETs deployment:



- in the first, exemplified by Maltese and UK authorities, business is the key driver of PETs adoption, reacting to data protection requirements that are assessed using standard appraisal tools;
- in the second, seemingly endorsed by the Estonian authority, standards, possibly set by government, drive PETs deployment, against a backdrop of reluctant businesses and apathetic consumers; and
- finally, in the third, PETs deployment is a reaction to active consumer concerns, to which businesses respond by competing for consumer trust.

#### 4.3.1 The role of public data protection authorities

The stakeholders are in agreement that raising awareness and educating stakeholders about the risks to and means of protection of personal information is the most important function of public bodies and business and consumer associations. One authority highlights the importance of getting decisionmakers in business involved, rather than preaching to the converted, i.e. the technical staff involved with data protection issues. Some also see a responsibility to monitor/test the available PETs, while some argue for an independent body for testing certifying PETs. Finally, levels of enforcement of data protection legislation are sometimes perceived as inadequate. Specific suggestions included:

- encouragement of the use of “privacy impact assessments”, so that data controllers understand the types of privacy risks their activities result in;
- dialogue between public bodies and businesses, to help the latter understand regulation and the need for PETs;
- advice from public bodies to businesses on concrete PETs, including information on emerging threats that individuals face as a result of online activity; and
- increasing the role of strategic litigation and subsequent sanctions to internalise the costs associated with data misuse or loss by businesses.

#### 4.4 Summary

Data protection authorities, business associations and consumer advocacy groups are in agreement over most of the important issues surrounding PETs. The risk associated with the use of personal data in electronic form is universally recognised as serious and growing. At the same time, consumer awareness of these risks is seen as low. PETs are seen as an effective means of data protection. The main benefits of PETs for data controllers are seen in their ability to foster trust and customer loyalty.

As one would expect, differences of opinion surface in certain areas. Business and consumer organisations emphasise that public bodies are to blame for some of the most notorious cases of data loss in recent years. They also stress the international dimension of the issue, arguing that, when it comes to data protection provisions, the system is only as strong as the weakest link in the chain, which might be a jurisdiction outside the European Union. While data protection authorities see the cost of PETs as an important impediment to their deployment, business associations consider the lack of a political imperative as more important. Businesses also highlight the refusal of consumers to pay for PETs.

We can observe an interesting disconnect among the views of data protection authorities: on the one hand, they tend to state that both overall adoption rates and consumer awareness of PETs are low; while on the other hand, they claim that one of the main benefits associated with the wider deployment of PETs would be an increase in consumer trust.

The argument could be made that consumers, overburdened by the (technical) intricacies of PETs, but at the same time seduced by the unquestionable benefits of online applications (such as social networking sites, online banking, e-commerce, etc.), engage in online transactions with vague concerns about privacy protection. In this situation, an increase in PETs deployment leading to an increase in consumer confidence across the board might provide a major stimulus to the development of online services, in which newly empowered consumers are prepared to undertake more activities online.

However, while this is a plausible scenario, it lacks empirical support. In fact, the rapid growth in online markets, and the testimonies deploring consumer carelessness and ignorance would suggest that consumer demand for better privacy protection is low.

The assertion by data protection authorities that the use of PETs can confer a competitive advantage on data controllers is more theoretical than empirical. If PETs are indeed a mark of quality to which consumers would respond, then PETs could result in product differentiation and command a price premium in the market place. However, empirical evidence shows the reputation loss from data losses to be relatively low and transitory and business associations complain about the unwillingness of consumers to pay for PETs.

Overall, the consultations suggest that many of the representative bodies with a remit that incorporates PETs are convinced of the need for PETs, but benefits are often asserted rather than demonstrated with evidence.

## 5 Case Studies

In this section, we present six case studies to illustrate how and why data controllers deploy PETs, what economic benefits they derive from PETs, and what role the public sector plays in this context. The detailed case studies presented in this section were selected on the basis of research conducted during an earlier phase of the study which yielded a total of 20 case studies provided in 0 and are intended to:

- provide examples of the costs and benefits of PETs deployment; and
- convey a picture of the range of issues that need to be considered in the assessment of the benefits of deployment.

The economic benefits of PETs for data controllers, which are the central focus of this study, are discussed both qualitatively and, where possible, quantitatively. As the case studies demonstrate, the benefits of PETs are often highly specific to the application with which they are used, and the wider context of deployment. This means that an assessment of the benefits of “PETs” as an abstract category is unlikely to achieve meaningful results. A detailed study of specific instances of PETs deployment, however, can establish:

- the role PETs can play given individual data controllers’ specific requirements (which depend on the legal, institutional and business context, as well as on the technology in question and details on how personal data is used); and
- the type and magnitude of the benefits of PETs deployment, contingent on a particular data controller’s (or class of data controllers’) circumstances, the costs of the PETs used, etc.

We begin this section with an introductory discussion of the challenges of establishing the benefits of PETs. The six detailed case studies follow as examples of how the assessment can be undertaken in practice. Finally, the lessons drawn from the case studies are summarised in the conclusion to this section.

### 5.1 Assessing the economic benefits of PETs

Considerable uncertainty exists about most of the key variables determining the benefits of PETs, including the risk of economic loss due to privacy breaches, the demand response to increased PET deployment and the efficacy of some of the technologies in the face of evolving threats. Perhaps the largest single source of uncertainty lies in the fact that much of the promise of PETs in terms of innovative business models and increased consumer trust is as yet unrealised.

Equally important is the difficulty of isolating the effect of PETs from the benefits of the applications with which they are deployed. Typically, PETs are used by businesses not for their own sake, but to a) reduce the risk of data loss (and the associated costs resulting from official sanctions or fines) or b) attract or keep customers who are concerned about privacy.

For example, the benefits of e-commerce in terms of convenience for shoppers and economies of scale for businesses could not have been achieved without PETs. But, it would be wrong to argue that PETs have caused all these benefits. Moreover, the same PETs might be deployed by different

businesses with very different results, depending on the market these businesses operate in, as well as business specific factors, such as strategy. Disentangling the contribution of PETs from these other factors is data-intensive and requires careful, case-by-case analysis.

A further problem lies in the diversity of PETs, i.e. the large variety of different technologies that are subsumed under the PET label. Each of these might yield categorically different benefits. For example, in terms of their effect, some PETs make personal data more secure, thereby reducing the expected loss associated with disclosing personal data, while other PETs remove the need to hold personal data, which eliminates the associated risk altogether.

As noted earlier, it is also important to recognise that many PETs have costs as well as benefits. The benefit of greater data security has to be weighed against those costs, which include the cost of buying (or designing) and maintaining the PET, as well as the potential economic benefits foregone through restrictions on the use of personal data. The fact that costs and benefits might be realised at different points in time (for example, data minimisation today may prevent data losses in the future, when conventional data protection measures may have become obsolete) makes conclusions about benefits based on observations of past performance problematic. This problem is especially acute in the PETs context, where technology is continuously advancing and where many observers pin their hopes on a ‘paradigm shift’, leading to a situation where privacy issue take on much greater importance than is currently the case.

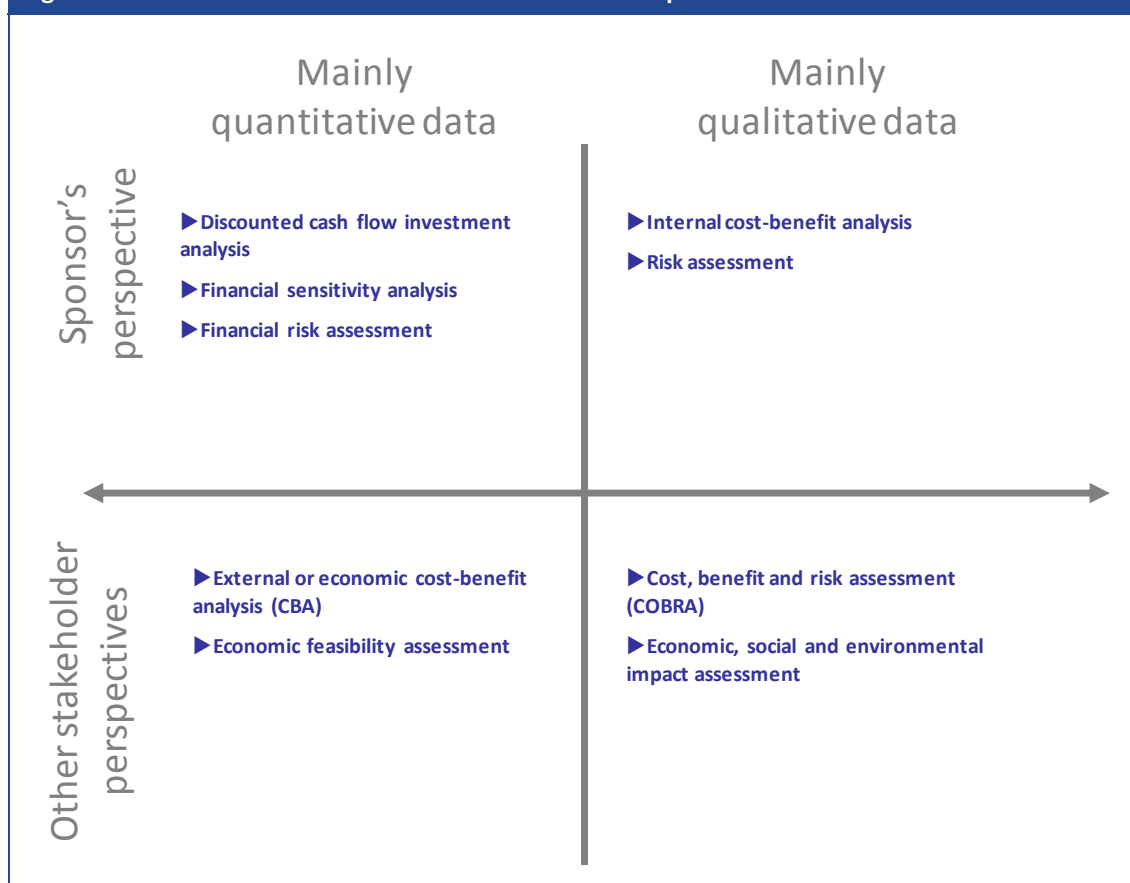
Finally, it should be remembered that the benefit of PETs for individual businesses might be small compared with the benefit to society as a whole, and that the benefits of better privacy protection are in part immaterial and do not necessarily translate into economic benefits for data controllers.

All of this makes it doubtful that the economic benefits of PETs can be quantified in the abstract. Rather, a careful assessment on a case-by-case basis is necessary, and even such an approach is likely to suffer from considerable uncertainties.

### 5.1.1 Possible approaches

In practice, the benefits of PETs deployment are assessed in a number of ways, which deal with the difficulties described above in ways that are more or less adequate. Clarke (2007) provides an overview of the techniques that can be used to develop a ‘business case’ for PETs, a diagrammatic representation of which is shown in Figure 21 below. The feasibility of different techniques depends on their data requirements. The ones listed on the left require detailed financial data, while the ones on the right rely mainly on qualitative factors. Clarke (2007) makes a further distinction between techniques that assess the value of PETs mainly from the “sponsor’s”, i.e. the data controller’s perspective and techniques that can be used to incorporate the effects on other parties. He notes that this is a more prominent concern for public sector organisations but is also important for private businesses. Which of the techniques shown in Figure 21 is appropriate thus depends on the situation of the data controller as well as on the available data.

Figure 21: Classification scheme for business case techniques



Source: Clarke (2007)

All the approaches listed above have in common that they require the prior specification of costs and benefits, i.e. the need for using PETs from the point of view of the data controller (and other stakeholders, depending on the circumstances).

The costs and benefits that need to be taken into account were discussed in detail in Section 3. Benefits are mainly the possible increase in demand due to PETs and the avoidance of the costs of privacy breaches, while costs include the direct costs of deployment as well as possible reductions in the ability of data controllers to use personal data.

Clarke (2007) notes that the assessment process itself can be of benefit to data controllers. Because exploring the benefits of deployment “signals the organisation’s willingness to address negative perceptions of its activities, and involves the engagement of stakeholders, benefits may arise from the mere act of conducting business case analysis, even if the eventual decision is to not proceed with the initiative”.

Another factor that needs to be taken into account is that, even if the costs appear high, investment in PETs may well be justified as a strategic measure, even though this is difficult to justify formally by means of standard investment appraisal methods. The reason for this is the potential for externalities, including greater innovation and overall greater levels of consumer

confidence leading to the creation of a larger, more comprehensive and more active market for digital economy services. While standard methodologies can theoretically be adapted to take such factors into account, in practice the inclusion of all relevant factors is difficult, giving the surrounding uncertainties, and thus rarely done.

The literature on PETs does not provide many examples of detailed cost-benefit analysis. Koorn et al. (2004) present a very simple hypothetical example of the costs and benefits of implementing a Privacy Management System (PMS). Looking at Table 11, it is clear that the authors see the PMS primarily as a labour-saving, efficiency-enhancing mechanism. Most of the items deal with labour costs that can be saved or reallocated once the system is up and running (management and secretarial labour costs, cost privacy audit, compliance). No detail is given on how the figures on the damage averted by the PMS were estimated. Other factors that would be relevant from an economic perspective, including the discount rate and the opportunity cost of the investment, are not provided in the example.

| Table 11: Return on investment from a Privacy Management System (PMS)                                                                                            |                              |                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|------------------|
| If PMS were not implemented, the minimum <i>annual</i> costs for an organisation employing 1,000 staff to comply with privacy policies are estimated as follows: |                              | Annual costs     |
| Salary costs Privacy Officer (100% time allocation)                                                                                                              |                              | € 100,000        |
| Management and secretarial salary costs                                                                                                                          |                              | 40,000           |
| Costs of privacy audit                                                                                                                                           |                              | 30,000           |
| Security costs with respect to privacy compliance (excluding generic information security required)                                                              |                              | 20,000           |
| Report maintenance, regulations, settling registered people's rights, information, image and other damage, etc.                                                  |                              | 20,000           |
| <b>TOTAL</b>                                                                                                                                                     |                              | <b>€ 210,000</b> |
| When using PMS:                                                                                                                                                  | Development & implementation | Annual costs     |
| Acquisition of PMS                                                                                                                                               | € 150,000                    |                  |
| Consultancy for PMS implementation (60 days)                                                                                                                     | 80,000                       |                  |
| Start-up costs after implementation                                                                                                                              | 20,000                       |                  |
| PMS operational costs                                                                                                                                            |                              | 30,000           |
| Maintenance ± 15% of acquisition cost per annum                                                                                                                  |                              | 22,000           |
| Costs of privacy audit                                                                                                                                           |                              | 10,000           |
| Salary costs Privacy Officer (50% time allocation)                                                                                                               | 50,000                       | 50,000           |
| <b>TOTAL</b>                                                                                                                                                     | <b>€ 300,000</b>             | <b>€ 112,000</b> |

Source: Koorn et al. (2004)

However, even this stylised example requires data that is typically not available outside the organisation undertaking the assessment. In our case studies, we used financial or at least quantitative measures where available. In cases where quantitative data could not be obtained, qualitative data was used instead.

The following six case studies are based on interviews with data controllers, as well as published sources. Every effort was made to arrive at a quantitative conclusion as to the benefits of PETs deployment for data controllers, although commercial sensitivity as well as the fact that some of the technologies we portray are not yet available as commercial products mean that the results are mostly qualitative.

In order to help the reader navigate the different case studies, all case studies follow a common structure:

- Each case study starts with a discussion of the application in the context of which the PETs are deployed.
- After this, the PETs themselves are discussed in appropriate technical detail.
- Based on this background information, the next sub-section examines the rationale for the deployment of PETs from the perspective of the data controller.
- Then follows a discussion of the effects of deployment, including, where possible, the quantification of costs and benefits.
- A separate sub-section considers the role played by the public sector in the deployment.
- Finally, each case study concludes with a summary of the insights it provides on the question of the economic benefits of PETs deployment for data controllers.

## 5.2 Case study I: GENOMatch

GENOMatch is a complex PET designed to be used with highly sensitive personal data (genetic information) in a strictly regulated environment (pharmaceuticals development). GENOMatch shows the importance of embedding PETs into a system of data protection that encompasses technical and organisational factors. It is a mature design that has been certified by data protection authorities in Germany. The GENOMatch example also draws attention to the difficulties faced by producers of PETs trying to overcome the perception that PETs are expensive and unnecessary, and highlights the importance of proactive data controllers as well as the role of intermediaries in driving PET adoption. Finally, the example shows that the economic benefits of PETs can be very application-specific. The way in which PETs benefit a business needs to be carefully analysed in order to derive meaningful quantitative predictions.

### 5.2.1 The application

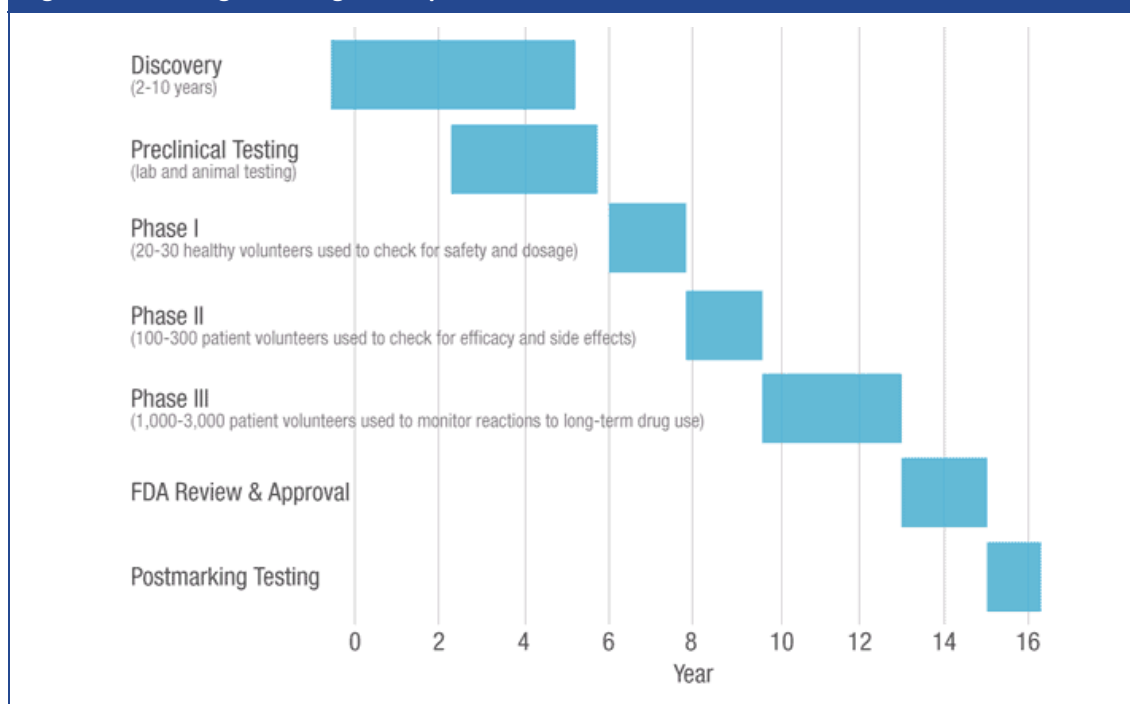
GENOMatch a system designed to protect the privacy of individuals participating in pharmacogenetic studies. Pharmacogenetics is the study of how genes influence individuals' response to drugs; as such, it is today a normal part of drug development as practiced by major pharmaceutical companies. In pharmacogenetic research, clinical data (i.e. observations on the effect of a new drug) is combined with genetic information on study participants to identify the influence of a person's genes on the effectiveness of the drug, adverse reactions, etc.

In practice, this involves taking blood and tissue samples from study participants, from which genetic material is extracted. The genetic data is combined with the clinical data and statistical methods are used to identify the relationship between genes and the effects of the drug.

The process leading up to the introduction of a new drug to the market is strictly regulated. It involves numerous studies, starting from laboratory and animal experiments and cumulates in clinical trials involving thousands of participants. Pharmacogenetic studies are part of these clinical trials, either as fully integrated components or added on to existing trials. Figure 22 below shows the sequence and illustrates the approximate duration of the different phases.

The cost of the process increases dramatically in the later (clinical) stages leading up to the application for approval by the relevant authority (e.g. the European Medicines Agency, the US Food and Drug Administration, etc.). The decision to undertake a Phase III trial is typically the most pivotal one, given the time and the enormous costs this involves. The studies in Phase III are designed to confirm the drug's effectiveness, monitor side effects, compare it to commonly used treatments, collect information that will allow the experimental drug to be used safely, and to evaluate the overall benefit-risk relationship of the drug. The results from the studies conducted during Phase III provide the data for the official approval process. Phase III typically lasts several years, and 70-90% of the drugs that reach this phase complete it successfully.<sup>66</sup>

**Figure 22: The stages of drug development**



Note: The Food and Drug Administration (FDA) is the government agency in charge of approving new drugs in the United States. In the EU, this function is carried out by the European Medicines Agency (EMA) and national authorities. The duration of the different stages is indicative.

Source: *investbio* ([http://www.investbio.com/clinical\\_trials\\_biotech.asp](http://www.investbio.com/clinical_trials_biotech.asp))

<sup>66</sup> See [http://www.investbio.com/clinical\\_trials\\_biotech.asp](http://www.investbio.com/clinical_trials_biotech.asp).



### 5.2.2 The PET

GENOMatch is a system for handling genetic samples in the context of pharmacogenetic research. It is designed to balance the confidentiality requirements of trial participants with the researchers' need to be able to link clinical and genetic data. GENOMatch was developed in 2003 in a cooperative project involving Bayer Schering Pharma AG, a leading German pharmaceutical company, researchers at the University of Kiel and the software developer Tembit Software GmbH. Bayer Schering Pharma AG ("Schering AG" at the time GENOMatch was conceived) was the instigator of the project and the first data controller to use the system.

The architecture of the PET is determined by the fact that the complete anonymisation of samples is not desirable:

- First, the authorities in charge of drugs licensing require access to all the data that have been used in the research leading up to the licensing application.
- Secondly, every participant has the right to end his participation at any time and to have his personal data permanently and verifiably deleted.
- Finally, participants must be identifiable in case:
  - a) their genes reveal information about illnesses (or predispositions to illnesses) about which the participants need to be informed in order to protect their health;<sup>67</sup>
  - b) there are interactions between genes and the drug that is being tested, which may require that an individual be withdrawn from the study.

All of this means that individuals' data must be traceable and identifiable at every stage, so that pseudonymisation, rather than complete anonymisation, is required.

The functions of GENOMatch are further determined by the practical steps involved in pharmacogenetic research:

- sample and save of DNA;
- decision on DNA analysis based on clinical findings and subsequent genetic data storage; and
- biostatistical analysis of clinical and genetic findings (pharmacogenetics).

Given these requirements, GENOMatch fulfils two specific roles:

- First, it creates different layers of information access depending on the different responsibilities of the various parties involved in the process (i.e. access keys are hosted by an independent provider with no access to the data itself; pharmacogenetic researchers have no access to clinical data as long as they are linked to a traceable link to an individual patient, e.g. the patient number or initial in the clinical data set); and

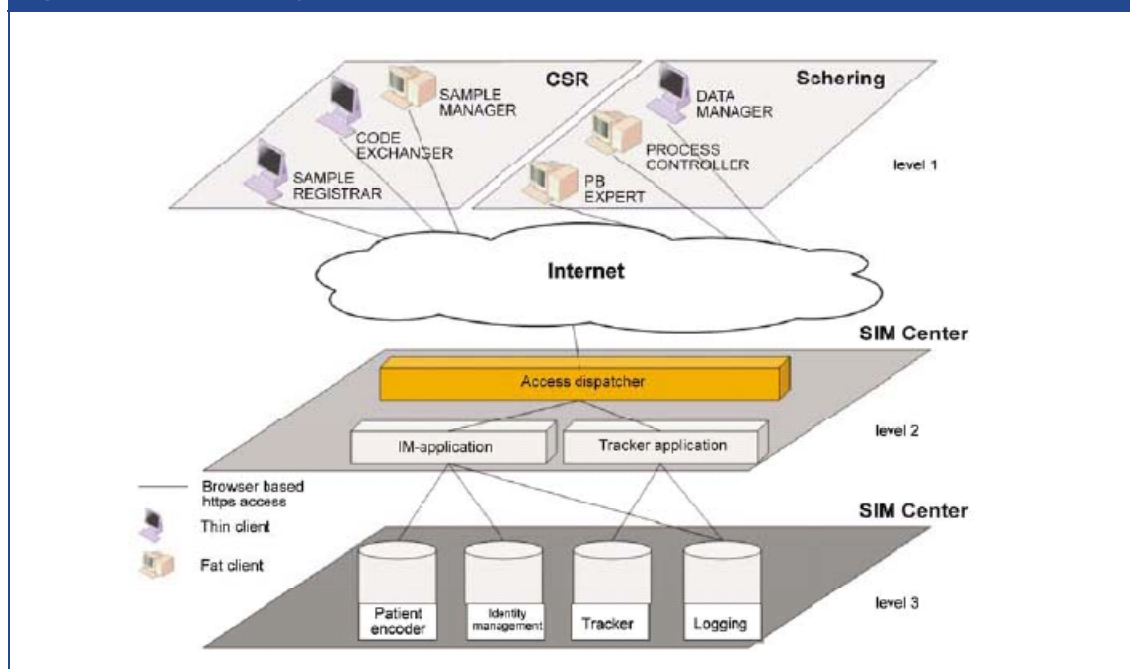
---

<sup>67</sup> Note that genetic information about an individual may also predict outcomes in family members.

- secondly, it allows samples to be identified (i.e. linked to specific individuals) at every stage of the process.

In short, security is provided by secure pseudonymisation throughout a given trial/research project. The three-layer architecture of GENOMatch is shown in Figure 23. Level one is a browser-based user interface through which users access the system over the Internet (via the secure https protocol) using role-specific credentials in the form of personal smart cards in combination with an individual PIN.<sup>68</sup> A software module called *role-based access dispatcher* ensures that users can access only that information which they need to fulfil the tasks assigned to their role.

Figure 23: GENOMatch system architecture



Note: The GENOMatch system consists of three levels. Level 1: user front end providing role-based access. All users communicate via the Internet (https). In this picture, the SDA is the Bayer Schering Pharma AG (Schering) who commissioned GENOMatch. Level 2: GENOMatch application. The access dispatcher ensures that only authorised users get access to their role specific function. Level 3: GENOMatch databases. The data-model ensures a strict separation of key code list administration (patient encoder and identity management), tracking information (tracker) and audit trail (logging).

Source: Reischl et al. (2006)

Level one comprises the Central Sample Repository (CSR), where the genetic samples are stored, and the Secure Data Area (SDA) where the Pharmacogenetics Biostatistical (PB) Experts carry out their analysis of the data.

Upon collection, each genetic sample is labelled with a Patient Number (PN), which is a pseudonym unique within each study, and a barcode (BC1). The sample is then sent to the CSR, where it is checked:

<sup>68</sup> Note that sensitive operations, such as the deletion of records, need to be confirmed by two users to take effect, which minimises the risk of abuse by insiders (i.e. users with valid credentials).

- whether the sample is useable; and
- whether patient consent was obtained.

The CSR then removes the labels, attaches a new barcode (BC2) which cannot be linked to PN or BC1 within the CSR (*double coding*) and puts the sample into storage.

The recoding process is done in two steps by two different individuals, the Sample Registrar (SR), who removes the PN, and the Code Exchanger (CE), who exchanges BC1 for BC2. Only then are the samples handed to the Sample Manager (SM) for storage. SR and CE each submit one pair of identifying information to the Secure Identity Management (SIM) Centre: (PN,BC1) and (BC1,BC2). This forms the key code list at the centre of the system, that is, the only part of the system through which clinical and genetic information can be linked.

Levels 2 and 3 together constitute the SIM Centre.<sup>69</sup> Level 2 contains the 3 applications that make up the system:

- the access-dispatcher software that manages the role-based user access;
- the identity management application; and
- the sample tracker application that allows tracking the status of a genetic sample at every stage of the process.

Level 2 is hosted by an independent application service provider, with no other involvement in the research process and, crucially, no access to any of databases. All the databases used by the level 2 applications are hosted separately in level 3.

The CSR together with the SIM Centre constitutes the DNA *biobank*, a secure database and storage system for genetic samples. Note that there is no direct communication between CSR and SDA – all data exchange takes place securely via the SIM Centre.

On the SDA side, there are three important functions:

- the Process Controller (PC), who is in charge of the administration of users and studies, but has no access to individual clinical data entries, only to workflows;
- the Pharmacogenetic Biostatistical Expert (PBE), who orders samples for genetic analyses and performs the statistical analyses; and
- the Data Manager (DM), who combines genetic and clinical data (which are linked in the SIM via the key code list) into a database for analysis.

Users on the SDA side - a small number of biostatisticians - never have access to personal data that is not de facto anonymised (i.e., it can be traced back to individuals only via the SIM Center).

---

<sup>69</sup> In the implementation by Bayer Schering Pharma, the SIM Centre is hosted by Dataport (<http://www.dataport.de>), a state-sponsored independent application service provider.

### 5.2.3 Discussion

#### ***Objective of /need for PETs***

The need for a strong data protection system that accommodates the potential for future tightening of the restrictions on the use of genetic data has been a crucial motivating factor for deploying PETs in this case.

Human genetic information is a type of personal information that is often viewed as deserving special protection.<sup>70</sup> The concern is that genetic information may reveal a large amount of detailed information on individuals (and their genetic relatives), including personal traits, hereditary diseases, etc. This places a high responsibility on organisations working with such data, including companies engaged in pharmacogenetic research.

GENOMatch has been designed to be fully compliant with existing privacy and data protection legislation. In addition, a main aim of the system was to provide flexibility in the face of an evolving legislative environment and changing public perceptions about the privacy risk associated with genetic research. Thus, the system actually provides for more privacy protection than is currently legally required. Features that exceed current requirements include the institutional separation of the SIM centre and the “four-eyes” policy requiring potentially risky data operations (e.g. the deletion of records) to be authorised by two accredited users.

However, the forward-looking attitude described above that led to the development of GENOMatch and its deployment (to date, two companies are using the system, with another one in the process of implementation) appears not to be widespread in the industry. According to our sources, there are some 500 companies worldwide that engage in pharmacogenetic research and could benefit from a system like GENOMatch.

The fact that the companies deploying GENOMatch do so voluntarily (while other companies operate – seemingly successfully – without it) suggests that there are economic benefits. If this is the case, the fact that others do not deploy PETs could suggest either a lack of awareness or insufficient enforcement of data protection legislation. The latter reason has been mentioned to us by German data protection professionals.

The company selling GENOMatch (Tembit GmbH) reports, however, that awareness of the need for PETs is increasing in the industry. There is interest in GENOMatch from companies in Europe, the US and the Middle East. A major barrier to increasing deployment rates is the time it takes for deployment decisions to be taken, in particular in the case of large companies, which suggest that GENOMatch could be moving up the S-curve as deployment takes off.

If we assume, as the companies deploying GENOMatch seem to, that there are tangible benefits from deployment, where might these come from? There is not much evidence that demand from individuals for better privacy protection is an important factor. The individuals that would be

---

<sup>70</sup> See for example UNESCO International Bioethics Committee. DRAFT International Declaration on human genetic data, Addendum 2, 8.10. 2003: “Human genetic data have a special status. Due consideration should be given and where appropriate special protection should be afforded to human genetic data and to biological samples”.

expected to react to PETs deployment in this case are the people who participate in pharmacogenetic studies. They are recruited by pharmaceutical companies, who need to recruit a sufficiently large number of subjects per study, as a certain sample size is required to ensure the accuracy of the statistical predictions.

We have been told that individuals are highly unlikely to opt out of pharmacogenetic studies (after all, the individuals are already participants in clinical trials). According to one source, only one in 10,000 participants withdraws consent. General practitioners, who are often consulted by individuals before the participation decision, seem to have no strong incentive of their own to counsel against participation or to insist on high standards of privacy protection on behalf of their patients.

However, one source also reports that study participants in the US have been known to withhold their samples due to privacy concerns.

The developers of the PET also assume there is a positive effect of PETs on the recruitment of study participants. This could be highly valuable for data controllers, as slow recruitment or withholding of samples can hold up the trial process and delay the introduction of a new drug. We have not been able to ascertain or quantify the effect of PETs on the recruitment of study participants, although if this effect exists, it may represent a significant incentive for PETs deployment.

Given the uncertainty surrounding the effect of PETs on individual study participants, potentially the most important driver of PETs adoption from an economic perspective are intermediaries. In the context of pharmacogenetic research, these are data protection officers inside the pharmaceutical companies and the ethics committees that oversee the research. The latter are the most influential, due to their power to delay the research programme if the standard of privacy protection is insufficient. The developers of GENOMatch see ethics committees as the most potent force in favour of increased PETs deployment.

### ***Effect of PETs***

GENOMatch has been characterised by one data controller as a ‘necessary compromise’, that is, an elaborate system that in some ways makes pharmacogenetic research more difficult, but whose implementation was deemed necessary to ensure transparency and allay concerns about patient confidentiality and the security of genetic information.

When considering the effects of the PET it should be remembered that the pharmaceutical companies (data controllers) have no interest in the personal data they collect outside their pharmacogenetic research. And even here, data on individuals is only required for reasons of transparency and accountability, as described earlier. The economic benefit of GENOMatch is thus only its contribution to conducting research, while the costs are simply the costs of buying, maintaining and operating the system. Two types of benefit can be distinguished:

- The first benefit of GENOMatch is greater legal certainty, with the associated benefits of reduced risk of sanctions and lower legal fees. An important contributing factor is the certification of the GENOMatch concept by the Independent Centre for Privacy Protection (ICPP) in Schleswig-Holstein, which we discuss in more detail below.

- The second benefit, which is likely to be much more significant than the first, is the contribution of GENOMatch to the smooth running of the drug development process. As clinical trials are very expensive, even short delays can cause costs in the order of millions of Euros. The actual cost of delay depends on many factors, including the overall length of the development stage before marketing authorisation is obtained, the size of the market (number of patients) etc., most of which are drug-specific. However, the costs are likely to be substantial: an estimate from the US<sup>71</sup> suggests that a delay of one week for a \$ 5 billion (€ 3.6 billion) drug would cost a pharmaceutical company \$14 million (€ 10.1 m). GENOMatch helps to minimise delays caused by concerns about privacy protection, either on the part of study participants or (more likely) ethics committees. The following theoretical example illustrates the size of this potential economic benefit of GENOMatch.

### Potential savings through GENOMatch

We consider the ability of GENOMatch to prevent delays in the clinical trials leading up to marketing authorisation to be the most direct and probably the largest source of economic benefits to data controllers. Here we present a hypothetical example of the costs of such a delay and compare it with the cost of GENOMatch.

The economics of the pharmaceuticals sector are governed to a considerable degree by intellectual property (IP) rules. Pharmaceutical companies secure patents for newly discovered drugs or treatments. This is done before any steps are taken towards commercial development. Given that patents expire after 20 years, the revenues for any given patent depend to a significant degree on how soon after the filing of the patent the new drug can be brought to market. In order to develop a drug from a patented invention to a market-ready product, pharmaceutical companies have to go through a lengthy and highly regulated development process (see Figure 22) before obtaining permission to market the new drug from the relevant authorities.

As the length of this process subtracts from the time left on the patent (the revenue period), it directly determines the revenues a company can earn from a patented drug. As out-of-patent drugs face competition from generics, which typically leads to a collapse in revenues for the patent holder, it is of paramount importance to avoid delays at the development stage.

Thus, the economic value of a new drug consists of the cost of the development stage and the revenues earned between the market introduction and the expiry of the patent. These costs and benefits are spread out over time, so the appropriate figure to consider for an overall assessment is the net present value (NPV), i.e. the sum of the discounted future cash flows. Given that there is a significant chance that a patented drug will not make it to market, the NPV needs to be adjusted for risk at the development stage. Here we use the risk-adjusted NPV (rNPV) as proposed by Stewart (2004). It is calculated as follows:

$$rNPV = \sum_{i=0}^n \frac{C_i R_0}{(1+r)^i R_i}, \text{ where}$$

<sup>71</sup> Quoted in a presentation by Pharsight Corporation at the first American Conference on Pharmacometrics (2008), available at: <http://tinyurl.com/yab2oyw>.

- $C_i$  is the cash flow at time  $i$ ,
- $R_0$  is the current likelihood of reaching the final cash flow,
- $R_i$  is the likelihood at time  $i$  of reaching the final cash flow,
- $R_0/R_i$  is the current likelihood (i.e., at time 0) of realising the cash flow of time  $i$ , and
- $r$  is the discount rate.

In the following, we will use estimates of the likelihood of eventual approval of a new drug at the different stage of development provided by Stewart (2004) and based on observations from the US. A summary is shown in the table below.

| Table 12: Success rates during the development process |         |          |           |          |
|--------------------------------------------------------|---------|----------|-----------|----------|
|                                                        | Phase I | Phase II | Phase III | Approval |
| Likelihood of eventual FDA approval                    | 20%     | 30%      | 67%       | 81%      |
| Average years to completion:                           | 0.5-1   | 1.5      | 3.5       | 0.5-2    |

Source: Stewart (2004)

To illustrate the potential effect of GENOMatch for the data controller, we use the rNPV for a fictional drug 'X'. For the calculations, we adapted a spreadsheet model of the risk-adjusted NPV for pharmaceuticals developed by Stewart (2004).<sup>72</sup> The choice of parameters in the model and the default values are based on the FDA approval process.

First we consider the cost of GENOMatch, information on which was provided by Tembit. GENOMatch is a custom-made product, initially tailored to the needs of an individual data controller (Bayer Schering Pharma). However, it is designed to be interoperable with a variety of data handling systems used in the pharmacogenetics sector and has been sold to one other company at the time of writing. While it is thus not an 'off-the-shelf' solution, GENOMatch is marketed as an integrated product that is operated by data controllers under licence. Maintenance and service are provided by Tembit on an ongoing basis. The approximate costs of the system are shown in the following table.

| Table 13: Direct cost of GENOMatch to data controllers |           |
|--------------------------------------------------------|-----------|
| Item                                                   | Cost*     |
| Licence                                                | € 250,000 |
| Annual maintenance and upgrades                        | € 40,000  |

Note: \* costs are estimates based on the current implementations of GENOMatch. Actual implementation costs may differ according to the specific requirements of the client, pre-existing data processing systems, etc. A different pricing model based on licenses for individual studies is used by Tembit when selling GENOMatch to public research institutions.

Source: Tembit Software GmbH

<sup>72</sup> The model can be downloaded here: <http://tinyurl.com/yfgj5cl>.

The first thing to note is that these costs are low compared with the typical costs of a clinical trial. An illustration of the costs typically incurred during a clinical trial is given in Table 14. In net present value terms (assuming a discount rate of 15%<sup>73</sup>), the cost of the entire trial to the pharmaceutical company is approximately € 20 million, while the discounted cost of GENOMatch (consisting of € 250,000 for the licence in year 1 and € 40,000 annually thereafter) is € 0.4 million, or 1.9% of the total (or just € 0.2 million or 0.9% if the cost of the licence is already written off and only the annual maintenance costs left to pay).

| Table 14: Example of clinical trial costs |           |             |              |
|-------------------------------------------|-----------|-------------|--------------|
|                                           | Phase I   | Phase II    | Phase III    |
| Duration (years)                          | 1         | 2           | 3            |
| Number of participants                    | 60        | 200         | 2,000        |
| Annual cost per participant               | € 8,734   | € 8,734     | € 4,367*     |
| Annual cost of animal studies             | € 363,901 | € 363,901   | € 363,901    |
| Total cost                                | € 887,918 | € 4,221,252 | € 27,292,576 |

Note: Average \$ values converted to € using the ECB exchange rate of 11/02/2010 (1.374). \* Annual costs per patient in Phase III can be considerably higher.

Source: based on Stewart (2004)

However, a low cost of the PET compared with other costs is not enough to justify its deployment economically. The relevant consideration is whether the PET leads to benefits that are absent without the PET. To assess this, we have to look at three cases:

- In the base case (CASE1), the company does not use any PET. The trial proceeds according to the probabilities associated with the completion of each phase and, once market approval is obtained, revenues are collected until the patent expires.
- In the second case (CASE2), privacy concerns (by an ethics committee or by participants themselves) during clinical trials mean that the process is delayed and a PET needs to be bought in order to continue. We assume a delay of six months.<sup>74</sup> The company is clearly worse off compared with the case where the trial runs according to plan without a PET.
- In the third case (CASE3), the PET is deployed on the company's own initiative and is operating throughout the clinical trial phase. This means that the company has to incur additional costs compared with the base case, but does not face the risk of costly disruption. We can distinguish between the case where the licence for the PET is bought at the start of the trial (CASE3a) and the case where the company has bought the PET at an earlier stage, so that during any specific trial only maintenance costs have to be paid (CASE3b).

<sup>73</sup> 9-15% is given as the range appropriate for pharmaceuticals investments by Stewart (2004). A lower discount rate would not significantly alter the picture.

<sup>74</sup> This includes the time required for customisation of the software and the necessary adaptation of processes such as the collection of samples. The installation of the software can be accomplished in a matter of weeks.

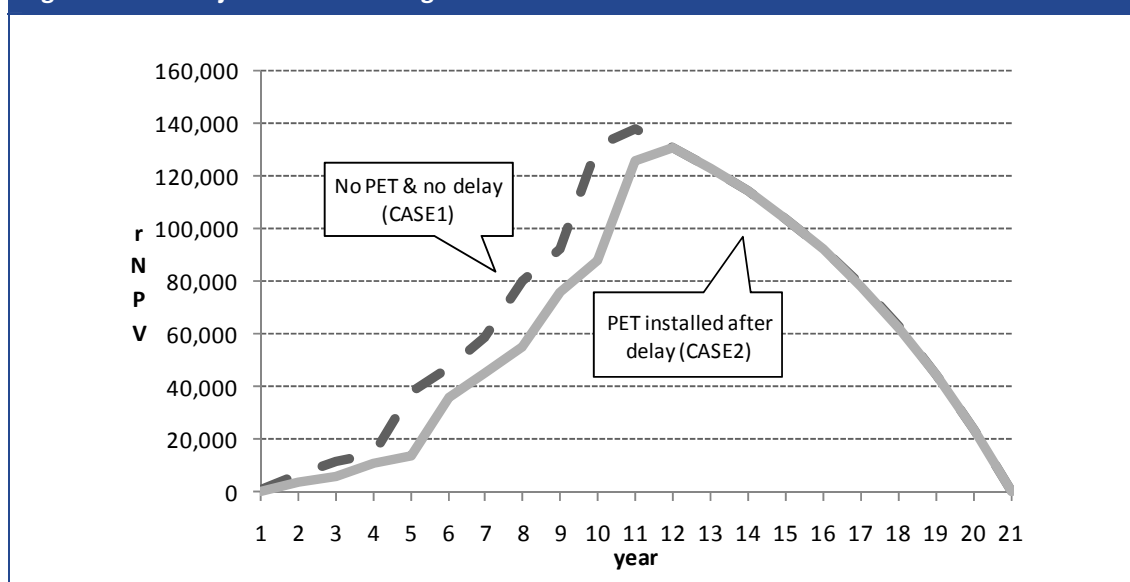


To provide a numerical example, we calculated the rNPV of drug X for the three cases using the parameters shown in Table 14 and the following assumptions about the market for X:<sup>75</sup>

- a patient population of 750,000;
- an annual revenue per patient of \$ 250 (€ 182);
- a peak market penetration<sup>76</sup> of 50%; and
- a discount rate of 15%.<sup>77</sup>

Figure 24 illustrates the effect of a delay on the rNPV of the drug over the lifetime of the patent. The shape of the curve shows how valuation jumps instantaneously upon successful completion of each clinical trial, in accordance with the probability of successful market introduction (see Table 12).

**Figure 24: Risk-adjusted NPV of drug X**



Source: London Economics, based on the model by Stewart (2004)

In order to show how the PET affects the economic outcome for the firm, we have to subtract the NPV<sup>78</sup> of the PET from the rNPV of the drug. The result is summarised in Table 15.

The first column of Table 15 shows the NPV of the drug under the four scenarios. It is highest if the trial proceeds according to plan and there are no additional expenses on PETs (CASE1). Given the

<sup>75</sup> A full list of the model parameters is included in 0.

<sup>76</sup> The model assumes that it takes two years from the introduction of the new drug to reach peak penetration.

<sup>77</sup> Lower discount rates do not alter the picture qualitatively. Their main effect is to lessen the disadvantage of having to pay the licence fee in CASE3 as the weight of the initial cost of the licence decreases relative to the value of the stream of maintenance payments.

<sup>78</sup> Note that the payment stream is not adjusted for risk, as the PET has to be maintained regardless of the progress of any particular clinical trial.

economics of the sector, even a relatively short delay in the development stage can decrease the value of the drug dramatically, in this case from € 757,299 to € 21,049 (CASE2, including the cost of the PET). The net NPV when the PET is used to prevent a delay (CASE3) is simply CASE1 minus the cost of the PET. Here it makes a considerable difference whether the upfront cost of the PET, i.e. the cost of the licence, needs to be paid (CASE3a), or whether the company had the PET installed for an earlier trial and now needs to pay only for ongoing maintenance and support. The cost of the PET in each case is the discounted value of the associated payment streams. Column 3 shows the net benefit of the PET (the saving made) compared with the case in which the lack of PETs leads to a delay.

**Table 15: Effect of PET**

| Scenario | Net rNPV in year 1 (€) | Cost of PET* | Max. net benefit (CASE2 minus CASE3) (€) | Probability of CASE2 such that $E[No\_PET] \leq CASE3$ |
|----------|------------------------|--------------|------------------------------------------|--------------------------------------------------------|
| CASE1    | 757,299                | -            | -                                        | -                                                      |
| CASE2    | 21,049                 | -            | -                                        | -                                                      |
| CASE3a   | 259,370                | 497,929      | 238,321                                  | 67.6%                                                  |
| CASE3b   | 469,370                | 287,929      | 448,321                                  | 39.1%                                                  |

Note: \* over the lifetime of the patent, calculated as the difference between the NPVs of cases 1 and 3, which equals the NPV of the payment streams associated with the PET if a) the licence is bought at the start of the trial and b) only maintenance costs are paid during the trial (i.e. the company owned the licence already at the start of the trial).

Source: London Economics

Given that some companies currently conduct their clinical trials without using adequate PETs, an obvious question is how likely an unproblematic research process without PETs (CASE1) is compared with the worst-case scenario (CASE2). Or in other words: when is the likelihood of a costly delay such that it justifies the cost of the PET? Formally, this can be expressed as:

$$E[No\_PET] \leq CASE3, \text{ where}$$

$$E[No\_PET] = pr(CASE1) + (1-pr)(CASE2),$$

i.e., when is the (certain) return from developing the drug with the PET (CASE3) at least as great as the expected return of developing it without the PET ( $No\_PET$ ), which depends on the probability ( $pr$ ) of facing a delay caused by privacy protection concerns (CASE2) or not (CASE1)?

Having calculated the rNPVs for the different scenarios, we can use the result to derive the probability with which investment in the PET will pay off. This is shown in the last column of Table 15. In the case where the company is already using the PET at the start of the trial (CASE3b), a 39.1% chance of a delay would make investment in the PET worthwhile. If the PET is bought at the start of the trial, this figure is still 67.6%. This suggests that as soon as there is a realistic prospect that privacy concerns might lead to a delay of at least some clinical trials, pharmaceutical companies would benefit unequivocally from deploying PETs. The low cost of technologies like GENOMatch compared with the total investment required in pharmaceuticals development suggests that they are a prudent investment even if clinical trials are often successfully conducted without them.

It should be noted our example is only a first approximation of the calculation a pharmaceutical company might make when exploring whether deploying a PET like GENOMatch would be economically beneficial. For example, we assume that GENOMatch is indeed effective in allaying the privacy concerns of individuals and ethics committees. However, the example demonstrates clearly that a) PETs are a very small cost factor in the context of pharmaceuticals research and b) deployment is economically beneficial with relatively modest assumptions about the effectiveness of PETs.

### ***The role of the public sector***

Although GENOMatch was developed through the initiative of a data controller (Bayer Schering Pharma), the public sector played an important role in its successful deployment and subsequent marketing. First of all, the interest in a strong PET for use in its pharmacogenetic research by Bayer Schering Pharma was caused at least in part by concerns about the possible introduction of stricter rules on the protection of genetic data.

The public debate about the threat to privacy arising from genetic research was seen by Bayer Schering Pharma as a potential threat to its ability to carry out the research necessary to bring new drugs to market. This shows that public debate about data protection issues can affect the behaviour of data controllers, even if the debate is not followed by formal legislation.

On the other hand, the slow take-up of sophisticated PETs by providers of pharmacogenetic research suggests that the enforcement of data protection legislation might be insufficient (alternatively, providers that choose not to use PETs may be located in jurisdictions with weaker data protection standards). Data protection authorities have an important role to play in increasing awareness of the obligations under existing data protection legislation. Improving enforcement should be an element of this approach.

An important aspect of the GENOMatch project is the cooperation between the public and private sectors. As mentioned above, the system was developed by Bayer Schering Pharma (initially only for use in its own research operation) in cooperation with software developers Tembit. However, the two also enlisted the help of researchers at Kiel University to a) incorporate academic expertise in the design of the system and b) achieve official certification for the system, which helps with marketing and lends credibility to the claim of economic benefits.

Seal of the ICPP Data  
Protection Audit



The certification was granted by the ICPP after a Data Protection Audit of the concept in 2003.<sup>79</sup> The Data Protection Audit of the ICPP Schleswig-Holstein is a recognised mark of quality by data protection professionals in Germany and beyond.

The Data Protection Audit is only available for public sector organisations, but Bayer Schering Pharma and Tembit were able to obtain it for GENOMatch by collaborating with Kiel University, a public higher education institution. Arguably, this restriction may be an impediment to the

<sup>79</sup> The audit report (in German) can be found at: <http://tinyurl.com/y8v45mz>.

deployment of PETs, as pure private sector PETs do not have access to the quality signal the Data Protection Audit provides.

The Data Protection Audit is an important part of the marketing effort for GENOMatch and serves in particular to highlight the legal certainty the system provides for data controllers. The effect on consumers is limited, but as we have seen, their role in driving PETs adoption is less important than that of professionals concerned with data protection and privacy, including data protection officers and ethics committees.

#### 5.2.4 Summary

An assessment of the economic benefit of PETs for data controllers requires a detailed understanding how privacy considerations matter under a specific business model and depends on the effect of PETs in the context of the specific application. In the case of GENOMatch, we find the benefit for data controllers (i.e. the institution carrying out pharmacogenetic research) to be increased legal certainty and lower compliance cost, as well as a decreased risk of delays in the clinical trials leading up to a new drug's approval by the relevant authorities. In this way, the PET helps to prolong the revenue stream from drug sales after approval, which, given the economics of the pharmaceuticals sector, is very valuable.

GENOMatch represents a more expensive solution than some of the available alternatives. It has implementation costs and ongoing maintenance costs, and requires a higher level of institutional capability than simpler, but less secure systems to process personal data in the context of pharmacogenetic research. This suggests that awareness and enforcement of existing data protection legislation is insufficient. In turn this points to a clear role for the public sector to increase awareness and/or strengthen enforcement. The developers of GENOMatch are trying to leverage the ICPP Data Protection Audit, a public data security certification scheme, to promote the system.

However, while official credentials such as the data protection audit are useful, they are little known to the general public, including decision-makers in companies. Their signalling potential is currently limited to data protection professionals. This situation draws attention to the important role of intermediaries in providing a case for PETs to businesses in situations where consumer interest in privacy is low. In the GENOMatch case we identified ethics committees as potentially important drivers of PET deployment, as they combine an interest in privacy protection with the power to force remedial action by companies engaging in clinical research.

Finally, the fact that GENOMatch was developed on the initiative of a data controller for its own use (and is now starting to be used by others) suggests that it has real economic benefits for deployers and we provided a numerical example showing that a system like GENOMatch is economically beneficial under plausible assumptions. The example also shows that the quantification of benefits requires a considerable amount of detailed information.

### 5.3 Case study II: PriPAYD

This second case study is about a PET concept that has not yet been implemented commercially at the time of writing. We include it to demonstrate the difficulties that a strong PET, using simple concepts and off-the-shelf technologies, faces in the market place. The example shows that these

problems persist even if the technology holds the promise of unambiguous commercial benefits to deployers. Further, it highlights a potential ambiguity in the application of data protection legislation, which can inhibit the deployment of PETs.

### 5.3.1 The application

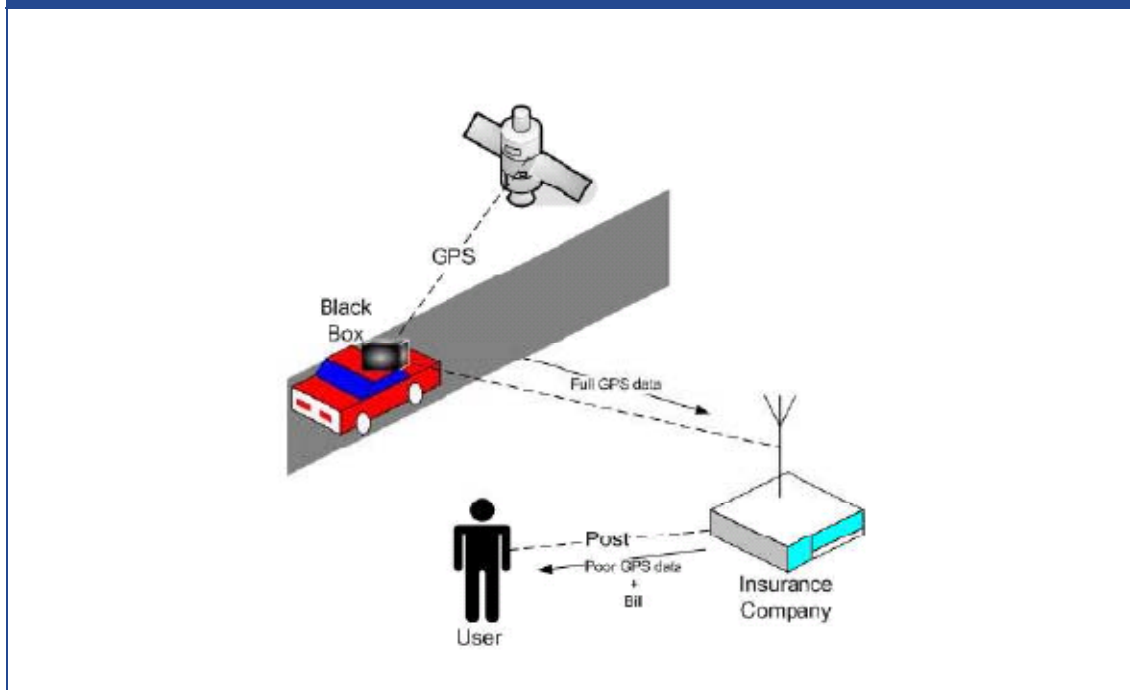
Pay-as-you-drive (PAYD) car insurance is a form of insurance in which premiums are calculated based on usage parameters. At the most basic level, premiums are based on vehicle-kilometres as measured by the car's odometer. The advantage to the policyholder of the PAYD model compared with traditional car insurance lies above all in its greater fairness, in the sense that drivers who use their car more face a greater risk of accident and thus should pay more for insurance. As PAYD discourages car use, it can be argued that it also has wider benefits to society, ranging from fewer traffic accidents to lower levels of environmental pollution.

From the insurers' point of view, the advantage lies in the fact that individual risks can be priced more accurately the more relevant information is known about policyholders' driving habits. In addition, the PAYD also allows insurers to reduce risks through tariff-driven behavioural changes. This implies that insurers' are potentially interested in all types of information that can be used to predict risk, specifically the roads used, time of day, vehicle speed, etc. In practice, this means that many providers of PAYD insurance collect not just the distance driven by policyholders, but considerably more detailed information as well.

Troncoso et al. (2007, 2008) divide the types of PAYD products available in Europe into three categories according to the degree of privacy invasion involved:

- The first category consists of policies under which (not privacy-invasive), vehicle-kilometres (not location specific) are collected once or twice a year from a fixed location; other systems also check via GPS that drivers adhere to the speed limit of a given road, but without recording the location. Only few of the available products fall into this category.
- In the second category (medium privacy-invasive) are policies that involve the collection of location data. Odometer readings are taken at fixed points for example at petrol stations or through receivers placed by the roadside. Other systems in this category offer discounts for drivers prepared to provide more extensive information such as length and timing of individual journeys, time/date of data download, vehicle speed, and driving behaviour (sudden starts/stops).
- In the category with the highest degree of privacy invasion are policies that require constant transmission of detailed data from a GPS device ('black box') installed in the policyholder's car to the servers of the insurance company. Some of these systems collect very extensive data, including not only vehicle position and speed, but also seatbelt use, rate of acceleration, observance of traffic signs, etc. This data is collected even though not all of it appears to be used in the premium calculations. A schematic depiction of this type of system is shown below.

Figure 25: Current PAYD model



Source: Troncoso et al. (2007)

PAYD insurance schemes create a large volume of data related to policyholders' driving habits and travel patterns. The data can be stored and used by insurance companies, but might also be passed on to third parties. Although PAYD car insurance currently remains a niche product, it has clear potential to take over a much larger share of the car insurance market in the future.

### Other applications

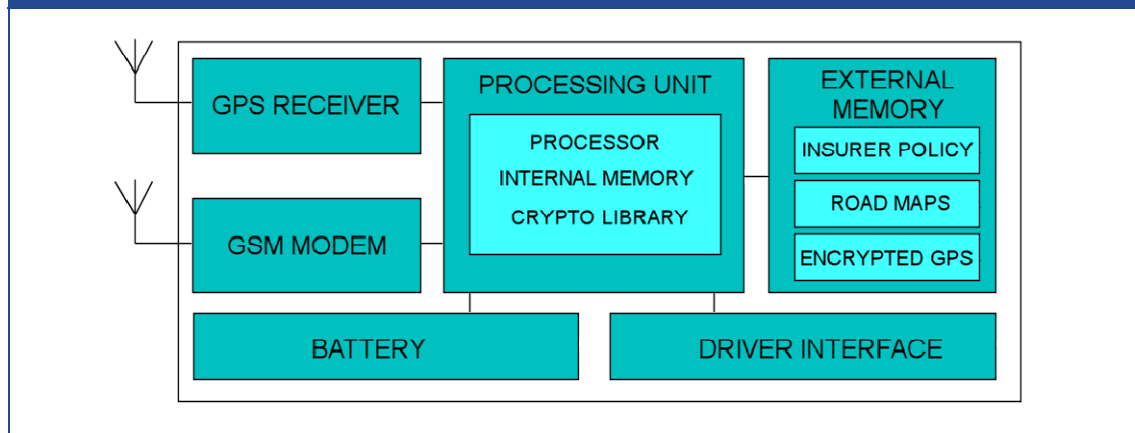
The PAYD concept – i.e. charging users proportionally to their road use – can also be adapted for use in road charging applications.<sup>80</sup> The system functions exactly like the insurance application described above. Recording usage information, either at fixed data collection points or via GPS devices can be varied according to route, time of day, type of vehicle, etc.

### 5.3.2 The PET

PriPAYD eliminates the need to transfer sensitive personal data in the context of a PAYD insurance scheme. PriPAYD achieves this by moving the storage and processing functions from an external server that can be accessed by the insurance company (and possibly other parties as well) to a black box inside the policyholder's car. The functions/components of the black box are shown below.

<sup>80</sup> See Balasch et al. (2010).

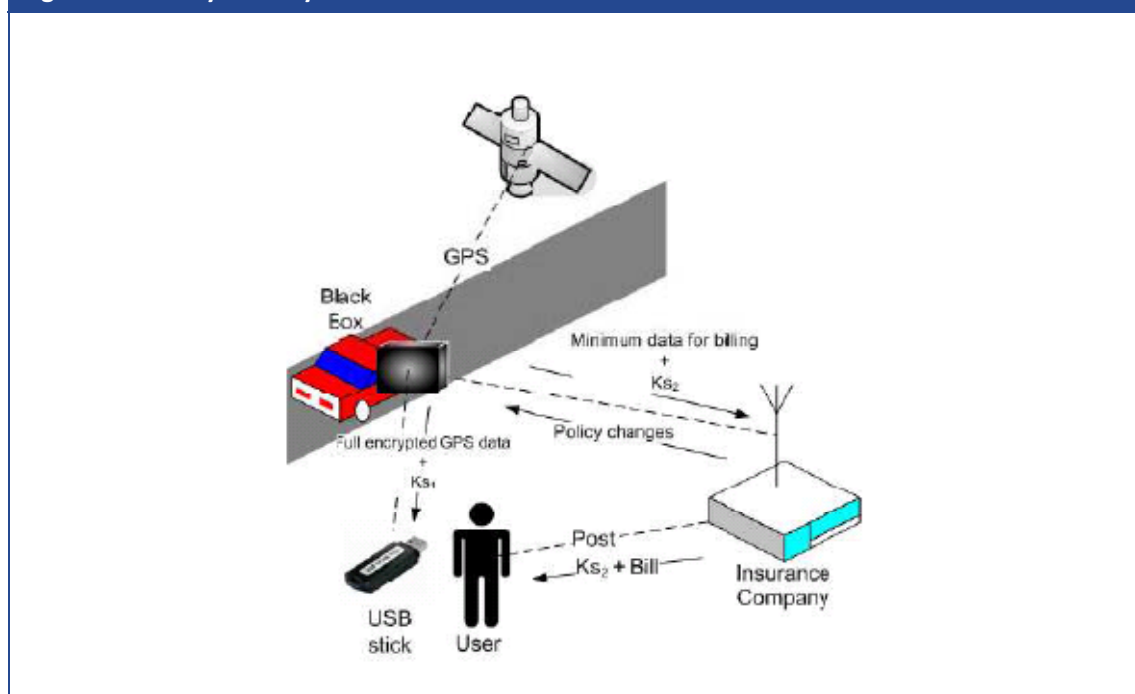
Figure 26: Black box, high-level specification



Source: Balasch and Verbauwheide (2009)

The entire calculation of the premium takes place in the black box according to the tariff set by the insurer (the tariff is installed on the black box and can be securely updated). The costs for each trip are calculated in real time and later aggregated into a final premium. Only the final premium is transmitted to the insurer, for example via GPRS or text message (SMS). For further security, the system uses public-key encryption in all transmissions and the policyholder is able to verify that only premium information is submitted. The system is illustrated in Figure 27 below.

Figure 27: Privacy-friendly PAYD model



Source: Troncoso et al. (2007)

In the PriPAYD model, only the policy-holder has access to the location data that are saved in the black box. To enable users to check that their premiums are correctly calculated, Troncoso et al. envisage that the data can be downloaded on a standard USB memory stick, again encrypted, with the key provided only to the policyholder. This feature also allows the policyholder to monitor the driver (where the two are not identical).

An important design feature is that PriPAYD does not require third-party certification. Even though the policyholder cannot easily discern how exactly the black box in his car operates, he can monitor the data saved on it and the data sent to the insurance company. However, users still have to trust that the black box functions in the way specified, i.e. that no hidden data exchange with the insurance company or other parties takes place.

PriPAYD thus combines data minimisation (pre-usage PET) and usage PETs including a verification mechanism and secure data transmission. PriPAYD enhances individuals' privacy by preventing casual and mass surveillance by insurance companies (or third parties who could gain access to the data, either through leakage or by buying it from an insurance provider) as well as aggregation (combining the datasets of multiple policyholders) and data mining of the resulting centralised databases.

PriPAYD currently exists only as a concept, which places it at the start of the S-curve tracing the adoption rate over time.

### **Costs**

As PriPAYD has not been implemented commercially, an exact cost comparison between existing models and PriPAYD is impossible. However, Troncoso et al. (2007, 2008) argue that the implementation of PriPAYD could be cost neutral.

In particular, the authors argue that, although PriPAYD requires a more capable black box than current systems as more computation takes place inside it, the requirements would be comparable to those of other commercial in-car GPS devices. The system would moreover use only existing, off-the-shelf technologies. The developers estimate a cost of less than € 50 per box in mass production.

A further source of savings compared with the status quo is communications. As only billing data is transmitted, the volume of data traffic decreases considerably.

However, potentially the largest cost advantage over current system lies in the savings that come from a less complex back-office function. As less data is handled, and the data that is handled is less sensitive, the cost of ensuring secure storage and processing is likely to be considerably lower with PriPAYD.

### **5.3.3 Discussion**

#### ***The need for PETs***

The collection of data on personal car usage represents a serious risk to privacy. Based on such data it is possible to construct detailed profiles of individuals' lifestyle and their daily routine.



However, there is no evidence that privacy concerns have hindered the development of PAYD insurance in Europe. One insurer (who is no longer offering the product for reasons unrelated to privacy) told us that they were not aware of any privacy concerns from their customers. Another insurer does not even list questions about privacy among the 23 “frequently-asked questions” on its website.<sup>81</sup> Of course this does not prove that there is no customer pressure for more privacy.

However, the fact that there are a number of insurance providers currently offering PAYD vehicle insurance without PriPAYD or similar systems in the European Union suggests that demand for PriPAYD or similar solutions is unlikely to come from consumers. Incentives to introduce PriPAYD must come either from insurers themselves, or be provided by government.

At the moment, it seems that privacy-invasive implementations of PAYD insurance are not usually considered to fall foul of data protection legislation. The following table lists seven different PAYD products that were sold in EU Member States in 2007 and vary in terms of their privacy-invasiveness. All of these were ostensibly deemed legal under current data protection legislations.

| Table 16: Please use sentence case |         |                           |                       |
|------------------------------------|---------|---------------------------|-----------------------|
| Provider                           | Country | Method of data collection | Privacy invasiveness* |
| 1                                  | NL      | Odometer read yearly      | No                    |
| 2                                  | DE      | GPS                       | No                    |
| 3                                  | ES      | Full GPS data             | Yes                   |
| 4                                  | UK      | Full GPS data             | Yes                   |
| 5                                  | IT      | GPS                       | Yes                   |
| 6                                  | NL      | GPS                       | Yes                   |
| 7                                  | AT      | Full GPS data             | Yes                   |

Note: \* assessment of privacy-invasiveness as per Troncoso et al. (2007).

Source: Based on Troncoso et al. (2007), Table 1

### Effect of PETs

Our discussion of the effects of PETs in this case is qualitative as PriPAYD has not been implemented and no data on costs and benefits for data controllers and other implications of deployment are available.

As discussed, neither consumer pressure nor enforcement of data protection legislation is currently providing enough pressure to drive deployment. However, the developers of PriPAYD argue that deployment would not be more costly than the systems currently in place, and might even lead to savings as data minimisation lowers the administrative costs. If this is true, this could place PriPAYD in the category of ‘positive sum’ PETs, i.e. technologies that enhance users’ privacy while also benefiting data controllers. So what is holding back deployment, apart from the fact that the technology is new and untested and therefore represents a risk for first-movers (a problem shared by all new technologies)?

<sup>81</sup> [http://www.coverbox.co.uk/your\\_questions.php](http://www.coverbox.co.uk/your_questions.php).

One problem with the technology is that, by depriving insurance providers of information about their policyholders, it may impede the design/adjustment of PAYD policies.<sup>82</sup> The reason why PAYD is potentially cheaper than traditional insurance is, after all, the fact that more information is used in the risk calculation. If less information is made available, this could lead to sub-optimal policies, which would hurt insurers as well as policyholders. However, we have no information on the magnitude of this potential cost. The developers of PriPAYD believe that detailed GPS data is not required for the calculation of existing policies. It should also be noted that PriPAYD does not preclude the voluntary disclosure of personal information, possibly in exchange for extra discounts, etc.

On the other hand, PriPAYD might confer a competitive advantage even in the absence of consumer switching. If the processing of details location data is not *strictly necessary* for providing PAYD insurance, collecting such data becomes *excessive* and is thus not permitted under the Data Protection Directive. Deployment of PriPAYD could then render all more data-intensive PAYD products excessive at a stroke, leaving competitors no choice but to adjust their systems and leading to a significant first-mover advantage for the first deployer.

This has potential market power implications (an entrant offering PriPAYD could de facto force competitors to adopt similar measures), but at the same time this danger should encourage PETs adoption. However, this depends on how data protection legislation is interpreted and enforced with respect to PAYD insurance.

### ***The role of the public sector***

The discussion above shows that the public sector can play a crucial role in promoting PETs deployment. First, given the existence of highly privacy-invasive PAYD policies in various European markets, there seems to be a need to clarify data protection legislation in this area and/or to improve enforcement.

Secondly, the public sector can promote PET adoption by pioneering privacy-friendly technologies such as PriPAYD, for example in the road pricing schemes that are currently being considered across the EU. In the Netherlands, a privacy-friendly road-pricing scheme similar to PriPAYD is being implemented with government support.<sup>83</sup> Another possibility is mandating the use of these technologies in the franchise contract in cases where the running of road-pricing schemes is contracted out to the private sector.

Demonstrating the usefulness of PriPAYD in such a way can overcome a crucial initial barrier to deployment, namely the uncertainty associated with new technologies. Once the system is demonstrated to work, this leads to progressively more firms adopting the technology (the adoption rate moves up the S-curve). Official certification schemes might constitute an important mechanism for raising awareness of the usefulness of privacy-friendly technologies in this area.

---

<sup>82</sup> One insurer we spoke to suggested that data GPS data collected from PAYD customers had been used in the design of policies.

<sup>83</sup> See <http://tinyurl.com/y9sor75>. Full implementation of the scheme is planned for 2018.

### 5.3.4 Summary

PriPAYD may offer a ‘positive sum’ solution to the problem of privacy-invasive implementations of PAYD insurance. The fact that companies offering such insurance have not yet adopted privacy-friendly technologies may be due to cost, although the developers of the technology argue that PriPAYD would be at least cost-neutral. If this is the case, the reluctance of businesses may be explained by the uncertainty surrounding the replacement of a proven technology (conventional PAYD insurance) with a new concept that has not been market-tested.

On the other hand, it is possible that insurers are currently benefiting from the ability to exploit the data on their PAYD customers, for example through better policy design. However, there are indications that at least some schemes collect an excessive amount of data even if these benefits are real. The question whether potential losses in functionality are outweighed by savings made as the need for safeguarding sensitive data disappears with PriPAYD cannot be answered a priori. However, it should be noted that PriPAYD leaves open the possibility for individuals to disclose more data voluntarily, in exchange for compensation (e.g. discounts on their premium).

There is no doubt that PAYD insurance in its current form is highly privacy-invasive. The public sector thus has a role to play in insuring that data protection legislation is respected. Cooperation with the private sector, for example by implementing privacy-friendly technologies in privately road-pricing schemes could serve to kick-start wider adoption in the private sector. The specific barriers to introducing a new PET to the market increase the role of information campaigns and official certification schemes.

## 5.4 Case study III: Pseudonymisation services

This case study analyses a company (here called ‘Company A’ for confidentiality reasons) that specialises in providing pseudonymisation services to public sector data controllers in the Netherlands, specifically organisations operating in the healthcare sector.

The key finding is that PET deployment is driven primarily by the legal requirement to comply with privacy law and enforcement through costly fines for non-compliance. This level of legal enforcement is fairly unique to key public services such as healthcare (and areas such as education) as privacy law distinguishes the severity of privacy risk in these sectors from others in the economy.

### 5.4.1 The application

In the Netherlands, GPs, hospitals and health insurers are required by law to provide patient medical information to national registers. Company A facilitates this data exchange via privacy enhancing technologies (PETs). These aim to preserve the privacy of patients and prevent organisations from misusing patient information. In addition, the creation of anonymised individual-level datasets permits the analysis of epidemiological trends, medical care prices and outputs in ways that were not possible previously. At present, Company A serves over 20 clients, consisting of: 2 large organisations (with over 250 employees each), 3 medium-sized organisations (with over 100 employees each) and over 15 medium and small organisations (with less than 100 employees each).

### 5.4.2 The PET

Company A provides “pseudonymisation” services for a variety of data controllers within the healthcare sector that are obliged by law to submit data to national registries. These services permit its clients to make data submissions to national registries in a pseudonymised form, which is a requirement of the national data protection authority.

Consistent with principles of data minimisation, the pseudonymisation service provided by Company A operates only with fixed data definitions that match the legal definitions of data that its clients must submit to national registries. This ensures that no information is unnecessarily transmitted.

A software module is installed at the client site in order for the first transformation of personal identifiers into a pseudonymised form to take place. The rationale for installing the software module at the client site is to ensure that no personally identifiable information is unnecessarily transmitted. This is in line with national data protection authority requirements for which options such as web-based data transfer methods are not permitted.

Once the initial transformation of personal identifiers into a pseudonymised form has taken place, it is encrypted and transferred to Company A’s pseudonymisation server. The transmission of the data in encrypted form makes it difficult for an unauthorised party to utilise the data at this stage. Company A’s pseudonymisation server is then responsible for producing the final irreversible pseudonyms.

While data is transmitted through Company A’s pseudonymisation server, technical measures have been taken to ensure that staff within Company A cannot access client data: (i) the pseudonymisation algorithm is held within a “black box”; (ii) “reverse engineering” personal identifiers is made prohibitively difficult as one would require access to the pseudonymisation algorithms, knowledge of the computing environment, the configuration of the environment and digital certificates to conduct it; and (iii) the division of labour within Company A implies that the number of individuals required for collusion to take place is likely to be too large for it to be feasible.

Company A also takes measures to reduce the probability that datasets are de-anonymised. To reduce the threat of de-anonymisation attacks, Company A creates “target specific” pseudonyms. These are pseudonyms specific to organisations receiving data from a client that make it problematic for third-parties to link datasets on the basis of pseudonymised identifiers.

### 5.4.3 Objective of using PETs

Health-sector organisations do not appear to be driven to deploy PETs on the basis of explicit demands being made by individuals or consumer groups for privacy. The driver of PET adoption among Company A’s clients appears to be requirement to conform to certain standards set by information security auditors.

There is a large incentive to adopt PETs when organisations fail to comply with information security standards because continuing non-compliance beyond a grace period leads to hefty fines

in the order of € 2,000 per day. While fines are not frequently levied, their magnitude is likely to be a large enough deterrent for firms to adopt PETs.

#### 5.4.4 Effect of PET

##### **Cost of compliance**

In order to avoid having to pay hefty daily fines, close to 20 health sector organisations have utilised Company A's pseudonymisation service, which consists of a quick scan report and pseudonymisation software. The quick scan report describes the data being exchanged between health sector organisations. This report is recognised by data protection authorities and auditors, which is useful to prove compliance with data protection laws. The software module, which is custom-built and installed for operation on each client site, is provided alongside ongoing support and software maintenance services. The total cost of this package is in the region of € 75,000 in year one and € 35,000 in subsequent years (for larger organisations). Table 17 below provides a breakdown of the various component costs.

| Table 17: Indicative cost of pseudonymisation services |           |
|--------------------------------------------------------|-----------|
| <b>Fixed costs</b>                                     |           |
| Quick scan report                                      | € 10,000  |
| Pseudonymisation software                              | € 30,000  |
| <b>Variable costs</b>                                  |           |
| Annual license fee                                     | € 10,000  |
| Annual fee for data exchanged                          | € 25,000* |

Note: \*Pay-as-you-go or pre-paid options are available for data exchanged, with pre-paid customers receiving a discount per unit of data sent or received. Most public sector clients tend to select the pre-paid contract option because of fixed budgets and large volumes of data that need to be transferred.

Source: London Economics

As the equation below shows, the cost of the PET (including initial costs and recurring annual costs) is equivalent to the total fine incurred over a period of 37.5 days.

$$\frac{\text{Cost\_of\_PET}}{\text{Daily\_fine}} = \frac{€75,000}{€2,000} = 37.5\text{days}$$

##### **Cost sharing arrangements**

Given the nature of the service provided – with data being protected both within organisations and as it is transmitted between them – and the large costs associated with the service, organisations deploying PETs strike various contracts to allocate costs.

Some larger organisations internalise the entire cost of the pseudonymisation services, thereby subsidising its free use for counterparties sending/receiving encrypted data. Other organisations split the cost equally or proportionately between them.

**Research benefits of PETs**

Organisations are incentivised to adopt PET because they would be unable to use individual-level datasets for the purposes of conducting analysis of epidemiological trends, medical care prices and outputs otherwise.

This is not possible without PETs as only aggregate data could be used without breaching privacy laws. The analysis that one client of Company A was able to conduct because of the deployment of PETs directly contributed to it receiving a government grant of “tens of thousands of Euros” according to a Company A representative.

**Competition**

There are small- and medium-sized organisations that are excluded from reaping the research benefits outlined above. Company A has attempted to market its products to small- and medium-sized healthcare and scientific research organisations that have smaller budgets. However, it was observed that the initial costs of the uptake of pseudonymisation services were too large for them to bear. This limits the number of firms within the research sector competing for funding grants, which could have an impact on the quality of research produced. In response to this, Company A is developing an “off-the-shelf”, lower cost, version of its pseudonymisation service that may be financially more accessible.

**5.4.5 The role of the public sector*****The current role of the public sector***

The public sector, through the enforcement of privacy law is a major driver of the deployment of PETs. As outlined above, the threat of sanctions that exceed the cost of the PET after a period of 37.5 days creates a large incentive for health organisations to deploy PETs.

In general, the national data protection authority operates with reference to ISO:27001, which sets an international standard for information security management systems. The standard specifies that personal information should be anonymised such that it cannot be observed directly in a dataset. In addition, it should not be possible to combine information from multiple datasets in order to reveal personal information.

More specifically, privacy law in the Netherlands further stipulates that PETs must be used in certain sectors where “sensitive” information is held, including the healthcare sector. This suggests why the vast majority of Company A’s 20 plus clients are in the healthcare sector and a minority are in other sectors where sensitive information is also involved, such as education.

***The potential future role of the public sector***

In order to facilitate the conduct of research by organisations that have access to detailed medical data, there may be an additional role that the public sector could play by subsidising the cost of PETs for organisation that might not be able to bear it independently/alongside a larger partner organisation, serving to create a more competitive research environment. The rationale for this type of public intervention is that research that may not have otherwise taken place becomes feasible through the subsidy.

In addition, the public sector could also have an insurance role to play. The reliance of several, key health sector organisations on Company A for pseudonymisation services creates a risk of costly business disruption if Company A should cease trading. Company A has taken the initiative to insure against its bankruptcy risk by striking a contract with Company B, which will take over its services in the event of Company A ceasing trading. However, this is an incomplete solution with residual risk. There is no guarantee that the required pseudonymisation service will continue seamlessly, which has the potential to put the privacy of patients at Company A's clients' institutions at risk. In cases like this, where there is a strong element of interdependence between private and public sector actors, there might be a role for the public sector in creating a more complete contingency plan for clients purchasing mandatory pseudonymisation services from the private sector.

#### 5.4.6 Summary

Privacy laws, particularly enforcement through costly fines, drive organisations to adopt PETs. Organisations operating in sectors that use sensitive information are particularly targeted by bodies such as data protection authorities. While the legal mechanism pushes organisations to adopt PETs, pull factors are also at play. In particular, coordination between multiple organisations facilitated by PETs has allowed for new, individual-level datasets to be created that permit more sophisticated analysis of the healthcare sector. Some smaller research organisations may not be in a position to adopt PETs and this could prevent them from conducting valuable research. The public sector may have a role in addressing this problem through the specific provision of a grant to encourage PET deployment. In addition, the public sector may have a role in minimising the consequences of bankruptcy (and the associated research costs) of companies such as Company A.

### 5.5 Case study IV: location-based mobile services

Recent years have seen a steep rise in the use of location-based services such as driving directions, weather forecasts and tourist information that are accessible through wireless devices such as mobile phones. With a wide variety of application providers developing these services (particularly with a large amount of open source software development taking place) there is a concern that data controllers, whether it be application providers or mobile network operators, are in a position to engage in privacy violations. This is particularly the case with the development of ever more sophisticated location-based services that require greater volumes of personal information in order to be effectively utilised. Privacy-enhancing technologies that are capable of managing the transmission of this information in a way that is consistent with individual privacy are desirable because of the growing level of interest in location-based services.

The interesting aspect of this case study is the public-private funding partnership through which the PET was *developed* – involving the European Union Framework Programme for Research and Technological Development (FP6) and a major European mobile network operator (i.e. the data controller). The motivation of the data controller to participate in this scheme appears to have been a desire to comply with privacy law, particularly in an attempt to anticipate the future demand for location-based services that would necessarily require PET deployment.

While this is encouraging from a privacy perspective, there may be competition issues relating to competitors who are unable to afford PETs and therefore unable to compete in the provision of location-based services. To address this effect, there may also be a role for the public sector in not

only encouraging PET development but also PET *deployment*, thus creating a level playing field in the market for cutting-edge location-based services.

### 5.5.1 The application

“Location-based services” (LBS) is a term used to describe mobile applications such as driving directions, weather forecasts and tourist information provided through wireless devices. The deployment of LBS typically involves a mobile network operator carrying information between application providers and users. It transmits information on users’ location and other attributes to the application provider which, in-turn responds to user requests via the mobile network operator.

The use of LBS carries privacy risk insofar as data controllers have access to information relating to users’ movements, which can potentially be used to identify users’ identities for the purposes of abusing private information. For instance, if a user accesses LBS primarily from their home, a data thief can potentially use a public address book to personally identify the user. This information, the combination of the user’s contact details and usage habits, can be sold on to third-parties that may provide the user with intrusive marketing materials. In order to comply with data protection laws, privacy enhancing technologies are therefore required to minimise the processing of personal data while maintaining the functionality of the LBS.

### 5.5.2 The PET

The PET developed for the purposes of LBS is a “location intermediary” component introduced in between the mobile network operator and the application provider that uses a system of pseudonyms aimed at ensuring data controllers only receive the information that is necessary for the provision of their service and the basic privacy principle of data minimisation, according to which “personal data must be [...] adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed”<sup>84</sup> is respected.

Upon subscribing to the desired location-based service and configuring his or her privacy policy, the user transmits a service profile to the intermediary, who stores user information in an obfuscated form, i.e., in a form such that the intermediary is able to match incoming data from the user with data from the application provider via a static pseudonym (pseudonym 1) – while withholding the identity of the user. One of the key benefits of this set-up is that all application providers are hosted by the same location intermediary such that a uniform system of consent and privacy policies can be utilised.

A second transaction pseudonym (pseudonym 2) provides further pseudonymity for the user as a new transaction pseudonym is generated for each information exchange, thereby making it more difficult for application providers to link a series of information exchanges with a single user. In the case of satellite navigation systems, for instance, a new transaction pseudonym might be generated for each road direction. In a densely populated area, in which a given satellite navigation system is being used by multiple users simultaneously, tracking individual users may be prohibitively difficult.

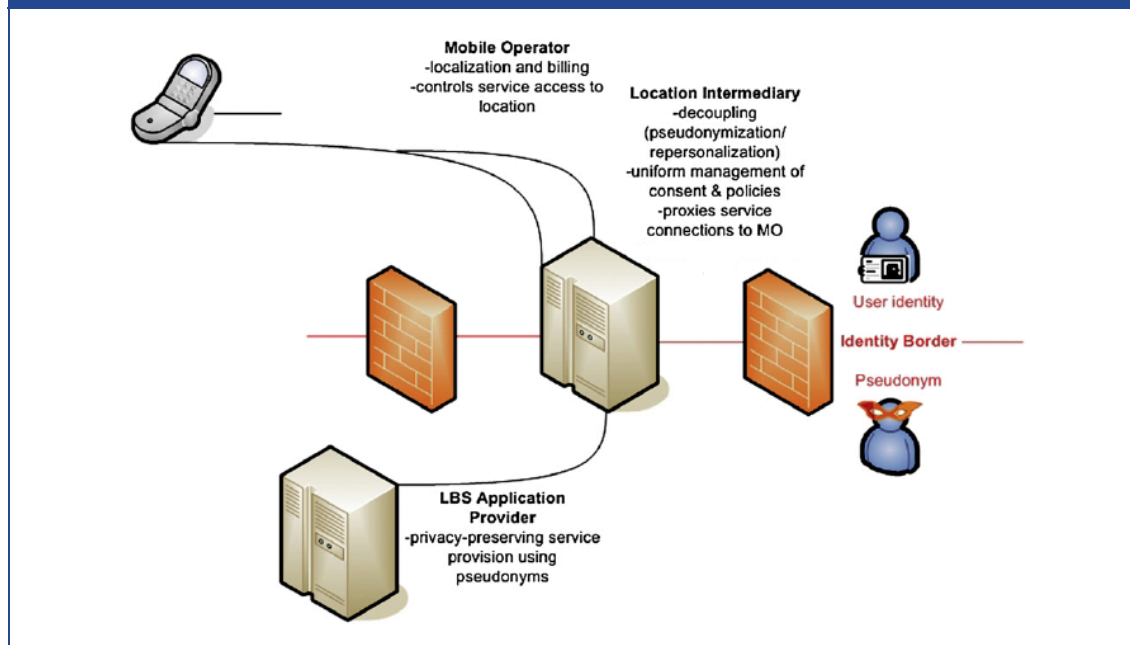
---

<sup>84</sup> Article 6(1)(c) Data Protection Directive.



The schematic in Figure 28 shows, generically, the information flows between users, data controllers and the location intermediary. Table 18 and Table 19 show how the use of the PET transforms the typical information distribution that arises with the use of LBS.

**Figure 28: LBS with location intermediary**



Source: Kosta et al. (2008)

**Table 18: Conventional LBS deployment distribution of information**

| Mobile network operator                                                                                                                                                                                                                                                                                                                                                                                         | LBS application provider                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>■ Contract data <ul style="list-style-type: none"> <li>– Name</li> <li>– Address</li> <li>– Phone number</li> <li>– ...</li> </ul> </li> <li>■ Position (at any time mobile device is switched on)</li> <li>■ Time of localisation</li> <li>■ IP-address</li> <li>■ Billing address</li> <li>■ Service profile information</li> <li>■ Transmitted information</li> </ul> | <ul style="list-style-type: none"> <li>■ User identity <ul style="list-style-type: none"> <li>– Name</li> <li>– Address</li> <li>– Phone number</li> <li>– ...</li> </ul> </li> <li>■ Position (while using service)</li> <li>■ Time of localisation</li> <li>■ Mobile operator</li> <li>■ Service usage patterns</li> </ul> |

Source: Kosta et al. (2008)

**Table 19: LBS partitioned information**

| Mobile network operator                                                                             | Location intermediary                                                                    | LBS application provider                                                                                  |
|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>■ Contract data</li> <li>■ Position (at any time)</li> </ul> | <ul style="list-style-type: none"> <li>■ Corresponding pseudonyms (1 &amp; 2)</li> </ul> | <b>Bound to static pseudonym 1:</b> <ul style="list-style-type: none"> <li>■ Intermediary used</li> </ul> |

|                                                                                                                                                                                                                                 |                                                                                 |                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mobile device is switched on) <ul style="list-style-type: none"> <li>■ Time of localisation</li> <li>■ IP-address</li> <li>■ Billing address</li> <li>■ Price category of services used</li> <li>■ Intermediary used</li> </ul> | <ul style="list-style-type: none"> <li>■ User location (when needed)</li> </ul> | <b>Bound to transaction pseudonym 2:</b> <ul style="list-style-type: none"> <li>■ Position</li> <li>■ Time of localisation</li> </ul> <b>General knowledge</b> <ul style="list-style-type: none"> <li>■ Subscription type</li> <li>■ Obfuscation of application parameters</li> </ul> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Source: Kosta et al. (2008)

Despite the development of this PET, it has not been deployed on a widespread basis at present. The sections below will highlight the economic considerations that have been made by the data controller in arriving at its deployment choice.

### 5.5.3 The objective of using PETs

The representative of the mobile network operator which had co-developed and deployed the PET stated that his organisation's motivation for PET deployment was driven primarily by legal considerations, particularly compliance with privacy law.

From a business perspective, the mobile network operator wanted to set up a platform for third-party application providers to supply LBS. To do this in a lawful manner, it had to include privacy-enhancing technologies in its platform, creating a "privacy gateway" (a relatively unsophisticated version of the location intermediary described above). The privacy gateway utilises some aspects of the PET outlined above, such as the uniform consent and privacy policy management system, but not others, such as the full suite of pseudonyms.

It was stated that privacy breaches had led to the amendment of privacy law, and that this was the primary driver of the development and deployment of more sophisticated PETs. Therefore, the deployment of the more sophisticated location intermediary will come about if it is mandated by law. This provides an interesting insight into the S-curve, namely that adoption rates of new or sophisticated technologies are initiated by step-wise changes in privacy law.<sup>85</sup>

In regard to consumer demand, the representative stated that consumers display transient, event-driven, privacy concerns around events such as data breaches. But, in general, the view is that consumer demand for mobile services were not driven by privacy considerations.

### 5.5.4 Effect of PETs

From the data controller's perspective the development and deployment of the privacy gateway has been a costly and time-consuming process.

<sup>85</sup> Asdf

**Shared costs**

The cost of the privacy gateway was stated to be “sizeable” but “in-line with the cost of developing any other service it provides”. In this particular case, the development of the PET was 50% subsidised by the European Union Framework Programme for Research and Technological Development (FP6) PRIME project. The research involved in the development of the PET was conducted jointly by the mobile network operator and a university research institute.

**Uncertain benefits**

The eventual deployment of the privacy gateway was a lengthy process. The representative noted that moving from the development phase to the adoption phase can be a “matter of months or even years” depending on the complexity of the PET. This is because while the costs associated with deployment are known, the potential stream of future benefits is highly uncertain. On the one hand, privacy law may become stricter in the near term making it necessary to adopt cutting-edge privacy-enhancing technologies. On the other hand, service providers may not develop applications that require a large amount of personal information and therefore the deployment of sophisticated PETs is not required.

For this reason, the privacy gateway has been adopted by the mobile operator rather than the more sophisticated location intermediary. Using data on service usage arising through these “version 1.0” services, the mobile network operator will be able to determine whether demand is high enough to make it profitable to deploy more sophisticated PETs in the future. Once this is established, the more sophisticated location intermediary will be rolled out.

The lengthy, iterative process of market-testing provides another insight into the slow adoption of technologies that is revealed by the S-curve. It also highlights how the existence of privacy requirements is at odds with the development of applications consumers may potentially value. One example that was cited is a mobile contact book that is integrated with a social networking site to show users who are online/offline. This application has not been rolled out because of legal concerns about the use of personal information.

**Competition effects**

Over time, as services play an increasingly important role for consumers’ mobile experience, the representative argued that the company’s early adoption of sophisticated PETs will put it in prime position to secure growth in its client base relative to other mobile operators. The representative argued that some operators are unable to afford the PETs that are legally required to host sophisticated mobile applications.

As such, privacy law appears to create a barrier to competition by imposing a relatively large cost on smaller mobile operators that prevent them from offering as high-a-quality service to users as its larger counterparts.

**Reputation effects**

The representative also argued that the early adoption of PETs by the company bears it some reputational benefits with data protection authorities. The company is continues to participate in

PETs development under the PICOS project, which is a part of the Seventh Framework Programme for Research and Technological Development.

### 5.5.5 The role of the public sector

At present, the public sector plays two central roles in the adoption of PETs in the mobile telecommunication sector. Firstly, it subsidises the *development* of PETs through the EC Framework Programmes. Secondly, it sets out the legal framework required in order to incentivise data controllers to protect their customers' privacy by *deploying* PETs.

Given the competition effect of privacy law on smaller mobile operators' ability to provide certain services to their users, there also may be a further public sector role in encouraging the deployment of PETs. Grants, for instance, to smaller organisations that must adopt PETs in order to provide LSB could help to mitigate the competition-reducing impact of privacy law. This may become increasingly relevant in the future when location-based services and other optional services drive consumer selection of mobile operators.

### 5.5.6 Summary

The use of privacy-enhancing, location-based technologies is driven primarily by data controllers' need to comply with privacy law and results in better privacy protection for consumers in this expanding market. However, uncertainty regarding the future profitability of sophisticated location-based services results in a slow deployment of PETs of equal sophistication.

As a result, the rate of development of location-based services may be held back, suggesting a role for public intervention. The public sector is currently closely involved in the development of PETs through funding initiatives such as the European Framework Programmes. Concerns that the cost of compliance with data protection legislation might prevent smaller companies from competing effectively in the market for location-based services may suggest a need for public sector intervention to mitigate the potential adverse effect on consumers.

## 5.6 Case study V: CCTV privacy zones

This case study analyses the use of privacy zones in CCTV surveillance. Use of privacy zones is a relatively mature PET which is standard in much CCTV equipment. This is an example of a PET in widespread use, which imposes only minimal additional costs compared with the underlying privacy-invasive CCTV applications. In the present case study, we consider the application of such a PET by the Danish Coastal Authority. In this case the PET was essential for the public authority to be able to realise the benefits of CCTV surveillance. The case thus highlights potential costs and benefits of a mature PET as well how large net benefits of PETs can work as a strong motivator for deployment of PETs.

### 5.6.1 The application

The Danish Coastal Authority (Kystdirektoratet) is a division of the Danish Ministry of Transport that constructs and maintains state coastal protection on the west coast of Jutland; operates harbours; and provides storm surge alerts. Furthermore, the Danish Coastal Authority is responsible for the operation of the locks at Thorsminde Harbour and Hvide Sande Harbour.

The locks at Hvide Sande Harbour consist of a so-called 'drainage' lock and a chamber lock. The drainage lock is used to regulate the content of salt in Ringkøbing fjord to a level of 8-14%. Surveillance of the harbour and the drainage lock is necessary to ensure a safe passage of ships into the harbour.

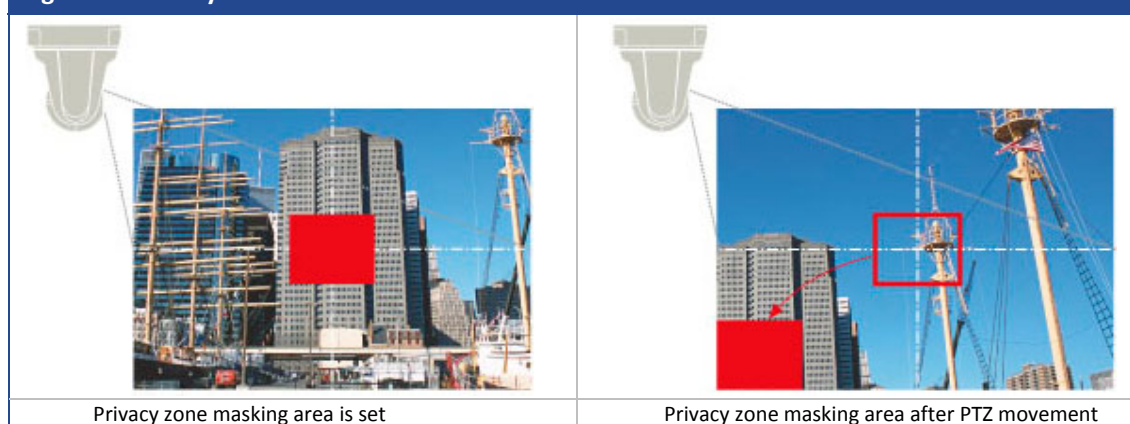
However, traffic in and out of the harbour varies considerably and is very low during night. Therefore, in order to enable staff to undertake other tasks while keeping the harbour and lock under surveillance, the Danish Coastal Authority uses CCTV surveillance.

### 5.6.2 The PET

The CCTV technology used by Hvide Sande harbour comprises a PET which allows blackened privacy zones to be designed on the footage. This means that data collected for images of the privacy areas is masked: no privacy-invasive visual images (e.g. persons going about their daily lives) can be seen by the operators. Moreover, the CCTV images are not recorded, which means data collection is minimised.

The zones are designed in such a way that the areas stay blackened even if the position of the cameras changes. For instance, if a building in the centre of the picture is sensitive and should not be put under TV-surveillance this area can be masked and will stay masked even if the camera is moved to another position implying that the building is no longer at the centre of the picture (as illustrated in Figure 29).

**Figure 29: Privacy zones in CCTV**



Source: Sony Pan Tilt Zoom

Technology for masking of privacy zones is relatively widespread in CCTV equipment and is widely used in a variety of different surveillance applications. Therefore, privacy zones can be viewed as a relatively mature PET (i.e., it is positioned relatively high on the S-curve tracing the take-up rate of the PET).

It is worth mentioning that the specific application of privacy zones used by the Danish Coastal Authority also comprises other privacy enhancing features. For instance, since the masking of privacy zones can only be altered by administrators, the system ensures that access to sensitive footage and data is limited.

### 5.6.3 Objective of using the PET

The overall objective of installing CCTV surveillance at the harbour was to achieve productivity gains by allowing staff to undertake other tasks while keeping the harbour area under surveillance. However, as a general rule, CCTV surveillance of public areas is prohibited in Denmark<sup>86</sup> because it is believed to compromise privacy. Exceptions include surveillance of entrances if the footage is only viewed 'live' and not recoded/stored for later use. Furthermore, there must be strong and objective arguments in favour of CCTV use.

Initially the CCTV equipment used by the Danish Coastal Authority did not include privacy zones. But, after consulting the Danish data protection authority privacy zones were put in place. The purpose of the privacy zones was to ensure that no private houses, gardens and public areas on land were displayed on the footage and that only the sea areas in and around the harbour and drainage locks were visible on the footage. The PET thus protects privacy in a broad sense, i.e. individuals are not being observed in situations considered private. It should also be noted that advances in technology, such as facial recognition software, mean that the threats to privacy from CCTV surveillance are increasing, which is likely to increase the role of PETs in this area. The possibility of defining privacy zones in CCTV technology appears to have been decisive for the approval by the Danish data protection authority in this case<sup>87</sup>.

### 5.6.4 Effect of PET

#### Costs

The costs associated with the implementation of privacy zones in CCTV surveillance systems are minor. For the Danish Coastal Authority, the fixed costs of the appropriate software were in the order of a few hundred Euros while the total fixed costs of the CCTV equipment amounted to approximately € 10,750<sup>88</sup>. Furthermore, there are virtually no on-going costs associated with the PET. It should also be mentioned that there are no other costs associated with the other privacy enhancing components of the system (i.e. non-storage of footage and administer-only access to amending privacy zones) which were also essential for obtaining the approval of the system by the Danish Data Protection Authority. The costs of privacy zones are summarised in Table 20 and amounts to less than 6% of the total costs of CCTV to the authority.

| Table 20: Costs of privacy zones in CCTV systems |         |
|--------------------------------------------------|---------|
| Costs                                            |         |
| Fixed costs                                      | < € 600 |
| Variable costs                                   | € 0     |
| Share of total CCTV costs                        | < 6%    |

Source: London Economics

<sup>86</sup> Ministry of Justice and Data Protection Authority (2008), 'TV-overvågning'. Guidelines on TV-surveillance. Available at [http://www.fpsikring.dk/upload/pjece\\_om\\_tv-overvågning.pdf](http://www.fpsikring.dk/upload/pjece_om_tv-overvågning.pdf).

<sup>87</sup> The approval is available at <http://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/tv-overvaagning-af-hvide-sande-havn/>.

<sup>88</sup> Using the ECB DKK/€ exchange rate of 7.4423 from 4<sup>th</sup> March 2010.

The fact that the costs of the PET are relatively minor may very well explain its high deployment. If the costs of using the PET is low then it is more likely that business and authorities will be inclined to adopt the PET. In the present case, if the cost of installing the privacy zones had been very high it could have implied that the Danish Coastal Authority would not have adopted it and instead would have been forced to abandon use of CCTV surveillance. In addition, widespread deployment of the PET may lead to further cost reductions by allowing firms producing equipment with the PET to achieve economy of scale in the production.

It should be noted, that while the software allowing privacy zones was not pre-installed in the CCTV equipment purchased by the Danish Coastal Authority, in general it is often pre-installed. It is possible that, in the case at hand, the costs of installing the privacy zones would have been even lower if the appropriate software had been purchased at the same time as the remaining CCTV equipment.

In addition to the costs of installing the privacy zones, a considerable amount of time was invested in consultations with first the local police and later the Danish Data Protection Authority in attempts to establish which legal requirements applied and how the CCTV technology should be designed so there were no violations of privacy. Consultations with the Danish Data Protection Authority lasted for about 1 year.

### **Benefits**

The most immediate effect of installing privacy zones were that they ensured the legality of the CCTV surveillance. If privacy zones had not been installed and no other PET had been adopted, this would most likely have implied that the Danish Coastal Authority would eventually have had to abandon CCTV surveillance. Furthermore, it is worth noting that the use of privacy zones in this case did not impair the quality of the CCTV footage for the purposes of safety surveillance because all the relevant (sea) areas were still visible after the privacy zones had been installed. It therefore seems appropriate to attribute the benefits of CCTV surveillance to the use of PETs.

Use of CCTV surveillance enabled the staff on duty to undertake work in locations other than the watch tower while keeping the harbour and drainage lock under surveillance. At the same time, staff at the harbour took on 'sand-testing', which was previously undertaken by other departments of the Danish Coastal Authority. Other new assignments included maintenance, cleaning, data handling and water testing<sup>89</sup>. According to the 2006 Annual Report of the Danish Coastal Authority, the new activities undertaken by staff at the lock and harbour led to productivity improvements equivalent to staff reductions of 7.5%<sup>90</sup>.

An alternative and conservative measure of the benefits arising from the PET is the annual profits from 'sand-testing' which is the most important new activity undertaken by staff at the harbour. Management at the harbour suggested that annual profits from this activity amount to approximately € 13,500<sup>91</sup> implying that the net benefit of the PET amounted to at least € 12,900 in

<sup>89</sup> Danish Coastal Authority, Annual Report 2006, available at [http://www.kyst.dk/graphics/Medie\\_KDI/01\\_om\\_os/01\\_07\\_Politikker%20og%20strategier/web\\_aarsrapport\\_06.pdf](http://www.kyst.dk/graphics/Medie_KDI/01_om_os/01_07_Politikker%20og%20strategier/web_aarsrapport_06.pdf).

<sup>90</sup> Danish Coastal Authority, Annual Report 2006, available at [http://www.kyst.dk/graphics/Medie\\_KDI/01\\_om\\_os/01\\_07\\_Politikker%20og%20strategier/web\\_aarsrapport\\_06.pdf](http://www.kyst.dk/graphics/Medie_KDI/01_om_os/01_07_Politikker%20og%20strategier/web_aarsrapport_06.pdf).

<sup>91</sup> Using the ECB DKK/€ exchange rate of 7.4423 from 4<sup>th</sup> March 2010.



the year of installation and at least € 13,500 in all subsequent years. The two alternative measures are summarised in Table 21.

| Table 21: Benefits of privacy zones |                                                                         |
|-------------------------------------|-------------------------------------------------------------------------|
| Alternative benefits measures       |                                                                         |
| Net profits generated               | > € 12,900 in the first year<br>> € 13,500 per year in subsequent years |
| Productivity savings                | 7.5 %                                                                   |

Source: London Economics

### 5.6.5 The role of the public sector

The role of the public sector in this case is dual. First, the case presented her concerns an application of privacy zones in the public sector resulting in documented productivity savings for this PET adopting authority. Secondly, the public sector played a key role in ensuring adoption of the PET. In particular, the PET was only adopted once the Danish Coastal Authority had consulted the Danish Data Protection Authority. Furthermore, by approving the CCTV surveillance system implemented by the Danish Coastal Authority at Hvide Sande Havn, the Danish Data Protection Authority essentially provides a seal of approval for the privacy zone technology. This may inspire other public and private companies to implement the technology.

However, the case also highlights that there might be problems with the clarity of privacy regulation. In particular, in this case, the initial CCTV equipment installed did not include privacy zones although the Danish Coastal Authorities had been in touch with the local police to enquire about the rules. The PET was only introduced later after resources had to be devoted to consultations with the Data protection authority. Consequently, lack of knowledge and clarity of the relevant privacy regulation seems to have acted as a barrier to the adoption of the PET. Thus, there seems to be scope for the public sector to clarify regulation in the area and through this channel promote deployment of PETs in the area of CCTV.

### 5.6.6 Summary

Privacy zones represent a strong PET, which, by enabling the Danish Coastal Authority to legally use CCTV surveillance, has resulted in clear benefits to the authority. The technology creates blackened areas, so-called privacy zones, in CCTV footage and thus limits surveillance to the relevant areas of the lock and harbour while providing privacy protection.

The use of CCTV surveillance meant that staff could physically be relocated to places where they would be able to undertake other activities without compromising safety in the harbour. The productivity improvements resulting from this were equivalent to staff reductions of about 7.5% and although there were initial start-up costs, these have clearly been outweighed by the benefits. However, the ultimate driver of deployment in this case seems to have been the data protection authority that advised the data controller on the deployment.

Privacy zones are relatively widespread and place high on the S-curve. This is perhaps because the costs associated with the PET are relatively minor and hence are not a deterrent to deployment.



## 5.7 Case study VI: Nightclub fingerprint identification

The case of fingerprint identification at a nightclub in Denmark shows that PETs may help resolve the trade-off between personal safety and privacy. Concerns for safety may induce use of potentially privacy invasive technologies in an attempt to contain the threat. We consider an application in the nightlife industry but the issues are also relevant in relation to for instance security checks in airports.

The present case study illustrates the fact that PETs may play a key role in mitigating privacy concerns while, at the same time, allowing the implementation of potentially privacy invasive technologies that may reduce threats to personal safety. This case study concerns the example of a Danish SME that is using strong PETs to ensure that its customer identification system adheres to data protection laws and to realise economic benefits.

### 5.7.1 The application

Crazy Daisy in Viborg (hereafter Crazy Daisy) is a Danish nightclub that is part of the NOx Network which is a chain of 55 nightclubs in Denmark. Crazy Daisy is located in the provincial town of Viborg and is one of the main nightclubs in the town.

As part of their mission, Crazy Daisy states that they try to offer an environment where ‘adults can meet and be entertained in a happy and safe environment’. In order to ensure this, the nightclub screens potential customers before allowing access to the nightclub. The screening process aims to identify under-aged customers, customers carrying weapons, potentially violent customers, drug users/dealers etc. ID requirements can be used to identify under-aged customers but it is harder to identify potentially violent customers or those likely to bring drugs into the nightclub.

Crazy Daisy has a MasterClub database containing information about customers and in particular about whether they have caused violent or drug-related problems at the nightclub in the past. People who have caused violent or drug-related problems may be banned from the nightclub either by the nightclub or through a police restraining order. A fingerprint identification technology is used to identify customers and link them to information about possible bans in the database. The MasterClub system is thus used in order to improve safety in the nightclub. However arguably the system is also privacy invasive and the use of PETs is necessary in order to ensure that the system adheres with data protection legislation.

### 5.7.2 The PETs

MasterClub is administered by MCB A/S (MCB) and the following personal data is included in the database: name, address, phone number, e-mail address, date of birth, gender, picture, time of entry into the nightclub, fingerprint template, and information about police restraining orders and bans from the nightclub (reason and length). Personal information stored in the MasterClub system as well as CCTV footage from within the nightclub may be shared with the police. Likewise, information about police restraining orders is included in the system. Individuals wishing to enter the nightclub are identified by the system on the basis of their fingerprint.

Due to the sensitivity of the information included in the MasterClub database, the system is potentially highly privacy-invasive. However, while individual identification on the basis of

personal data is required in order to enforce bans from the nightclub, MCB's system also includes PETs in attempts to protect privacy via technical means (e.g. standard information security measures such as encryption) and processes (e.g. time-based limits for data storage).

The fingerprint identification technology in place has been approved by the Danish Data Protection Authority<sup>92</sup>, in part because it contains the following PETs:

- Only 'templates' of fingerprints are stored; full fingerprints are not stored and while templates can be used for identification it is not possible to reconstruct the full fingerprint from the template. Hence there is some level of data minimisation.
- The system includes sticky policies which imply that fingerprints are automatically deleted if a customer has not visited the nightclub within the past 90 days; pictures are deleted if the customer has not visited the nightclub within the past 180 days; other general personal information is deleted 24 months after the most recent visit; information about the length of bans remains in the database for the duration of the ban; information about the reason for bans remains in the database for the duration of the ban unless consent is withdrawn; CCTV footage is deleted after 30 days.
- Usage logging of all access to information in the system.
- Encryption of personal data sent to MCB.
- Firewall protection of access to the database.
- Administrator locked access to information about reasons for bans.

Furthermore, consumers must give written consent to Crazy Daisy before a record can be created in MasterClub and if customers withdraw the consent Crazy Daisy must delete their record from the register (except length of ban, name and address). This can be viewed as a manual sticky policy in addition to the automatic sticky policy included in the system. Customers who do not provide consent are not allowed access to the nightclub.

Finally, the Danish Data Protection Authority was convinced that personal information would be stored at a physically secure location.

### 5.7.3 Objective of using the PETs

One of the key arguments in favour of the MasterClub system was that it would allow the nightclub to base admission on more accurate and better quality data. Crazy Daisy argued that the system would enable a systematic, fair and non-discriminatory way of administering bans from the nightclub. Any person who is not banned according to information contained in the MasterClub system will be allowed access to the nightclub and thus the nightclub does not need to rely on subjective judgments of who might be potential trouble-makers. However, the key drivers of the deployment of PETs in this case were the data protection legislation and privacy concerns among

---

<sup>92</sup> Case description and approval from the Danish Data Protection Authority available at <http://www.datatilsynet.dk/afgoerelser/arkiv-over-afgoerelser/artikel/adgangskontrol-paa-diskoteker/>

nightclub guests. The PETs are indented to mitigate the potentially severe risks to privacy of the fingerprint technology.

#### 5.7.4 Effect of PETs

##### **Benefits**

Since the PETs legalise the MasterClub system all benefits of the MasterClub system can be attributed to the PETs.

##### **Benefits to consumers**

The technology increases the speed of the screening process and reduces the length of queues outside the nightclub meaning that consumers waste less time and become less frustrated while queuing. Furthermore, the number of violent episodes at or in connection with the nightclub decreased. According to local media, both the owner and the police have registered a reduction in the number of violent episodes in and around Crazy Daisy.<sup>93</sup> By improving nightlife safety the system has positive externality effects for non-violent consumers visiting the nightclub. The reduction in criminal behaviour in the nightlife sector mainly arises because the system has a deterrent effect on potential troublemakers. Firstly, it deters some individuals from visiting the nightclub and secondly, those who do visit the nightclub may cut their criminal behaviour.<sup>94</sup>

##### **Benefits to Crazy Daisy**

Clearly, the improved safety may also provide Crazy Daisy with a competitive advantage over other nightclubs by making the nightclub more attractive to potential consumers and thus raising revenues. Further, the management may be able to reduce staffing because the security situation has improved.

Furthermore, the number of verbal and physical assaults on door-staff decreased. This was in part because of a faster screening process (and thus lower levels of frustration); and partly because screening processes are now considered more objective. Consequently, the work environment for staff at the nightclub has improved.

##### **Costs**

The costs to Crazy Daisy include a one-off cost of installing the technology (including the DKK 1,000 (€ 134) fee for the approval by the Danish Data Protection Authority) and operational costs. It has not been possible to fully evaluate the size of the costs and benefits to the nightclub of the MasterClub system and in particular of the PETs but since the approval of the system by the Danish Data Protection Authority the system has been adopted by a number of other nightclubs in

<sup>93</sup> DR P4 Midt & Vest, 'Fingeraftryk holder ballademagere væk', 26. December 2009, available at <http://www.dr.dk/Regioner/Vest/Nyheder/Viborg/2008/12/26/095512.htm>.

<sup>94</sup> Justitsministeriet (2009), 'Betænkning om restaurations adgang til identitetsoplysninger på personer med restaurationsforbud', Betænkning nr. 1504.

Denmark. This clearly suggests that there are economic incentives for the nightclubs to install the system and hence that the benefits to the nightclub exceeds the costs.

### 5.7.5 The role of the public sector

The public sector in this case acts as an enforcer of the data protection legislation and this legislation will most likely have had some influence on the implementation of PETs into the MasterClub system. After dealing with the Crazy Daisy case, the Danish Data Protection Authority developed 13 guidelines for nightclubs wishing to establish similar identification systems. These recommendations strongly promote the types of PETs used in the MasterClub system.

Furthermore, since the system has been implemented, the Ministry of Justice has published a report recommending use of the MasterClub system and establishment of a common private register around the core principles of the system. The idea is that this would enable nightclubs across Denmark to gain instant access to information about police bans using the individual's fingerprint and/or personal identification number.<sup>95</sup> The main argument presented in favour of such a system is that it would help ensure certain identification of guests such that banned individuals are in fact excluded from the nightclubs.

However, opponents of the idea of a common private identification system using fingerprint technology have argued that it is excessive to record fingerprints (or templates) because alternative and less privacy invasive technologies (such as membership cards) are available.<sup>96</sup>

### 5.7.6 Summary

Fingerprint identification at Crazy Daisy provides an example of how the use of PETs may facilitate use of databases with personal information in small businesses. The interplay of several different PETs in this case was essential in order to obtain approval of the identification system from the Danish Data Protection Authority and therefore to derive benefits from the identification system. The case highlights the possible conflict between personal safety in the nightlife and privacy. PETs may be the solution to this problem.

## 5.8 Summary

The six case studies presented in this section illustrate the diversity of PETs and the way their benefits are dependent on the circumstances of their deployment.

On one hand, this makes it difficult to derive conclusions that are valid for all PETs. On the other hand, however, the case studies highlight a number of key issues that help to explain the current, low deployment levels and offer pointers to areas in which public policy might effectively serve to increase the level of privacy protection offered by data controllers. A high level summary of the results of the case studies is provided in Table 22.

---

<sup>95</sup> Justitsministeriet (2009), 'Betænkning om restaurations adgang til identitetsoplysninger på personer med restaurationsforbud', Betænkning nr. 1504.

<sup>96</sup> Danish Biometrics, 'Når teknologiforståelsen mangler', 12. September 2009.

Although not a new insight, an important lesson from the case studies is that individuals do indeed face substantial threats to their privacy from a number of sources. Personal data ranging from movement patterns to medical histories and genetic information is customarily collected and stored by data controllers across a wide range of industries, from nightclub operators and insurers to mobile phone operators and pharmaceutical companies.

The ubiquity of services that require personal data means that individuals in practice often have little choice over whether to disclose personal data or not as not doing so would result in considerable inconvenience or prevent them from using certain services altogether. This means there is a clear need for PETs across a wide range of applications. The examples presented here show that most PETs are composite technologies that use simple security measures (encryption, access management) in conjunction with other mechanisms to enhance overall privacy.

Data minimisation is a very important aspect of PETs that is realised to varying degrees in the technologies we analysed. Out of the six examples, PriPAYD and CCTV privacy zones are the purest data minimisation tools. Other PETs (privacy-enhanced LBS, patient data pseudonymisation, fingerprint identification) reduce the personal data requirement of the associated applications, but leave a considerable amount of personal data at the disposal of the data controller.

Mechanisms to obtain consumer consent seem play a relatively minor role. Only in the GENOMatch example (and to some extent in the fingerprint identification example) does an individual's consent feature prominently in the design of the PET. That consent mechanisms are relatively underdeveloped is on the face of it surprising given the prominence of the consent requirement in data protection legislation.

Obtaining consent, possibly repeatedly, is a technical challenge as it requires a feedback loop between data controllers and individuals. The requirements in terms of bandwidth and individuals' engagement in the process are considerable.

The development of PETs that minimise explicit consumer involvement in the decision as to whether or to what extent personal data is used can be seen as a consequence of the technical difficulties in implementing effective consent mechanisms (in particular, the lack of user friendly interfaces). While this undoubtedly represents an increase in convenience compared with more consent-oriented PETs, it is questionable whether this approach is effective in allaying consumer concerns about privacy. Lack of transparency regarding data use continues to be a challenge not sufficiently addressed by many mainstream PETs.

PETs are application-specific. While some (GENOMatch being the best example) have been designed to fit a narrow purpose (i.e., enabling privacy-enhanced pharmacogenetic research in the context of pharmaceuticals development), many others can be used in a broader range of applications. Which type is more likely to be used by data controllers is a priori unclear.

While multi-purpose PETs might be cheaper (due to economies of scale in their production) than customised PETs, their deployment might require greater creativity on the part of the data controller in order to make sure they are used effectively. The use of highly focused PETs, on the other hand, while possibly more expensive, is likely to be easily understood by data controllers, which facilitates effective deployment.

A related lesson is that PETs do not have to be complex. The ideas behind PriPAYD and CCTV privacy zones are in fact extremely simple: in both cases, the PET simply suppresses the collection of sensitive personal data by the data controller. (Note that ‘complexity’ here refers to the concept of the PET, not the technical details of its implementation. While the idea of privacy zones in CCTV images is very simple, the technology behind them is very sophisticated.)

It also appears that simple PETs, which do not reduce the functionality of the application they are used with, face no opposition from data controllers. The best example in the case studies is GENOMatch, which seems to have no downsides for the data controller and has already been widely deployed as a consequence.

That technologies such as privacy zones are easy to understand and implement might also mean that they spread more easily. They move up the S-curve more rapidly. The differences in maturity between the different technologies discussed in the case studies suggest that the development of adoption rates over time may be technology-specific. More complex technologies (such as GENOMatch and privacy-enhanced LBS) are likely to be adopted at a slower rate, as the learning process for data controllers is more involved.

Our case studies illustrate clearly that data controllers are often reluctant to deploy PETs. The main reasons are a perceived lack of benefits (GENOMatch, privacy-enhanced LBS) and the potential for diminished usefulness of personal data if PETs are deployed (PriPAYD). An important insight, confirming the views of many stakeholders, is that consumer pressure typically is not an important driver of PETs deployment. Intermediaries, such as ethics committees in the GENOMatch case study, on the other hand, can play a very important role in incentivising PETs deployment.

The case studies also provide strong evidence that the role of the public sector is very important: a lack of enforcement of existing privacy rules and/or inadequate sanctions for infringements appears to depress deployment rates in many cases.

The requirements for consent and proportional data use in particular appear insufficiently enforced. The case studies (specifically GENOMatch and PriPAYD) also suggest that data controllers in some areas may not be using the best available technology to ensure individuals’ privacy is protected. The need to comply with privacy legislation is often the most effective driver of PETs deployment (e.g. in the patient data pseudonymisation example).

On the other hand, there is evidence (GENOMatch, privacy-enhanced LBS, CCTV privacy zones, fingerprint identification) that the public sector is using a variety of approaches to effectively cooperate with data controllers to increase PETs deployment. This support can range from the endorsement of certain PETs by public bodies (fingerprint identification) to active support of the development of PETs (GENOMatch, PriPAYD, privacy-enhanced LBS), official certification (GENOMatch) and pioneering deployment by public bodies (PriPAYD, CCTV privacy zones). The case studies show that, with the right incentives, data controllers work effectively together with public bodies to spread PETs deployment.

| Table 22: Case studies summary                             |                                                                                                                              |                                                                   |                                                         |                                                          |                                                                           |                                                                                                          |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------------------------------|----------------------------------------------------------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
|                                                            | GENOMatch                                                                                                                    | PriPAYD                                                           | Privacy-enhancing location-based services (LBS)         | Health-sector patient data pseudonymisation              | Privacy zones in CCTV                                                     | Fingerprint identification                                                                               |
| Threat to privacy                                          | Severe                                                                                                                       | Moderate                                                          | Potentially severe (contingent on growth in use of LBS) | Severe                                                   | Moderate                                                                  | Severe                                                                                                   |
| Type of PET (Hacohen classification PU=Pre-usage, U=Usage) | Encryption (U)<br>Data separation (U)<br>Access management (U)<br>Consent (PU)                                               | Data minimisation (PU)<br>Encryption (U)<br>Data verification (U) | Data minimisation (PU)<br>Encryption (U)                | Data minimisation (PU)<br>Encryption (U)                 | Data minimisation (PU)<br>Limitation of use (PU)<br>Access management (U) | Data minimisation (PU)<br>Data quality (U)<br>Encryption (U)<br>Sticky policies (U)<br>Usage logging (U) |
| Maturity (position on the S-curve)                         | (2 successful implementations so far. 1 in progress), constant improvements being reported                                   | Very low (concept stage)                                          | Low (PET developed, adoption low)                       | Medium (widespread deployment among large organisations) | High (widespread)                                                         | Medium (spreading)                                                                                       |
| Cost of PET                                                | ≈ € 250,000 per licence + € 40,000 p.a. for maintenance & upgrades                                                           | ≈ status quo                                                      | ≈ “other mobile services”                               | € 40,000 (one-off) and € 35,000 p.a.                     | Low                                                                       | Medium                                                                                                   |
| Drivers of PET adoption                                    | Pressure by intermediaries (ethics committees, data protection professional, inside the companies and DPAs)<br>Concern about | Enforcement potential competitive advantage                       | Enforcement Potential competitive advantage             | Enforcement Research                                     | DP laws<br>Maturity and low costs of PET                                  | Enforcement Potential competitive advantage                                                              |

|                             |                                                                                                           |                                                                                                                |                                               |                                                      |                                                                                          |                                                                                                         |
|-----------------------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------|------------------------------------------------------|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
|                             | individuals' willingness to participate in studies                                                        |                                                                                                                |                                               |                                                      |                                                                                          |                                                                                                         |
| Benefits to data controller | Potentially lower cost of compliance<br>Legal certainty<br>Prevention of costly delays to clinical trials | Savings compared to status quo (potentially 'positive sum')<br>Potential competitive advantage for first mover | Potential competitive advantage in the future | Freedom to conduct research on individual-level data | Legalises use of CCTV technology and the potentially large benefits from that technology | Potential competitive advantage for first mover<br>Legalisation of benefits to use of MasterClub system |

Source: London Economics



## 6 Business survey

In order to gain additional insights into the economic benefits of PETs, we surveyed the business sector across the 12 selected Member States. In accordance with the terms of reference of the study, at every stage of the exercise, an effort was made to include a substantial proportion of SMEs in the survey sample.

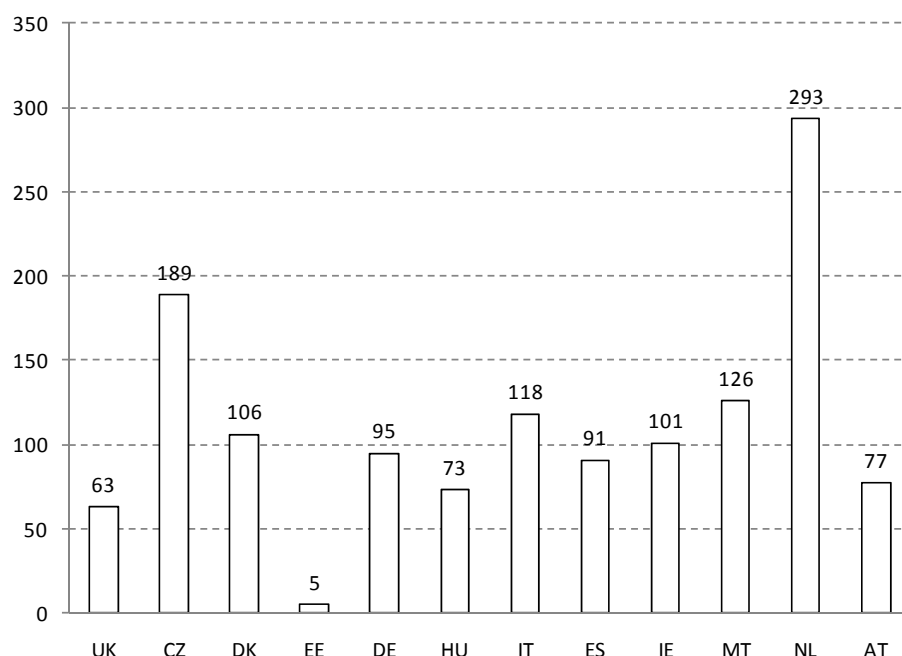
The survey explores the use of PETs and personal data by businesses, as well as their views on the associated costs and benefits. The 16 questions in the survey are presented in 0. The survey was administered between October 2009 and February 2010. Apart from 5 responses from the Netherlands that were submitted on paper, the whole survey was conducted online.

This section first provides summary statistics on the companies that participated in the survey. Next, it describes and analyses respondents' views on, and experience with, the use of PETs in their business.

### 6.1 Response sample and respondent profile

#### 6.1.1 Response sample

A total of 1,337 usable responses were received in response to the survey. The response sample size per country is shown in the figure below. These responses include partial answers, which means that the number of usable responses varies from question to question. A total of 197 answers with no or very little information content (e.g. answers only about the type of data held) were discarded. The sample covers all the 12 Member States selected for analysis (Figure 30), although for most of the analysis responses were pooled.

**Figure 30: No. of responses to business survey per Member State**

Source: London Economics

### 6.1.2 Respondent profile

Table 23 shows that the sample comprises a very broad range of industrial sectors. This is consistent with the aim to gain a holistic view of the role of PETs for businesses. Note that businesses were not preselected on the basis that companies in some sectors, such as ICT, are a priori more likely to use or be aware of PETs. Rather, the assumption is that personal data is increasingly collected and used by all kinds of businesses, including those whose core activity has nothing to do with data processing of any kind. Comprehensive privacy protection can only be achieved with the participation of the business sector as a whole. A narrow focus on businesses with a pre-existing interest in data protection issues would thus have been inappropriate for our purposes.

To achieve consistency in reporting, sectors were classified according to NACE Rev. 1.1. Although services account for the bulk of respondents (sections G to S comprise 84% of the sample), the manufacturing (9%) and construction (3.4%) are also represented. The fact that a large proportion of respondents put themselves in the 'other services' category is common when a relatively coarse categorisation such as NACE sections is used.

**Table 23: Distribution of firms by activity**

| NACE*<br>Section | Sector of main activity                                              | No.   | Perce<br>nt |
|------------------|----------------------------------------------------------------------|-------|-------------|
| A                | Agriculture, forestry and fishing                                    | 19    | 1.4%        |
| B                | Mining and quarrying                                                 | 8     | 0.6%        |
| C                | Manufacturing                                                        | 120   | 9.0%        |
| D                | Electricity, gas, steam and air conditioning supply                  | 24    | 1.8%        |
| E                | Water supply; sewerage, waste management and remediation activities  | 1     | 0.1%        |
| F                | Construction                                                         | 46    | 3.4%        |
| G                | Wholesale and retail trade; repair of motor vehicles and motorcycles | 92    | 6.9%        |
| H                | Transportation and storage                                           | 51    | 3.8%        |
| I                | Accommodation and food service activities                            | 44    | 3.3%        |
| J                | Information and communication technology                             | 148   | 11.1%       |
| K                | Financial and insurance activities                                   | 82    | 6.1%        |
| L                | Real estate activities                                               | 23    | 1.7%        |
| M                | Professional, scientific and technical activities                    | 108   | 8.1%        |
| N                | Administrative and support service activities                        | 93    | 7.0%        |
| O                | Public administration and defence; compulsory social security        | 48    | 3.6%        |
| P                | Education                                                            | 94    | 7.0%        |
| Q                | Human health and social work activities                              | 69    | 5.2%        |
| R                | Arts, entertainment and recreation                                   | 49    | 3.7%        |
| S                | Other service activities                                             | 218   | 16.3%       |
|                  | Total                                                                | 1,337 | 100%        |

Note: \* Rev. 1.1.

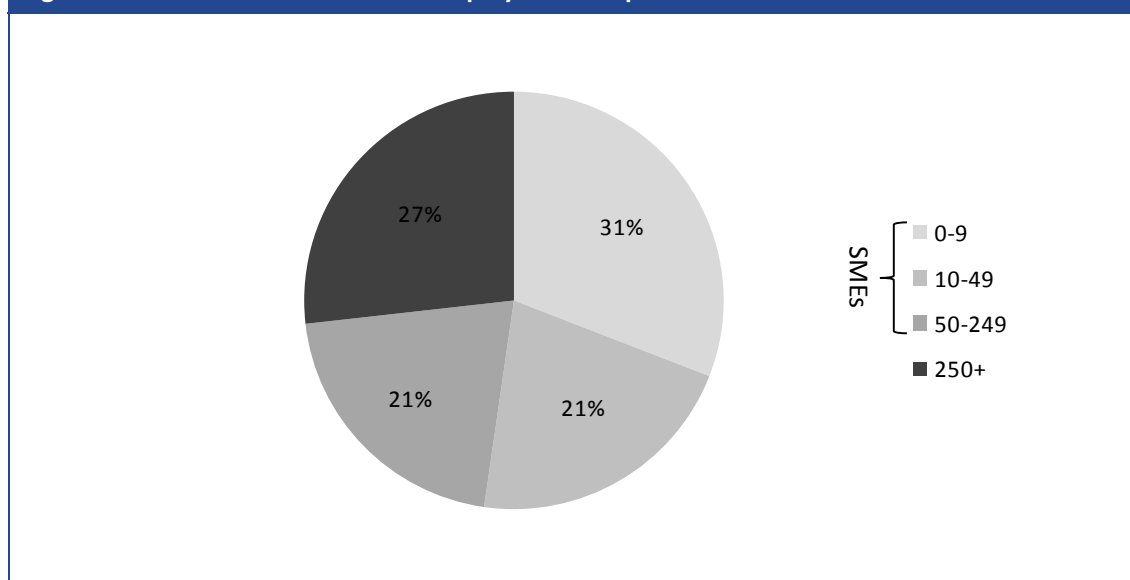
Source: *London Economics*

While the distribution of survey responses across industries varies between Member States, there is no evidence of a systematic distortion or overrepresentation of sectors in specific Member States.<sup>97</sup>

An important objective of the empirical part of the study is to adequately reflect the views and experiences of SMEs, who form the overwhelming majority of businesses in the EU and whose willingness to adopt PETs consequently is indispensable for achieving better privacy protection. 73% of the responses collected in our sample are from SMEs as classified by the number of employees (< 250). As Figure 31 shows, the sample also achieves a good representation of each of the SME sub-classes of micro (<10 employees), small (<50 employees) and medium-sized (<250 employees) businesses.<sup>98</sup>

<sup>97</sup> A cross plot of sectors and Member States is included in 0.

<sup>98</sup> See the EC's definition of SMEs at: [http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index\\_en.htm](http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm).

**Figure 31: Size distribution of no. of employees of respondents**

Source: London Economics

## 6.2 Use of personal information

The view of businesses on PETs will be coloured by the extent to which they use personal data. On a simple level, the more personal data they use in their day-to-day activities, the more important PETs potentially become. In the following figure we show the extent of use of personal information among survey respondents.

As expected, a large majority of around 90% of businesses keep some personal data on customers, staff<sup>99</sup> and suppliers. More than 80% also keep personal information on third parties (in the questionnaire the example of 'commercial databases' was given for third-party personal information; it is assumed this category comprises things such as address lists for direct marketing for example).

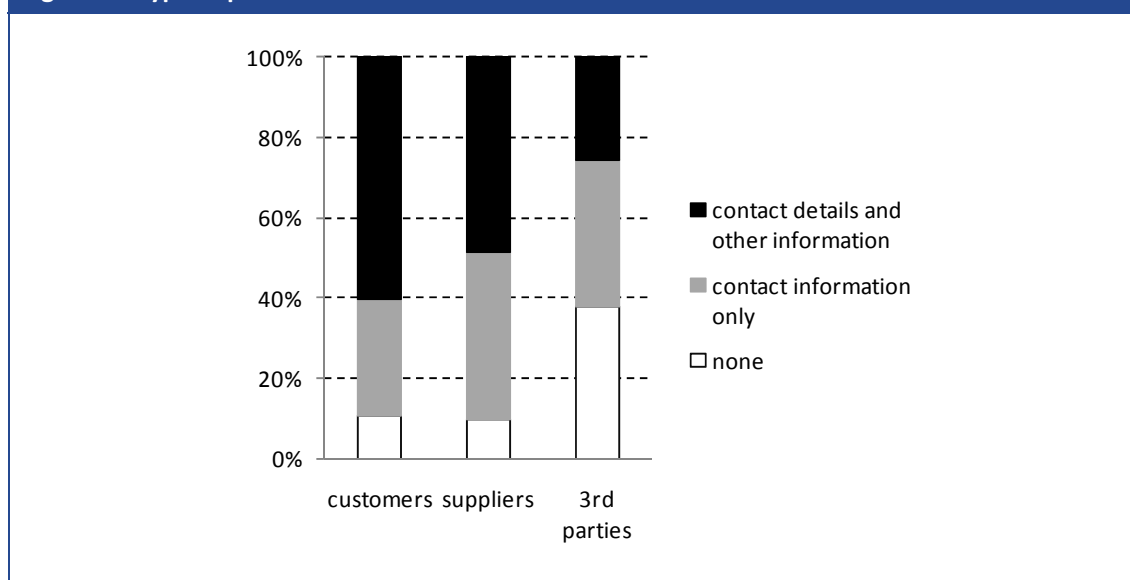
The extent of data use was further explored by asking whether respondents used 'contact details only' or 'contact details and other information'. While this distinction is still relatively coarse, we consider that contact details alone represent a much more limited threat to privacy than more detailed information.

Interestingly, 60% of respondents hold detailed personal data on customers. Personal data on third parties is more likely to consist only of contact details, which could suggest that simple address lists are the most commonly traded form of personal data. However, at 25%, the

<sup>99</sup> Unsurprisingly, most detailed personal data (i.e. 'contact details and other information') is held on staff. This is likely to include data whose collection is mandatory (e.g. payroll information for taxation purposes).

proportion of detailed personal data on third parties that is being kept by businesses is not insignificant.

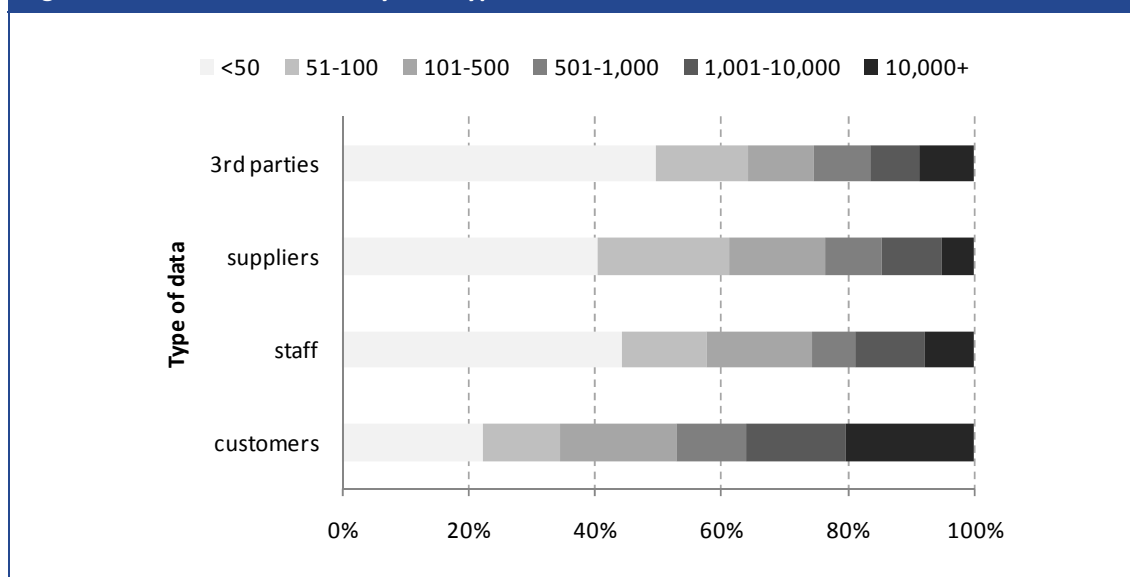
**Figure 32: Type of personal data held**



Source: London Economics

Not only is data on customers typically the most detailed, it is also the type of which companies keep the largest number of individual records. Figure 33 shows that 20% of the databases with personal data on customers contain more than 10,000 records. That the largest number of records is held on customers is not surprising as customers are the largest group of individuals a typical business interacts with. It is nonetheless an important result as it confirms that customers face significant threats to their privacy by companies, including SMEs, across a range of business sectors.

Figure 33: Number of records, by data type



Source: London Economics

Moreover, 87% of databases with more than 10,000 records contain detailed personal data (contact details and other information). The following table shows that there is a moderate positive association between the number of records and the level of detail held on customers ( $\gamma \approx 0.5$ ). We can conclude that where businesses hold a lot of data, they are also likely to store more detailed personal data on their customers than if only small datasets are kept.

Table 24: Relationship between volume and detail of customer data held by survey respondents

| Type of records                     | No. of records |            |            |            |              |            | Total        |
|-------------------------------------|----------------|------------|------------|------------|--------------|------------|--------------|
|                                     | <50            | 51-100     | 101-500    | 501-1,000  | 1,001-10,000 | 10,000+    |              |
| None                                | 23             | 13         | 7          | 2          | 1            | 2          | 146          |
| Contact information only            | 131            | 60         | 76         | 40         | 40           | 31         | 388          |
| Contact details & other information | 118            | 77         | 142        | 95         | 152          | 216        | 803          |
| <b>Total</b>                        | <b>272</b>     | <b>150</b> | <b>225</b> | <b>137</b> | <b>193</b>   | <b>249</b> | <b>1,337</b> |
| <i>gamma = 0.466 ASE = 0.033</i>    |                |            |            |            |              |            |              |

Note: The 'gamma' test statistic (Goodman – Kruskal Gamma) is a non-parametric measure of correlation based on the difference between concordant pairs (C) and discordant pairs (D):  $G = (C-D)/(C+D)$ , i.e. gamma is the surplus of concordant pairs over discordant pairs, as a percentage of all pairs, ignoring ties. Its value ranges between +1 and -1.

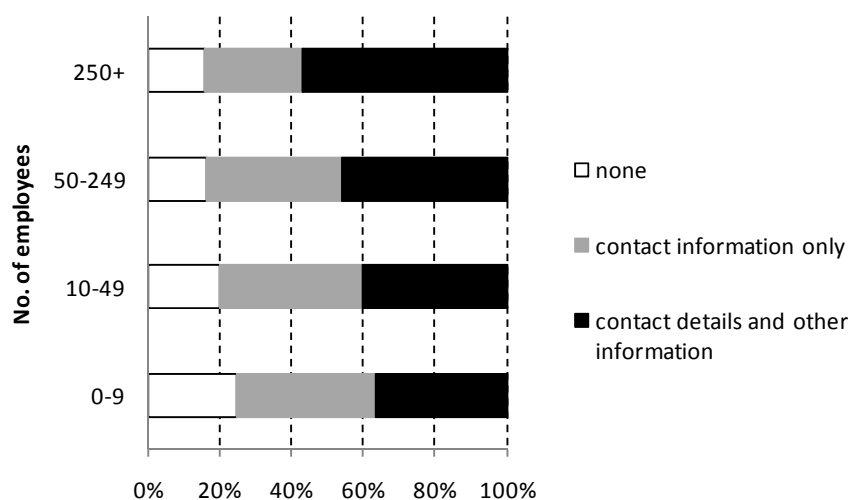
Source: London Economics

### 6.2.1 Size and sector effects

When looking at the types of personal data held by businesses of different sizes, it is evident that there is a clear association between company size (measured by the number of employees)

and data type (Figure 34)<sup>100</sup>. Although business of all sizes keep personal data, smaller businesses keep both less data and less detailed data than larger ones. While only 36% of micro-enterprises (0-9 employees) store more than basic contact details, for the non-SMEs in the sample (> 250 employees) this figure is 57%. That data usage increases with company size is true whether one looks at data on customers, on suppliers or on third parties (the relevant figures are shown in 0).

**Figure 34: Type of personal data (customers, suppliers 3rd parties), by business size**

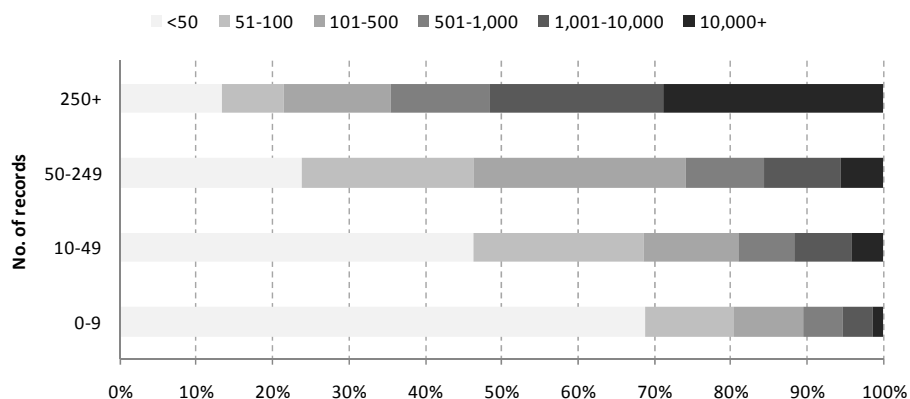


Source: London Economics

In terms of the volume of data held, the difference between companies of different size is even more pronounced. Whereas only 3.6% of the SMEs in the sample hold more than 10,000 records of personal data, for non-SMEs it is 29%. Over 50% of companies with more than 250 employees hold personal data on more than 1,000 individuals.

<sup>100</sup> Data on staff, which clearly correlate with business size, were omitted.

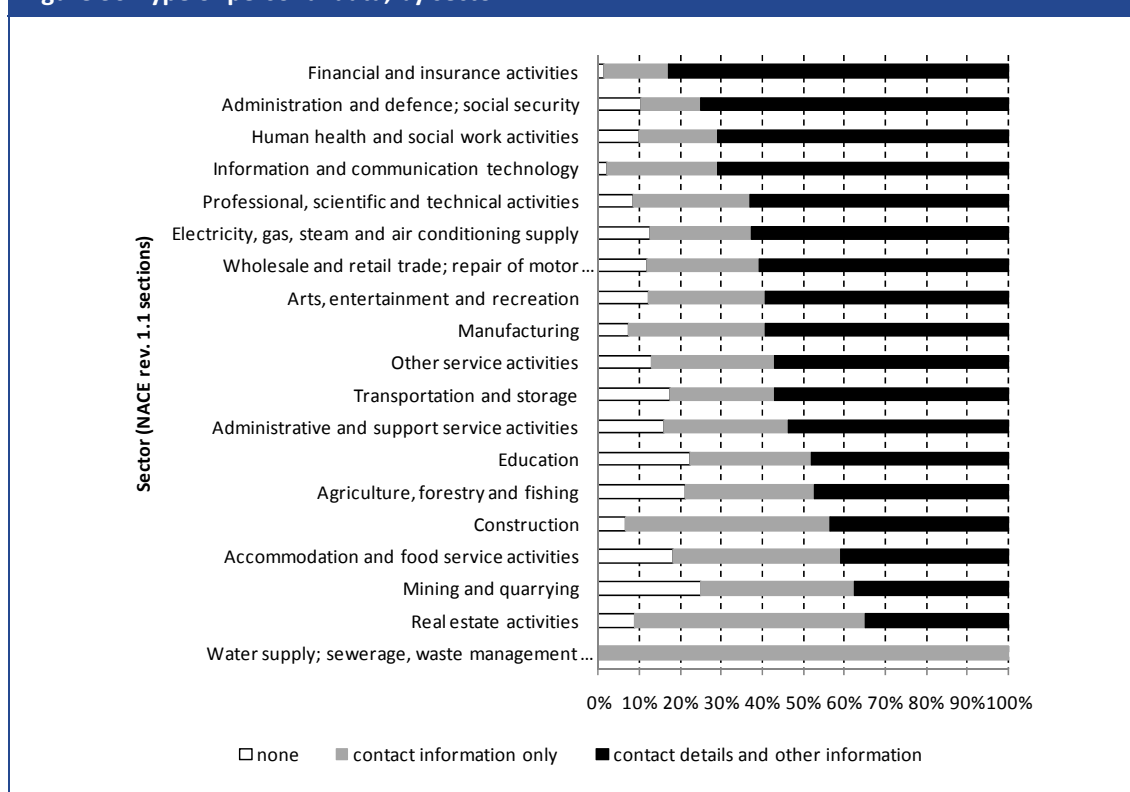
Figure 35: Number of records, by company size



Source: London Economics

When looking at different sectors, one finds that financial services, social services and health-related services, as well as professional and ICT services are most likely to keep detailed personal data. General services activities and manufacturing, which are among the largest categories, are markedly less data intensive. Although the breadth of the sector categories allows only a broad overview, the data suggest that the use of personal information and hence the role for PETs will differ considerably across sectors.



**Figure 36: Type of personal data, by sector**

Note: sectors = NACE (rev. 1.1) sections.

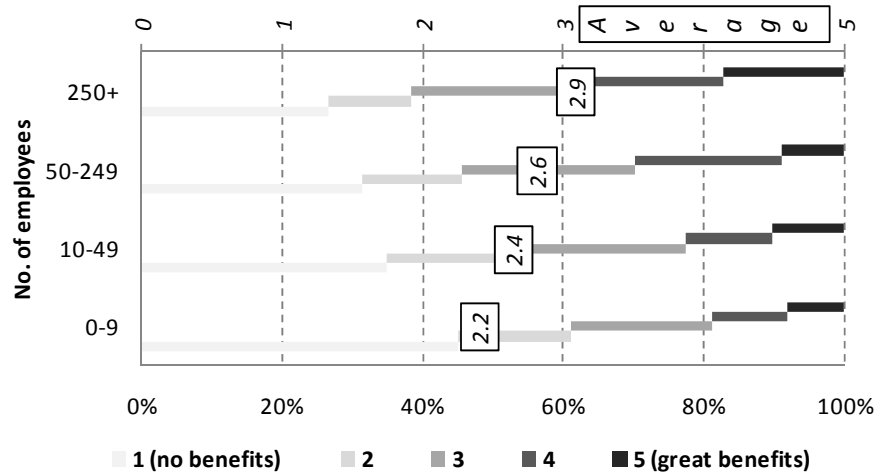
Source: London Economics

## 6.3 PETs and the benefits of holding personal data

### 6.3.1 Benefits

As discussed in Section 3.2, the benefits that data controllers derive from personal data are an important factor in the decision whether to deploy PETs. First of all, PETs, especially those that minimise data collection, have a clear role if data controllers do not benefit from collecting and storing personal data. However, if the data is useful, then the question is whether PETs help or hinder the realisation of the benefits.

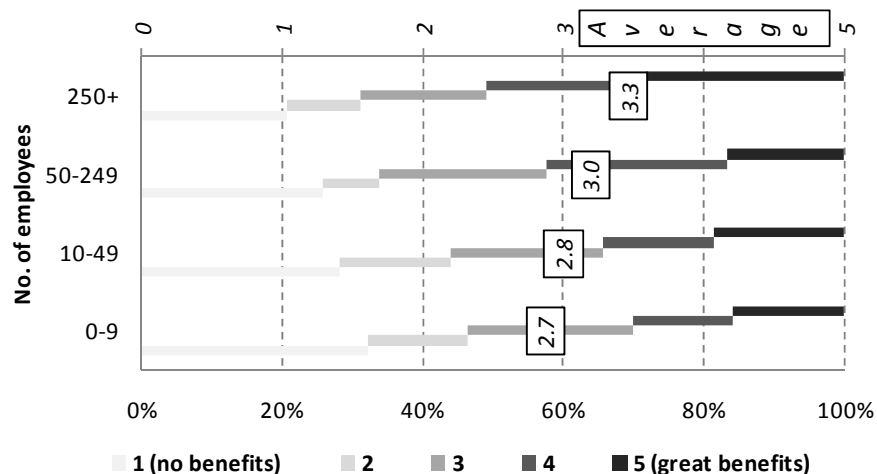
The business survey asked whether businesses currently derive an economic benefit from holding personal data on customers, staff, suppliers and third parties. A summary of the replies is shown in Figure 37. The figure shows that significant minorities of businesses report no benefits from the personal data they hold. Overall, the larger the business, the greater the benefits: looking at the average response (the upper scale in Figure 37) we find low to moderate benefits. All size classes report average benefit scores between 2 and 3 on a 1-5 scale. However, 17% of non-SME respondents report “great benefits” from personal data, while among micro-enterprises this figure is only 8%. Conversely almost half (45%) of micro-enterprises reported that they get no benefit from the personal data they hold, while for the non-SMEs in the sample the figure is only 27%.

**Figure 37: Overall benefit of personal data, by size of data controller**

Note: combined score of benefit from personal data on 1) customers, 2) staff, 3) suppliers, and 4) 3rd parties.

Source: London Economics

A more detailed examination of the results reveals that data on customers is viewed as the most beneficial, with just over half of non-SMEs reporting benefit scores of 4 and 5 (the average score is 3.3, see Figure 38). Lower benefits are reported from data on suppliers, staff and third parties in that order (the detailed figures are provided in 0).

**Figure 38: Benefit of personal data on customers, by size of data controller**

Note: combined score of benefit from personal data on 1) customers, 2) staff, 3) suppliers, and 4) 3rd parties.

Source: London Economics

Excluding sectors with small numbers of responses<sup>101</sup>, the sectors that hold detailed data, such as financial services and ICT services, report relatively average benefits. This suggests that the usefulness of data is sector specific and different PETs may be appropriate depending on the sector. Where businesses gain economic benefits from holding personal data, PETs that allow them to process the data securely are likely to be called for; in industries where the benefit of having personal data is low, on the other hand, data minimising PETs may be more useful.

### 6.3.2 Risks

In the following section, the focus is on businesses that keep personal records on customers. The fact that information on staff and suppliers is often mandatorily kept makes it difficult to infer privacy problems related to these types of data. Businesses are divided into SMEs (< 250 employees) and larger companies (> 250 employees) for the purpose of the analysis in the rest of this section.

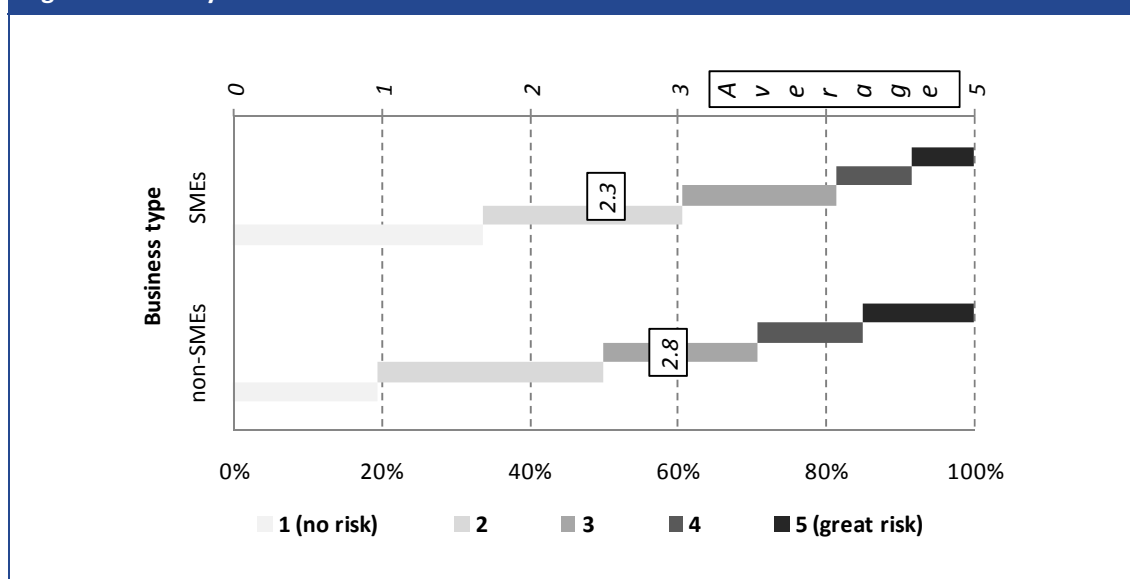
Survey respondents perceive only a low to medium risk of harm to their business due to the misuse of personal data (or the threat thereof). However, larger businesses see the risk as significantly greater than SMEs, with almost 30% seeing the risk as great (5) or moderately great (4).

Larger businesses also report more frequently that privacy concerns (either their own or their customers') have prevented them from developing new business activities in the past (14.2% of larger businesses say this is the case, as opposed to 9.3% of SMEs). However, it is not clear if a greater awareness of the risk led these businesses to apply greater caution, or if experience or past analysis of privacy risks while investigating new business opportunities caused the greater risk awareness.

---

<sup>101</sup> Electricity, gas, steam and air conditioning supply, mining and quarrying and water supply, sewerage, waste management and remediation activities. See 0.

Figure 39: Privacy risk to businesses



Source: London Economics

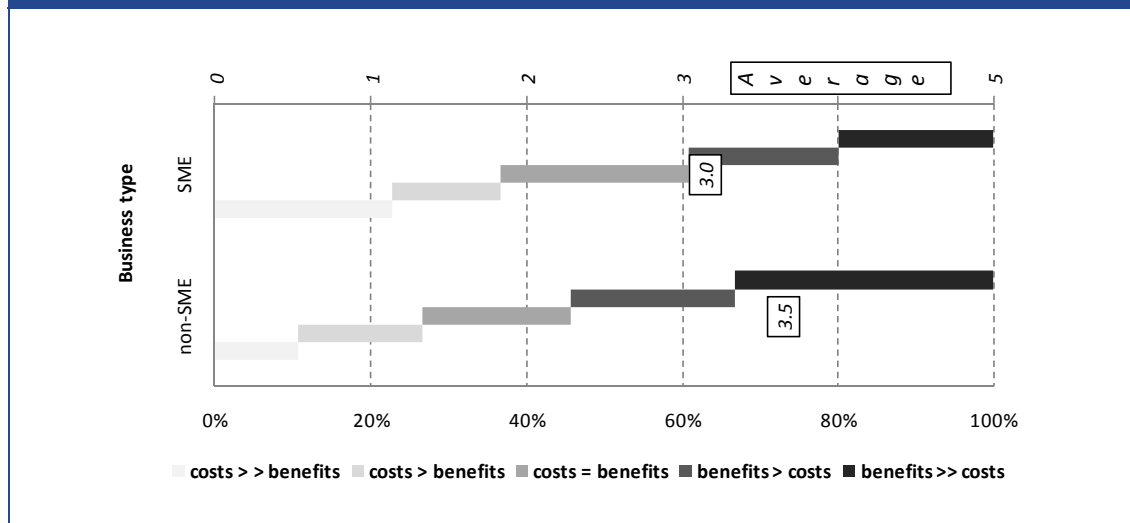
### 6.3.3 The net benefit of PETs

Companies were also asked to judge the net benefit of PETs, taking into account their use of data and the risks they perceive resulting from it. The survey asked respondents to consider specifically how PETs change the cost-benefit assessment of their use of personal data. For example, the benefits a business derives from personal data could be increased through PETs because customers are more willing to provide accurate information than would be the case without PETs. On the other hand, PETs might limit the exploitation of personal data, which may reduce the benefit. Thus, the aim of the question was to make respondents consider the benefit of PETs not in the abstract, but in the context of how they use personal data, which was established in the previous questions.

The responses, summarised in Figure 40, show a clear dichotomy between the views of SMEs and larger companies. On average, larger businesses see greater net benefits from PETs than SMEs. Over half (54%) of non-SMEs see the benefits associated with PETs protection of personal data protected as greater than the costs, with a third stating that benefits are significantly greater. On the other hand, SME respondents are almost equally split between those that see PETs as a net cost (37%) and to those that see them as an overall benefit (39%). A significant proportion of both groups see neither net benefits nor net costs from the deployment of PETs (non-SMEs = 19%, SMEs = 24%).

Overall, the assessment of businesses is positive. Sizeable proportions of businesses, including a majority of the larger companies in the sample, see PETs as overall economically beneficial. However, a significant proportion of respondents remain to be convinced about the economic benefits of PETs. Since smaller enterprises tend to use less data than larger ones, the cost-benefit assessment of SMEs may reflect a lower need for PETs on their part. But, it could also represent a lack of information.

Figure 40: Net economic impact of PETs



Source: London Economics

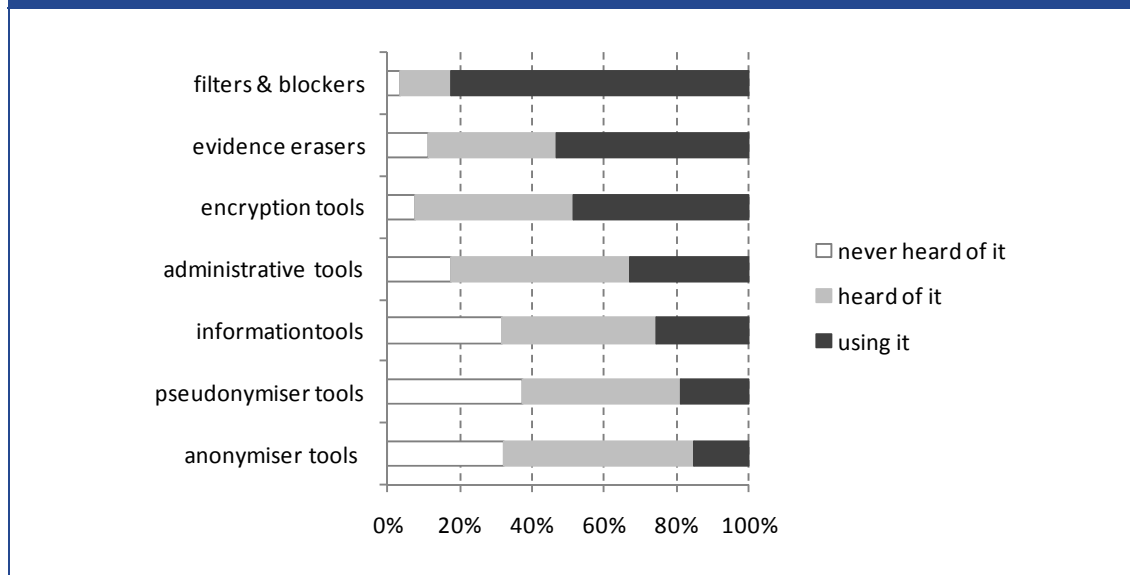
Looking at the awareness among businesses of PETs, one observes that some PETs are widely used and known about, while others remain obscure (Figure 41). By far the most familiar category of PETs for businesses is filters and blockers. Over 83% of the respondents report that they are using these technologies already, with only 3% claiming never to have heard of them. The use of encryption tools (49%) and evidence erasers (53%) is also widespread.

Interestingly, the remaining technologies are also quite well known, but comparatively rarely used. Around half of our respondents report having heard about these technologies (anonymiser tools, pseudonymiser tools, information tools and administrative tools), but considerably fewer are using them. Information tools, pseudonymiser tools and anonymiser tools are the most obscure PETs, with around a third of respondents unaware of their existence.

It is possible that businesses might not be able to classify the PETs they use into the PETs categories provided in the survey. These categories are based on the META GROUP (2005) classification. On the other hand, the lack of awareness could be evidence of a serious information failure, as some of the strongest and most promising PETs seem to be little known.

A comparison of SMEs with larger companies shows a generally higher level of PETs awareness and usage among larger companies. The difference is especially pronounced in the categories information tools and administrative tools, which are used by 55% and 42% of non-SMEs respectively, compared with 25% and 20% of SMEs (see detailed figures in 0).

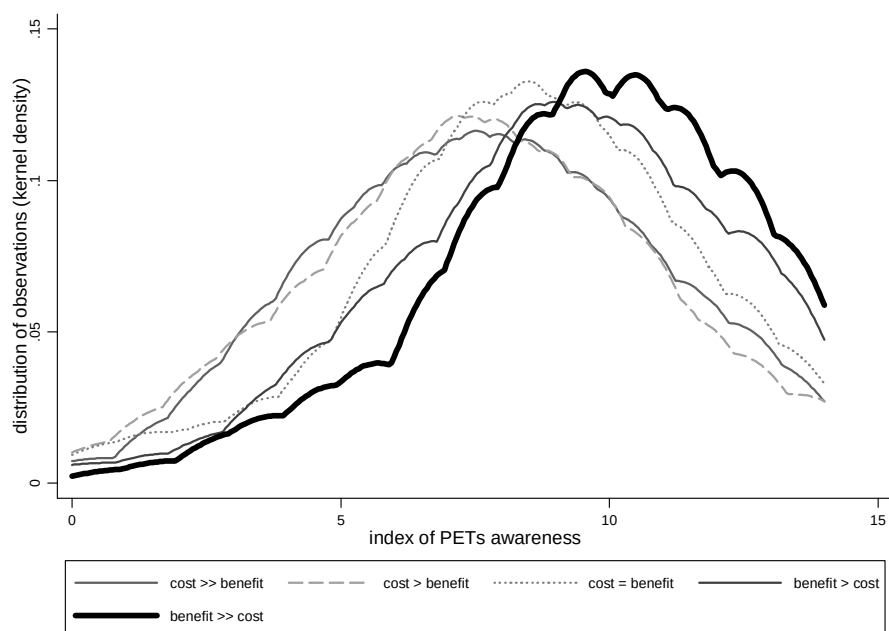
Figure 41: Awareness of PETs



Source: London Economics

In order to explore whether there exists a relationship between awareness of PETs and perceived benefits, the following “awareness index” was created: for each of the seven technologies, 1 is added to the index if the technology is known and 2 if it is being used. This creates an index with a range 0 (the respondent is unaware of all seven types of PETs) to 14 (the respondent is using all seven types). For each level of perceived benefit (1-5), we plotted the estimated distribution across the observed values of the awareness index. The resulting five distribution curves are shown in Figure 42.

Figure 42: Awareness and perceived benefits



Source: London Economics

Each of the five curves represents a distribution of observations<sup>102</sup> over the range of values of the awareness index (i.e. 0-14). The parabolic shape of the curves is reminiscent of a normal distribution, with relatively few observations at the two extremes and the largest number of observations somewhere in the middle. For example, in Figure 42, the maxima of all five curves lie in the region between 6 and 10 on the awareness scale, whereas relatively few observations are on the far right and - especially - left. The slightly skewed shape means that complete ignorance of PETs is rare irrespective of the perceived benefits.

In Figure 42, the two curves furthest to the left are made up of responses saying that the costs of PETs deployment exceed the benefits. That their maxima are to the left of, and lower than, the other curves' shows that a negative view of the benefits of PETs deployment coincides with comparatively low scores on the awareness index. In other words, the respondents with the most negative view of the benefits of PETs deployment know comparatively little about the technologies.

The graph thus shows a clear linkage between the size of the perceived benefits and the awareness of/experience with PETs: the more businesses know about PETs, the greater they judge the benefits of deployment compared with its cost. Companies with the highest valuation of the

<sup>102</sup> Technically speaking, the curves are plots of the estimated kernel densities of the five distributions. These are estimates of the shape of the distributions (more precisely, their probability density functions) based on the finite number of observations in our survey (plotting only actual observations would not result in a continuous curve).

benefits of deployment (“benefits >> costs”) show the greatest awareness (the thick black curve is the one furthest to the right).

The following table shows the perceptions of the impact of PETs on the economic value of personal data for companies that are using at least one type of PET. Large majorities of PETs users report that it is economically rational for them to do so: for 73% of non-SMEs and 64% of SMEs the use of PETs either leaves unchanged or increases the value they derive from personal data.

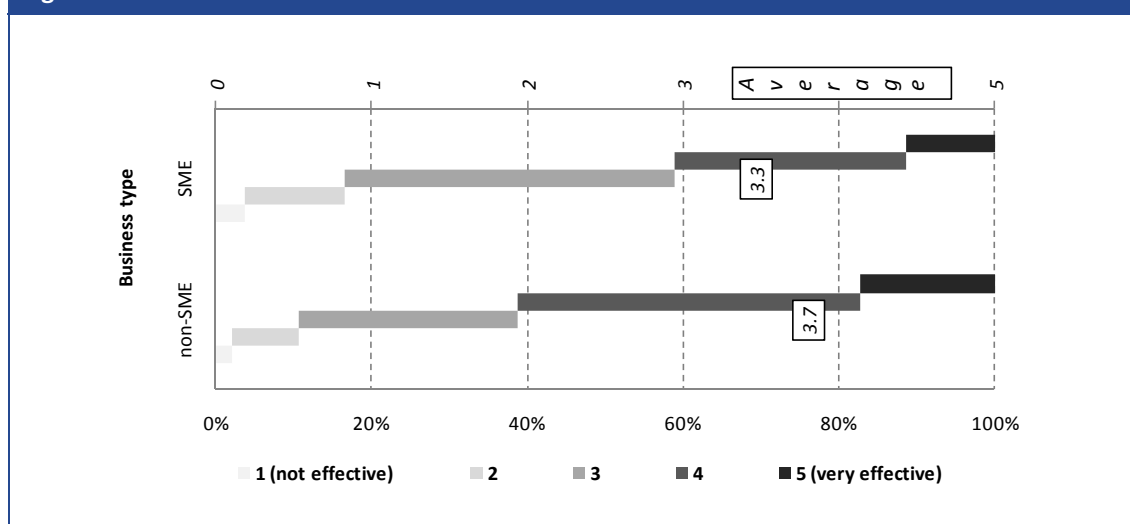
**Table 25: Net economic impact for businesses deploying PETs**

|                   | Non-SME      |            | SME          |            |
|-------------------|--------------|------------|--------------|------------|
|                   | Observations | % of total | Observations | % of total |
| Costs >> benefits | 21           | 10.3%      | 99           | 21.8%      |
| Costs > benefits  | 33           | 16.3%      | 63           | 13.8%      |
| Costs = benefits  | 37           | 18.2%      | 105          | 23.1%      |
| Benefits > costs  | 45           | 22.2%      | 87           | 19.1%      |
| Benefits >> costs | 67           | 33.0%      | 101          | 22.2%      |
| <b>Total</b>      | <b>203</b>   |            | <b>455</b>   |            |

Source: London Economics

The businesses in the sample have an overall positive view of the effectiveness of PETs. Only very small proportions (< 4%) regard them as not effective at all. However, it is noticeable (Figure 43) that larger businesses are much more convinced of the effectiveness of PETs than SMEs, with over 60% giving effectiveness scores of 4 or 5 (“very effective”).

**Figure 43: Effectiveness of PETs**



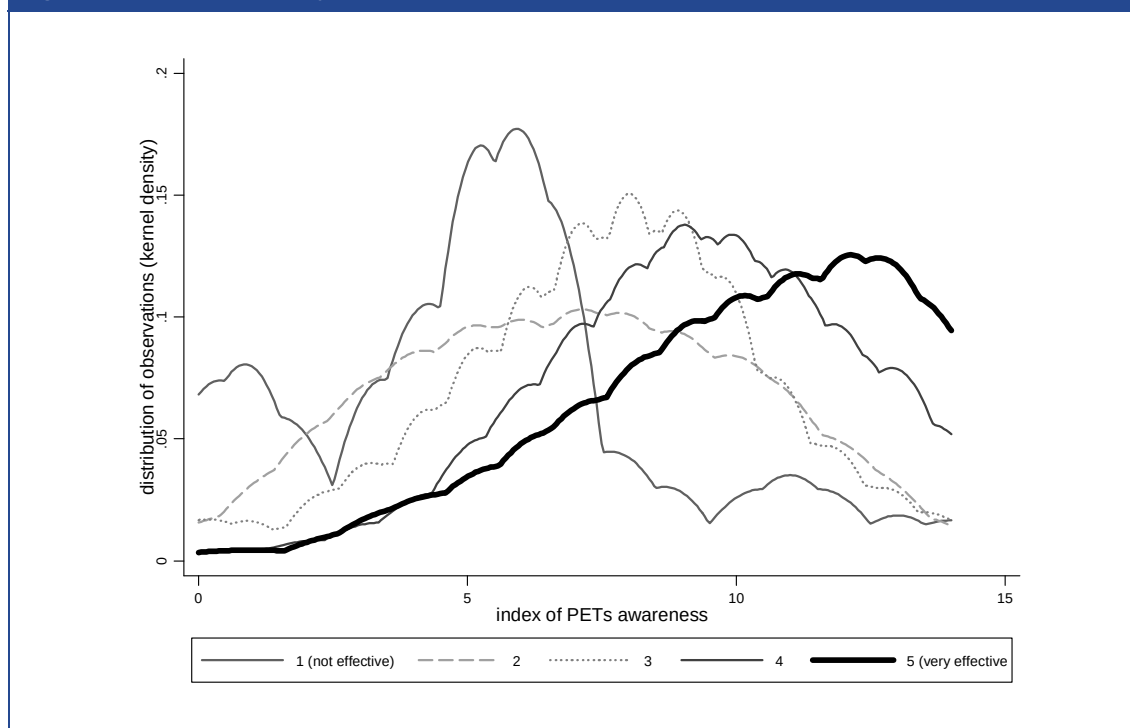
Source: London Economics

A plot of the distribution of responses on the effectiveness question across the awareness index described above reveals the following picture (Figure 44): the more knowledge businesses have of PETs, either because they are using them already, or because they are aware of their existence,



the higher – on average – the rating of their effectiveness. It is remarkable that a relatively large fraction of companies that see PETs as not effective have very little experience of them (the spikes of the ‘not effective’ curve are located to the left on the awareness axis; note, however, that this curve is estimated based on only 30 observations, which contributes to the lack of smoothness of the curve).

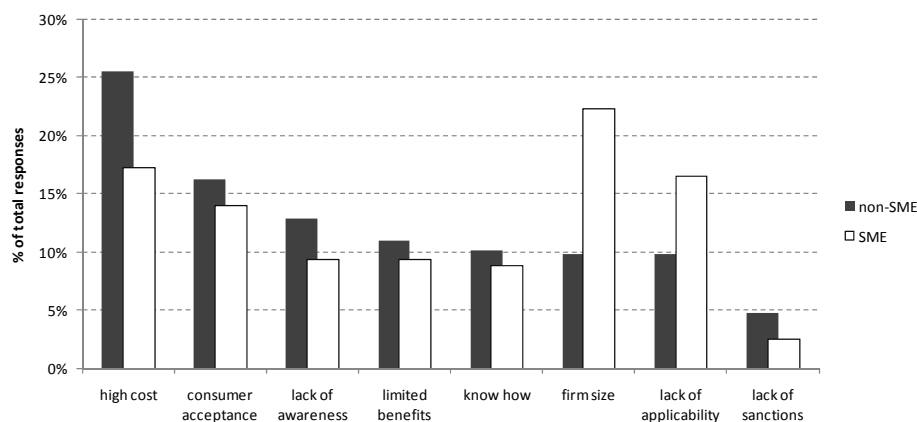
Figure 44: Awareness and perceived effectiveness



Source: London Economics

### 6.3.4 Factors limiting deployment

Finally, the survey looked at factors preventing deployment. The responses show that cost is the major issue for larger businesses, followed by the fact that consumers accept the status quo. In contrast, SMEs report that their decision not to deploy PETs is driven by a perception that these technologies are not applicable to them. That SMEs cite firm size as the most important reason for not deploying PETs could result from the fact that SMEs do in fact use less personal data than larger businesses. On the other hand, SMEs do use significant amounts of personal data (see Figure 34), which might suggest that a lack of awareness of the applicability and benefits of PETs on the part of SMEs is in fact a more important limiting factor.

**Figure 45: Factors preventing deployment of PETs**

Source: London Economics

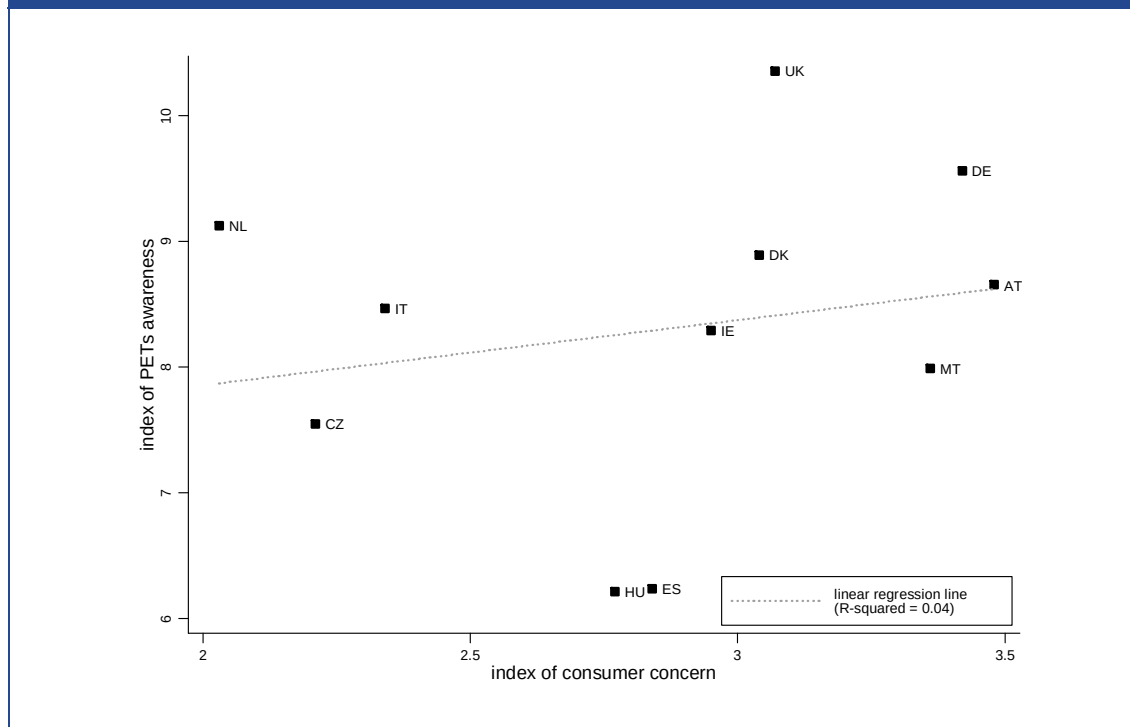
The question whether consumer pressure is impacting on PETs deployment is of great interest from a policy point of view. As Figure 45 shows, businesses often see consumers' acceptance of the current level of protection as a reason for not deploying PETs. An explicit comparison of the level of consumer concerns about data privacy and the awareness/usage level of PETs across countries confirms that consumer perceptions are not a significant determinant of PETs deployment overall.

Figure 46 shows a plot of the values of the awareness index described above (equal to 0 if companies are unaware of PETs and equal to 14 if companies are using all seven types of PETs) and an index of consumer concern. This index was constructed on the basis of results from the 2008 Eurobarometer survey on data protection. The survey asked the question: "Different private and public organisations keep personal information about people. Are you concerned or not that your personal information is being protected by these organisations?" Responses were recorded on a scale of 1 ('not at all concerned') to 4 ('very concerned'). The index in Figure 46 is computed as the average score per country.

Overall, the association between PETs awareness and the level of consumer concern in a country is positive but weak. Companies in countries with very high levels of consumer concern, such as Germany and Austria, use, or know about, PETs more than in most other countries.<sup>103</sup>

<sup>103</sup> However, the example of the Netherlands shows that high levels of PETs awareness can coexist with low levels of consumer concern. Whether this is evidence of a more 'proactive' (as opposed to defensive) approach to PETs deployment is interesting from a policy point of view. However, exploratory analysis using a country-level privacy policy index (see <http://tinyurl.com/3bt4a4>) showed no evidence of a strong relationship between the strength of a country's privacy regime and PETs usage on the one hand and consumers' privacy concerns on the other.

Figure 46: Consumer concern and business awareness of PETs



Source: London Economics

## 6.4 Summary

Our survey aimed to gain insights into businesses' views on the economic benefits of PETs based on the understanding that the views on PETs will depend on:

- the extent to which businesses – including SMEs – use personal data;
- the risks that result from the data use; and
- and the characteristics (including cost and effectiveness) of the technologies themselves.

These considerations are reflected in the design of the survey in two ways: first of all, the sample includes all types of businesses, irrespective of any pre-conceived notions about which industries or types of businesses may have the greatest need for PETs. Secondly, SMEs, which are a group of businesses often overlooked in the discussions on PETs but of special interest for this study, form a large part of the sample (73%). The survey covers companies in all the major sectors of the economy (NACE Sections A to S), with services predominating.

Personal data of varying detail is widely held by businesses. This is true for SMEs as well as larger businesses, although larger businesses tend to hold more detailed data. A majority of the respondents hold detailed personal data on customers. Over 50% of companies with more than 250 employees hold personal data on more than 1,000 individuals. The degree of detail generally increases as the number of records per database increases. It is also evident that certain sectors

are more data-intensive than others. Financial services, social services and health-related services, as well as professional and ICT services all report above average data use.

Interestingly, significant minorities of businesses report no benefits from the personal data they hold. Overall, the larger the business, the greater the perceived benefit. The sectors that hold detailed data, such as financial and ICT services also report relatively large benefits. Data on customers are seen as the most beneficial type.

Businesses perceive only a low to medium risk of harm arising from the misuse of personal data (or the threat thereof). However, larger businesses see the risk as significantly greater than SMEs. A small proportion of companies report that these concerns have prevented them from developing new business activities.

In the light of the previous findings, it is not surprising that, when it comes to PETs, SMEs' cost-benefit calculus differs from that of larger firms. The survey provides clear evidence that SMEs judge the benefits of PETs deployment considerably lower than non-SMEs. Partly, this is likely to reflect the fact that SMEs have less need for PETs owing to their less intensive data use. On the other hand, the survey provides evidence that they are less informed about PETs, which might bias their perceptions on their usefulness.

When considering businesses' awareness of PETs, one can see that this depends largely on the type of technology in question. Filters and blockers are very widely used (83% of respondents report using them), and the use of encryption tools (49%) and evidence erasers (53%) is also widespread. Information tools and administrative tools, on the other hand, are less well known, especially by SMEs. This is potentially problematic as some core PETs, such as P3P, fall into these categories. Moreover, PETs in these categories are relevant in applications where data use cannot be minimised, which means that privacy protection is likely to be incomplete without them.

The survey shows that the level of information businesses have about PETs affects their perception of benefits. The more businesses know about PETs, the greater they judge the net benefits of deployment. This can be interpreted as evidence of an evolutionary learning process. As technologies become more mature, information about their usefulness spreads. The relatively widespread use of filters and blockers would suggest that these are more mature technologies than some of the other categories. A further implication is that there might be a role for public bodies to increase awareness about technologies that are proven to enhance privacy, but have not yet found wide acceptance in the market.

That PETs are seen as effective by a large majority of businesses suggests that businesses could be won over if they have adequate information. In general, the more experience businesses have with PETs, the greater the reported perception of their effectiveness.

High costs and consumer acceptance of the status quo are cited as the most important factors limiting PETs deployment by larger businesses. For SMEs the fact that they do not consider PETs as applicable to their business is the most important barrier.

Overall, it is evident that SMEs use less personal data than larger businesses, although a majority of them use personal data in some form. At the same time, SMEs are less knowledgeable about PETs and less convinced about the economic benefits of deploying them. An important insight is

that many companies, SMEs in particular, hold data from which they derive no economic benefits. This suggests a role for data minimising PETs.

## 7 Options for public-private cooperation

Part of the brief for this study is to examine the role cooperation/joint action of data controllers with national authorities or international organisations might play in enhancing the economic benefits of PETs. Evidence the role of public-private cooperation comes from three sources: theoretical considerations, case studies and the opinions of businesses and other stakeholders recorded in our surveys.

### 7.1 Theoretical arguments

Section 3 highlighted a number of barriers to the effective deployment of PETs. There are several ways in which action by public sector bodies can help overcome these barriers by complementing the efforts by actors in the private sector.

The scope for cooperation seems particularly strong when it comes to:

- encouraging innovation;
- coordinating investments; and
- sharing information.

Establishing how PETs can be used most effectively and transposing these insights into guidelines for PETs design and deployment is a further way in which the public sector is well-placed to assist private sector efforts. In the following sub-sections we discuss the four issues in turn. It should be noted that the options discussed in this sub-section are based on theoretical considerations and thus more speculative than the options that were raised by stakeholders during consultations.

#### 7.1.1 Encouraging innovation

A promising approach to encouraging innovation in PETs is to establish public-private-partnerships aimed at expanding the diversity and quality of PETs. European Union Framework Programmes are a high-profile case in point because they specialise in developing “disruptive” technologies – i.e., technologies that are a significant break from current thinking. Under the framework programmes, specific PETs (for example privacy-enhancing identity management in the PRIME project) are developed in subsidised research projects and can then be used by data controllers, most of which could not have hoped to develop the PETs themselves.

#### 7.1.2 Coordinating investments

Firms might face various coordination problems if the effectiveness of the PETs that they invest in is reliant on other firms’ investment decisions. The difficulty of resolving these coordination problems should be considered on a case-by-case basis because the nature of the technological interrelationships between PETs has a significant effect on the necessity of coordination or not.

If the overall level of security individuals enjoy is determined by one firm’s investments into PETs – for example, ISPs that have some control over the conditions under which a large number of computers are able to access the Internet – then this firm can be unilaterally targeted by

policymakers. That is, policymakers can target “control points” that have discretion over the flows of large volumes of information over the Internet.

Alternatively, the overall level of privacy protection for certain applications may depend on individual data controllers’ investments in a more complex way. For example, as Grossklags et al. (2008) show, if PET effectiveness depends on the weakest link or the sum of all investments, then a large homogenous population of firms (e.g., a market containing a large number of SMEs) will typically under-invest in information security. Consequently, there is a role for cooperation/joint action among market participants to ensure that either:

- the cumulative investment in the market is sufficiently high, or
- the level of privacy protection offered by the weakest link is sufficiently high.<sup>104</sup>

How the investment decisions of individual data controllers affect the overall level of PETs deployment determines the appropriate policy response. With regard to some privacy enhancing technologies, data controllers can independently and successfully deploy PETs. With regard to others, data controllers may need to be encouraged to adopt PETs via technological leadership, subsidies, coordination or other public or private actions.

An interesting result on the potential importance of investment coordination is provided by Hess et al. (2007). The authors analyse possible ways in which firms might coordinate over solutions to security threats in an experimental setting. They find that, if participants are required to make investments in some ordered way, for example, with the largest firms going first, then other firms are more likely to make the investment contribution required of them. An association for firms engaged in the protection of personal data could be set-up to play this coordination role.

### 7.1.3 Stimulating information sharing

The availability of information on risks associated with personal data has a potentially important impact on the effectiveness with which PETs are deployed. In principle, it may be crucial for information to be made available on the rapid pace at which threats to individual privacy develop because this helps firms to allocate information security budgets.

However, the very firms that stand to benefit from information sharing usually face incentives to withhold information regarding privacy breaches that they have experienced, as public knowledge has been observed to affect firms’ market valuation.<sup>105</sup> A loss of reputation could involve loss of customers, poorer relationships with suppliers and higher insurance costs. Survey evidence collected by the Computer Security Institute in 2007 shows that 26% of data controllers cited negative publicity as a key reason to withhold information on a security breach.

---

<sup>104</sup> See Section 3.3.4, p. 48.

<sup>105</sup> See the results by Acquisti et al. (2006) discussed in Section 3.4.2.

In addition, there are several immediate consequences that follow a privacy breach that limit organisations' willingness to be transparent about data breaches. Regulatory bodies may levy fines or demand wholesale changes in information security systems. The Federal Trade Commission in the US for example fined ChoicePoint € 11.1 million (\$ 15 million) after a data breach (FTC 2006). Data breaches may also lead to subsequent liability cases as injured parties file civil lawsuits. Furthermore, organisations are usually required to inform injured parties of data losses, which can involve substantial costs.

Public-sector bodies can help to solve the incentive problems firms face. If the intention of information sharing is to collect information on trends in security threats, public agencies can play a coordination role. This might be most effective if information from firms is collected anonymously, which would protect firms from negative share price reactions or loss of reputation. This anonymity may also help to improve the quality of information provided.

This is only a partial solution however. Firms still have the incentive to underreport their problems as long as it is costly to put internal monitoring systems in place. Moreover, as long as firms are publicly fined for data breaches, cooperative solutions to information sharing problems will only be partly resolved.

An obligation to inform consumers of data breaches, as exists for example in some US states, may also help consumers to make informed decisions and create demand incentives for firms to deploy PETs. However, empirical evidence shows very little impact of disclosure laws on the incidence of data theft.<sup>106</sup> This does not mean, however, that disclosure laws do nothing to increase levels of privacy protection, e.g. by incentivising firms to deploy more or better PETs, which may reduce economic losses per incident (rather than the number of incidents).

#### 7.1.4 Overcoming behavioural biases

One of the key barriers to PETs deployment is the misalignment between individuals' beliefs about privacy and their real-life choices. As discussed in Section 3.2, the presence of behavioural biases can explain this mismatch.

In many cases, there are relatively simple remedies for such behavioural biases. Hottell et al. (2006), for example, find that the level of home-based wireless security people enjoy is not affected by factors such as education levels – i.e., people would not necessarily use the Internet more securely as a result of greater computer literacy. Instead, the default settings on wireless routers determine how secure home-based wireless communications are – individuals tend not move away from the status quo when installing new pieces of equipment.

This standard result from the literature on experimental economics can lead to PETs perhaps not being applied in as an effective way as they possibly could be. However, by agreeing standards such as “safety by default” with the producers of wireless routers, a large impact on individual privacy could be achieved. Public sector bodies, such as national data protection authorities, can

---

<sup>106</sup> See Romanosky et al. (2008).



work with data controllers and the PETs industry to ensure that individuals' behavioural responses to PETs are taken into account at both the design and the deployment stage.

## 7.2 Case study evidence

The case studies presented in Section 5 provide various examples of public sector action supporting private sector initiatives to enable or increase the benefits of PETs. Here we summarise the different approaches we identified.

### 7.2.1 Setting privacy-friendly framework for data controllers

The most fundamental role of the public sector and also the most potent instrument to increase privacy protection is the setting of standards through legislation and regulation, as well as the subsequent enforcement through sanctions.

Compliance with existing privacy protection standards has been one of the most important reasons for developing/deploying PETs in our case studies. Anticipation of future changes in legislation was also mentioned as a motivating factor in one case, which underlines the importance of public policy towards privacy issues for shaping PET deployment decisions.

A view that was raised repeatedly during our research on the case studies was that enforcement of the rules is not always satisfactory, which reduces the incentive for data controllers to deploy PETs.

In this light, a proactive stance of data protection authorities is required in addition to a robust and transparent legal framework. Publicising the legal requirements for privacy protection and working with data controllers to make sure these are respected, including advising on the deployment of adequate PETs, have been described to us as more effective than an ex-post enforcement strategy. The effectiveness of the threat of sanctions in incentivising PETs deployment differs between the cases we researched, which is likely to reflect differences in monitoring levels across different sectors/applications (e.g., the healthcare sector faces greater scrutiny than the car insurance sector).

### 7.2.2 Pioneering PETs deployment

Public bodies can play a pioneering role by deploying PETs before they are taken up by private sector data controllers. This serves a three-fold purpose:

- First, by deploying PETs, the public sector data controller makes sure that the personal data it is responsible for is protected.
- Secondly, by setting an example, the public sector deployer demonstrates the economic benefits of PETs to other data controllers who would not have been aware of the benefits otherwise. This strategy can be interpreted as an attempt to help speed up the progress of a PET along the S-curve.
- Thirdly, the introduction of a privacy-enhanced option into the market might put pressure on data controllers that do not yet deploy PETs to do so in order to avoid a potential backlash from consumers. The case study on CCTV privacy zones is an example of a public

body deploying PETs, which, through these mechanisms, could result in more PETs deployment overall.

Another way in which public bodies can bring about the adoption of PETs is through procurement process. Making PETs a mandatory requirement in public procurement provides a strong incentive for data controllers to invest in PETs, as not doing so would exclude them from tendering for contracts with public sector clients. This option was highlighted during interviews for the case study on PriPAYD, in the context of a planned road pricing scheme in the Netherlands that is reportedly going to require contractors to use PETs.

### 7.2.3 Subsidising PETs

Another important function of the public sector is the support of PETs development through funding for research programmes. Our case studies show examples of PETs originating in (at least partly) publicly funded universities (PriPAYD) and PETs developed in cooperation between universities and businesses (GENOMatch).

In addition, research funding is provided by the European Union via its *Framework Programmes for Research and Technological Development*, currently in its seventh cycle (FP7). The Framework Programmes have proved a productive source of innovation in PETs. Our case study on privacy-enhanced LBS is an example of a PET originating in EU-funded research (PRIME).

As was mentioned in the LBS case study, subsidies could be extended to PET deployment rather than development – this might be especially effective among SMEs, which, according to our survey of businesses, are more likely than larger businesses to find the costs of PETs to exceed their benefits in the context of their use of personal data.

### 7.2.4 Endorsement/certification of PETs

If public bodies are not in the position to deploy PETs themselves or mandate deployment by others, an attractive option is to publicly endorse PETs, either informally of by providing official credentials. GENOMatch is an example of a PET with an official ‘stamp of approval’ in the form of a formal Data Protection Audit. Explicit endorsement by government also features in case studies on CCTV privacy zones and fingerprint identification. More informal support can be given in a variety of ways, for example by discussing them in official reports, presentations at workshops and conferences, etc.

Public endorsements promote PETs deployment principally in two ways:

- First, they help to advertise PETs to data controllers. This lowers the marketing costs for PETs developers and the search costs for data controllers.
- Secondly, endorsements can help data controller to realise the benefits of PETs by reassuring individuals or intermediaries with concerns about privacy and by demonstrating the data controller’s commitment to privacy protection more generally. The official endorsement can act as a sign of quality, which increases trust in PETs. Possibly, this also confers a competitive advantage on data controllers that deploy PETs vis-à-vis those that do not.

### 7.3 Views of businesses and stakeholder organisations

Our consultation exercise asked stakeholders (national data protection authorities and business and consumer associations) for their views on cooperation between public and private sector actors to promote the deployment of PETs. Stakeholders saw awareness-raising as the most important function of public bodies with respect to promoting PETs deployment.

A number of specific measures were suggested by stakeholders (see Section 4.3):

- First, public bodies and businesses should engage in dialogue to help the latter understand regulation and the need for PETs.
- Secondly, the use of “privacy impact assessments” to help data controllers understand the types of privacy risks their activities result in should be encouraged.
- Thirdly, public bodies should offer advice to businesses on concrete PETs appropriate for their activities and on emerging threats. Finally, the role of strategic litigation and subsequent sanctions should be increased to internalise the costs associated with data misuse or loss by businesses.

Our survey of businesses also asked respondents to comment on ways in which the public sector could help businesses to realise the benefits of PETs. Respondents reported a wide variety of views. A concern that was repeatedly mentioned is the perceived lack of standards (or the non-transparency of existing rules) as well as a lack of consistency across jurisdictions. A number of respondents also called for tougher penalties for infringements, although some saw a danger that privacy obligations may become a burden on business (one respondent mentioned the “demonisation” of the use of personal data as a concern).

The provision of information about PETs as well as about the risks to privacy was mentioned frequently as an area where public sector initiative would be welcome. However, some businesses expressed a lack of confidence in the public sector when it comes to privacy issues. Several respondents thought that examples of data loss by public sector organisations undermine governments’ credibility when it comes to the promotion of privacy friendly practices such as PETs.

Providing financial support for PETs was seen as an attractive option by respondents, with some calling for direct subsidies, others for subsidising PETs development or financing pilot projects. Respondents also stressed the need for simple, ‘off-the-shelf’ technologies.

### 7.4 Summary

The public sector has a very important role to play in assisting data controllers if the benefits of PETs are to be realised. All of the PETs we discussed in the case studies show some form of public sector involvement, even in cases where PETs were developed and deployed purely on the initiative of data controllers in the private sector. Four main areas in which public sector initiatives can complement the efforts of private data controller to enhance privacy can be identified:

- Setting and enforcing privacy standards;
- Supporting PETs development through direct or indirect funding;

- providing credentials and official endorsements; and
- promoting PETs through information campaigns and ongoing contact with data controllers.

A more speculative role for cooperation between the public and the private sector based on theoretical considerations is in the coordination of investments in PETs, which might increase the overall effectiveness of deployment.

An area where concerns were raised by the respondents to our business survey is the lack of user-friendliness of some PETs. This suggests that closer cooperation between PETs developers and businesses, especially SMEs, which are more sceptical about the benefits of PETs than larger businesses (see Section 6.3), is needed to ensure that state-of-the art PETs meet the needs of businesses of all sizes.

Providing information about PETs to data controllers continues to be an important task for public bodies such as national data protection authorities. The business survey showed that awareness of state-of-the-art PETs is still low, especially among SMEs. Concerns about costs and doubts about the applicability of PETs, again frequently observed among SMEs, are other areas that could be effectively addressed by information campaigns.

However, rather than sporadic publicity drives, information and advice should be provided on an ongoing basis. Several sources pointed out the need for constant engagement by data protection authorities to foster a climate in which data controllers can receive the maximum economic benefit from PETs.

In this context, it is also important to consider the role of the public sector in setting an example of good practice in upholding privacy standards. A number of respondents to our business survey were sceptical about the role of public sector in promoting PETs because of a perception that public bodies are among the culprits when it comes to failures to protect personal data and ensure user privacy.

## 8 Conclusions

The study shows clearly that the benefits of PETs are technology-specific as well as dependent on the applications in which PETs are deployed. The concept of PETs encompasses a wide variety of different technologies that enhance individuals' privacy in various ways. Data protection plays a role in many PETs, but anonymisation, data minimisation and the fulfilment of consent requirements are equally important aspects of PETs.

The costs and benefits thus vary across technologies. While some PETs involve virtually no additional costs compared with the privacy-invasive status quo, others require a substantial financial investment from data controllers. Moreover, the deployment of PETs in certain cases requires changes in the data controller's business model. Perhaps most importantly, the decision to deploy PETs can involve a trade-off between the ability to use personal data and the benefits of PETs (e.g. a lower risk of data theft).

The benefits of the same PET can differ across applications. Factors such as whether the PET is deployed by a large or a small business or whether the data controller operates in a market where consumer demand is sensitive to PETs deployment all affect the benefits that may be derived from PETs.

The complexity of the issue of economic benefits makes it impossible to quantify the economy-wide benefits to data controllers of PETs deployment. Rather, the evidence suggests that the net economic benefit of PETs deployment needs to be assessed on a case-by-case basis.

Although survey evidence shows high levels of concern about privacy by individuals, there is little evidence that the demand by individuals for greater privacy is driving PETs deployment. If individuals are well informed and acting rationally, the demand for increased PETs deployment is a function of:

- individuals' risk aversion;
- the risk of data loss/privacy invasion; and
- the efficacy of PETs in reducing the risk.

However, in practice, individuals are faced with:

- uncertainties about the risk of disclosure of personal data;
- a lack of knowledge about PETs; and
- behavioural biases that prevent individuals from acting in accordance with their stated preference for greater privacy.

Factors such as these help to explain why the stakeholders, who were consulted for the present study, attest to a widespread indifference on the part of individuals when it comes to actual buying decisions. Evidence from event studies analysing the share price reaction of companies that experienced privacy incidents as well as evidence from economic experiments support the conclusion that demand for PETs from individuals is not an important driver of deployment.

On the other hand, the incentive for data controllers to deploy PETs could consist simply of data controllers' own fear of data loss. This assumption is plausible as data controllers stand to lose more in absolute terms in cases of data loss than individuals. Reasons for this include the volume of data, which in the case of data controllers can involve data on employees, suppliers, customers, etc., as well as the fact that liability for data loss typically rests with data controllers, which exposes them to sanctions and damages claims following a privacy incident.

To the extent that there is a demand for PETs, data controllers may also gain a competitive advantage through PETs. As discussed above, there is little evidence that this is the case in the consumer market at the present time, but competition as a driver of PETs deployment seems to play an important role in the business-to-business market (i.e., in cases where a data controller outsources data storage or processing to another company).

However, data controllers also benefit from the electronic processing of personal data. The main sources of benefit are greater efficiency in carrying out processes electronically; personalising goods and services; and exploiting personal data in the production of new goods and services.

Overall, the evidence on deployment incentives means (assuming that PETs deployment is to some degree discretionary, i.e. not mandatory under data protection legislation) that PETs may involve a trade-off for data controllers: while deployment of PETs can be beneficial, for example allowing savings on data protection measures, using PETs might reduce the benefits data controllers derive from the availability of personal data as an economic resource.

In the calculation of data controllers, the cost of foregone options involving the use of personal data has to be added to the upfront costs of PETs as well as the cost of training and ongoing maintenance to ensure effective deployment.

The uncertainty of some of the costs and benefits of PETs also explains why firms might rationally postpone the deployment of PETs while waiting for more information, in order not to limit their future choices.

Slow deployment of PETs, even in cases where there seems to exist a strong economic case for them, can also be explained by economic theories of technology adoption. These theories suggest that the deployment levels of new technologies are initially low, but then pick up as the technologies mature or as information about the technologies spreads among potential users, before finally flattening out as the market becomes saturated or new technologies emerge that replace them (this results in an S-shaped pattern of the adoption rate).

However, there are also theoretical arguments that market imperfections may hold back PETs deployment. These market imperfections include asymmetric information, externalities, lack of information sharing about privacy risks and coordination failures.

The existence of market failures implies that there may be benefits from PETs deployment which data controllers are currently not realising. To the extent that market failures are an issue in the context of PETs, this points to a potential role for the public sector to help data controllers overcome the barriers holding back PETs deployment.

Cooperation between the public sector and data controllers can help to increase the deployment of PETs and the effectiveness of deployment. Here, governments have a fundamental role in formulating standards of privacy protection.

Data protection legislation supports data controllers by setting the framework in which they can operate in a way that is compatible with the privacy demands of society at large. Enforcement of these rules helps data controllers by penalising non-compliant behaviour, thus preventing data controllers from gaining a competitive advantage by not taking the necessary steps to protect privacy. Respondents to the business survey repeatedly mentioned that stronger enforcement of existing rules would help them realise the benefits of PETs.

Public sector endorsements of PETs or official certification schemes can be an effective tool to help data controllers realise the benefits of PETs. From the point of view of data controllers, such endorsements help to raise awareness of PETs and increase the trust of consumers and intermediaries, which can yield direct economic benefits. Trusted privacy credentials can also give data controllers an advantage in the business-to-business market. For example, companies looking for a data storage provider might use official credentials as a quality indicator. In addition, official endorsements represent free positive publicity for PETs and the data controllers that deploy them.

Finally, innovation in PETs may be sub-optimal because of market failures (e.g. coordination problems) that lead to underinvestment in PETs. The existence of market failures indicates a role for the public sector to ensure that sufficient PETs development is taking place. The European Union is already very active in this area, funding research into PETs through its Framework Programmes, which is producing market-ready prototypes of PETs (e.g. the PRIME)). The research on PETs taking place in universities, typically at least partly state-funded, is another important area where public sector involvement is important, especially when it complement private-sector research.

It should be noted that, according to the survey results presented in this study, SMEs are less convinced of the benefits of PETs than larger businesses. This may suggest that targeted information campaigns could be used to increase the awareness of PETs among SME data controllers.

However, SMEs also use less personal data than larger businesses, which may suggest the need for PETs by SMEs may be lower. On the other hand, the fact that SMEs often report that they do not derive economic benefits from the personal data they hold suggests that data minimisation has an important role to play in this area.

## 9 References

- Acquisti, A. (2004), "Privacy and Security of Personal Information: Economic Incentives and Technological Solutions," in J. Camp and S. Lewis (eds.), *The Economics of Information Security*, Kluwer.
- Acquisti, A. and Varian, H. R. (2005), "Conditioning Prices on Purchase History," *Marketing Science*, 24, 3, 1–15.
- Acquisti, A., Dingedine, R. & Syverson, P., (2003), "On the Economics of Anonymity", in *Financial Cryptography*, pp. 84-102.
- Acquisti, A., Friedman, A. and Telang, R. (2006), "Is there a cost to privacy breaches? An event study", *Workshop on the Economics of Information Security (WEIS)*, University of Cambridge, UK.
- Alexander, J. T., Davern, M. and Stevenson, B. (2010). "Inaccurate age and sex data in the Census PUMS files: Evidence and Implications". Mimeo, available at: <http://tinyurl.com/y9zlfsl>.
- Anderson, R. (1993), "Why cryptosystems fail", in *Proceedings of the 1st ACM conference on Computer and Communications Security*, pp. 215-227.
- Anderson, R. and Moore, T. (2006), "The Economics of Information Security", *Science*, 314 (5799), 610-613.
- Anderson, R., Böhme R., Clayton R. and Moore T. (2009), "Security Economics and European Policy", in *Managing Information Risk and the Economics of Security*, pp. 1-26.
- Backes, M. and Dürmuth, M. (2007), "Enterprise Privacy Policies and Languages", in Acquisti, A., Gritzalis, S., Lambrinoudakis, C. and De Capitani de Vimercati, S., *Digital privacy: Theory, Technologies and Practices*, pp. 135-154.
- Balasch, J. and Verbauwheide, I. (2009), "An Embedded Platform for Privacy-Friendly Road Charging Applications." *Design, Automation and Test in Europe (DATE 2010)*, IEEE.
- Balasch, J. Rial, A., Troncoso, C., Preneel, B. and Verbauwheide, I. (2010), "PrETP: Privacy-Preserving Electronic Toll Pricing". Available at: <http://tinyurl.com/ycl6joz>.
- Berendt, B., Günther, O., Spiekermann, S. (2005), "Privacy in e-commerce: stated preferences vs actual behavior", *Communications of the ACM*, 48 (4), 101-6.
- Bohm, N., Brown, I. and Gladman, B. (2000), "Electronic Commerce: Who Carries the Risk of Fraud?" *Journal of Information Law and Technology*, October 2000.
- Borking, J. (2009), Why adopting of privacy enhancing technologies (PETs) takes so much time. Presentation at the DG Justice Workshop on the Economic Benefits of PETs, 12 November 2009. Available at: <http://tinyurl.com/ybrtk4w> [slides] and <http://tinyurl.com/yax43a6> [paper].



- Calzolari, G. and Pavan, A. (2006), "On the Optimality of Privacy in Sequential Contracting," *Journal of Economic Theory*, 130, 1.
- Campbell, K., Gordon, L., Loeb, M. and Zhou, L. (2003), "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market", *Journal of Computer Security*, 11, 3, 431–448.
- Cavusoglu, H., Mishra, B. and Raghunathan, S. (2002), "The effect of internet security breach announcements on market value of breached firms and internet security developers", in *International Journal of Electronic Commerce*, 9.
- Chatterjee, D. Richardson, V. J. and Zmud, R. W. (2001), "Examining the Shareholder Wealth Effects of Announcements of Newly Created CIO Positions", *MIS Quarterly*, 25, 1, 43-70.
- Chaum, D. (1981), "Untraceable electronic mail, return addresses, and digital pseudonyms", *Communications of the ACM*, 24 (2), pp. 84–88.
- Chaum, D. (1983), "Security without Identification: Transaction Systems to Make Big Brother Obsolete," *Comm. ACM*, 28, 10, 1030–1044.
- Clarke, R. (2007), "Business Cases for Privacy-Enhancing Technologies". In: Subramanian, R. (Ed.), *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*, 12-Jun-2007, Hershey, USA, IDEA Group Publishing.
- David, P. (1969), "A Contribution to the Theory of Diffusion", Mimeo. Stanford University.
- Davidson III, W. L. and Worrell, D. L. (1992), "The Effect of Product Recall Announcements on Shareholder Wealth", *Strategic Management Journal*, 13, 6, 467-473.
- Davies, S. (1979), "The Diffusion of Process Innovations", Cambridge University Press: Cambridge.
- Dingledine, R. and Mathewson, N. (2005), "Anonymity loves company: Usability and the network effect", in *Designing Security Systems That People Can Use*, O'Reilly Media.
- Dixit, A. and Pindyck, R. (1994), "Investment under Uncertainty", Princeton University Press: Princeton.
- Dos Santos, B. L., Peffers, K. and Mauer, D. (1993), "The Impact of Information Technology on the Market Value of the Firm", *Information Systems Research*, 4, March, 1-23.
- Dwork, C. (2006), "Differential Privacy". Available at: <http://tinyurl.com/yeyxv5e>.
- Earp, J., and Baumer, D. (2003), "Innovative web use to learn about consumer behaviour and online privacy, *Communications of the ACM*, 46 (4), 81-3.
- Edelman, B. (2006), "Adverse Selection in Online Trust Certifications," Working Paper, Harvard University.

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

Federal Trade Commission (2006), "Stipulated final judgement and order in US v Choicepoint", FTC File 052-3069.

Feigenbaum, J., Freedman, M. J., Sander, T., Tomas, S. and Shostack, A. (2002), "*Economic Barriers to the Deployment of Existing Privacy Technologies*", Proceedings of the Workshop on Economics and Information Security, pp. 16–17.

FIDIS (2007), *FIDIS Deliverable D7.5: Profiling the European Citizen: Cross-Disciplinary Perspectives*, European Union IST FIDIS Project.

Fischer, F., Mansmann, F., Keim, D. A., Pietzko, S. and Waldvogel, M. (2008), "Large-Scale Network Monitoring for Visual Analysis of Attacks", in *Proceedings of the 5th international workshop on Visualization for Computer Security*, Springer-Verlag, pp. 111-118.

Fischer-Hübner, S. (2002), "IT-Security and Privacy-Design and Use of Privacy-Enhancing Security Mechanisms", *LNCS Journal*, vol. 1958, Springer Heidelberg.

Fischer-Hübner, S., Sören Petterson, J., Bergmann, M., Hansen, M., Pearson, S. and Casassa Mont, M. (2007), "HCI Designs for Privacy-Enhancing Identity Management" in Acquisti, A., Gritzalis, S., Lambrinoudakis, C. and De Capitani de Vimercati, S., *Digital privacy: Theory, Technologies and Practices*, pp. 229-252.

Fritsch, L. (2007), "State of the art of Privacy-enhancing Technology (PET)". *Norwegian Computing Center Report*, No. 1013. Available at: <http://publ.nr.no/4589>.

Gal-Or, E. and Ghose A. (2005), "The Economic Incentives for Sharing Security Information", *Information Systems Research*, 16 (2), pp. 186-208.

Geroski, P. A. (2000), "Models of technology diffusion", *Research Policy*, 29, 4-5, 603–625.

Goldberg, I. (2007), "Privacy Enhancing Technologies for the Internet III: Ten years later", in Acquisti, A., Gritzalis, S., Lambrinoudakis, C. and De Capitani de Vimercati, S., *Digital privacy: Theory, Technologies and Practices*, pp. 3-18.

Gordon, L. A., M. Loeb and W. Lucyshyn. (2003), "Sharing information on computer systems security: An economic analysis", *Journal of Accounting and Public Policy*, 22 (6), pp. 461–485.

Griliches, Z. (1957), "Hybrid Corn: An Exploration in the Economics of Technological Change," *Econometrica*, Vol. 25, pp. 501-522.

Griliches, Z. (1957), "Hybrid Corn: An Exploration in the Economics of Technological Change," *Econometrica*, Vol. 25, pp. 501-522.

- Grossklags, J., N., Christin, and Chuang, J. (2008), "Security investment (failures) in five economic environments: A comparison of homogeneous and heterogeneous user agents", available at: <http://tinyurl.com/yedlcqr>.
- Hall, B. and Khan, B. (2003), "Adoption of New Technology," NBER Working Paper 9730.
- Hann, I-H, Hui, K-L, Lee, T. S. and Png I. P. L. (2002), "Online Information Privacy: Measuring the Cost-Benefit Trade-Off," Proceeding of the 23rd International Conference on Information Systems.
- Hannan, T. and McDowell, J. (1984). "The determinants of technology adoption: the case of the banking firm", *Rand Journal of Economics*, 15, 328–335.
- Hansen, M (2006), "Privacy-Enhancing Identity Management," Information Security Technical Report, 11, 3, 119–128.
- Hendricks, K. and Singhal, V. (1997), "Delays in new product introductions and the market value of the firm: The consequences of being late to the market", *Management Science*, 43, 4, 422–436.
- Hermalin, B. and Katz, M. (2006), "Privacy, property rights and efficiency: The economics of privacy as secrecy", *Quantitative Marketing and Economics*, 4(3), 209-239.
- Hess, R., Holt, C. and Smith, A. (2007), "Coordination of strategic responses to security threats: Laboratory evidence", *Experimental Economics*, 10 (3), 235-250.
- Hottell, M., Carter, D. and Deniszczuk, M. (2006), "Predictors of home-based wireless security", in *The Fifth Workshop on the Economics of Information Security*.
- Hovava, A. and D'Arcy, J. (2003), "The impact of denial-of-service attack announcements of the market value of firms", *Risk Management and Insurance Review*, 6, 2, 97–121.
- Hui, K-L and Png, I. P.L. (2005), "Economics of Privacy" in *Handbook of Information Systems and Economics*, Elsevier.
- Im, K. S., Dow, K. E. and Grover, V. (2001), "Research Report: A Reexamination of IT Investment and the Market Value of the Firm – An Event Study Methodology", *Information Systems Research*, 12, 1, 103-117.
- Ingham, H. and Thompson, S. (1993), "The adoption of new technology in financial services: the case of building societies", *Economics of Innovation and New Technology*, 2, 263–274.
- Jarrell, G. and Peltzman, S., "The Impact of Product Recalls on the Wealth of Sellers", *The Journal of Political Economy*, 93, 3, 512-536.
- Jiang, X., J. I. Hong, and J. A. Landay, (2002). "Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing", UBICOMP 2002.
- Karjoth, G. and Schunter, M. (2002), "A privacy policy model for enterprises", in *Proc. 15th IEEE Computer Security Foundations Workshop (CSFW)*, 271-281, Cape Breton, Nova Scotland.

Karjoth, G., Schunter, M. and Waidner, M. (2002), "The platform for enterprise privacy practices: Privacy-enabled management of customer data", in *Proc. Privacy Enhancing Technologies Conference*, vol. 2482 of LNCS, 69-84, Springer Heidelberg.

Karshenas, M. and Stoneman, P. (1993), "Rank, stock, order and epidemic effects in the diffusion of new process technologies", *Rand Journal of Economics*, 24, 503-528.

Koorn, R., Borking, J., van Gils, H., ter Hart, J., Overbeek, P. and Tellegen, R. (2004), *White Paper for Decision-Makers*. Ministry of the Interior and Kingdom Relations (NL), The Hague.

Kunreuther, G. and Heal, G. (2003), "Interdependent Security", *Journal of Risk and Uncertainty*, 26 (2), 231-249.

Levin, S., Levin, S. and Meisel, J. (1987), "A dynamic analysis of the adoption of a new technology: the case of optical scanners", *Review of Economics and Statistics*, 69, 12-17.

Lorrie Faith Cranor (2003), *The role of privacy enhancing technologies*. In *Considering Consumer Privacy: A Resource for Policymakers and Practitioners*. Center for Democracy and Technology, edited by Paula J. Bruening, March 2003.

Low, S., Maxemchuk, N. F. and Paul, S. "Anonymous Credit Cards," *Proc. 2nd ACM Conf. Computer and Communications Security*, ACM Press, 108-117.

Lynn, B., Prabhakaran, M. and Sahai, A. (2004), "Positive results and techniques for obfuscation", in *Proc. of Advances in Cryptology – EUROCRYPT 2004*, vol. 3027 LNCS, pp. 20-39, Springer Heidelberg.

Machanavajjhala, A., Gehrke, J., Kifer, D. and Venkitasubramaniam, M. (2007) "ℓ-Diversity: Privacy Beyond k-Anonymity". *Transactions on Knowledge Discovery from Data*, vol 1, no. 1, 2007. Available at: <http://tinyurl.com/yz9bunw> [accessed 02 Dec 2009].

Machanavajjhala, A., Kifer, D., Abowd, J., Gehrke, J. and Vilhuber, L. (2008) "Privacy: Theory meets Practice on the Map". mimeo. Available at: <http://tinyurl.com/ydkb942> [accessed 02 Dec 2009].

Mansfield, E. (1968), "Industrial Research and Technological Innovation", New York: Norton.

Moore T. (2005), "Countering Hidden-Action Attacks on Networked Systems", in *Fourth Workshop on the Economics of Information Security*, Harvard.

Narayanan, A. and Shmatikov V. (2007), "Uncircumventable Enforcement of Privacy Policies via Cryptographic Obfuscation", in Acquisti, A., Gritzalis, S., Lambrinoudakis, C. and De Capitani de Vimercati, S., *Digital privacy: Theory, Technologies and Practices*, pp. 155-171.

Nelson, R. and Winter, S. G (1982), "An Evolutionary Theory of Economic Change", Cambridge: Harvard University Press.

Pennings, J. and Harianto, F. (1992), "The diffusion of technological innovation in the commercial banking industry", *Strategic Management Journal*, 13, 29-46.

- Rogers, E. (1995), "Diffusion of Innovations", The Free Press: New York.
- Romanosky, S., Telang, R., Acquisti, A. (2008), "Do Data Breach Disclosure Laws Reduce Identity Theft?" Carnegie Mellon University - Heinz College of Information Systems and Public Policy Working Paper. Available at: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1268926](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1268926).
- Romeo, A. (1975), "Inter-industry and inter-firm differences in the rate of diffusion of an innovation", *Review of Economics and Statistics*, 57, 311–319.
- Rose, N. and Joskow, P. (1990), "The diffusion of new technologies: evidence from the electric utility industry", *Rand Journal of Economics*, 21, 354–373.
- Rothschild, M. and Stiglitz, J. (1976), "Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information", *The Quarterly Journal of Economics*, 90(4), 629-649.
- Samuelson, P. (2000), "Privacy as intellectual property", *Stanford Law Review*, 52, 1125.
- Stewart, J. J. (2002), "Biotechnology valuations for the 21<sup>st</sup> century". *Milken Institute Policy Brief*, 27.
- Shapiro, C. and Varian, H. (1999), "Information Rules: A Strategic Guide to the Network Economy", Harvard Business School Press.
- Shmatikov, V. and Brickell, J. (2008), "The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing". In *Proc. of 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, Las Vegas, NV, August 2008, pp. 70-78. ACM, 2008.
- Shmatikov, V. and Narayanan, A. (2008), "Robust De-anonymization of Large Sparse Datasets (How To Break Anonymity of the Netflix Prize Dataset)". In *Proc. of 29th IEEE Symposium on Security and Privacy*, Oakland, CA, May 2008, pp. 111-125. IEEE Computer Society, 2008.
- Stigler, G. J. (1980), "An Introduction to Privacy in Economics and Politics", *Journal of Legal Studies*, 9 (4), 623-44.
- Stiglitz, J. E. and Weiss, A. (1981), "Credit Rationing Markets with Imperfect Information", *The American Economic Review*, 71 (3), 393-410.
- Stoneman, P. (2001), "The Economics of Technological Diffusion", Blackwells: Oxford.
- Su, C., Zhou, J., Bao, F., Wang, G. and Sakurai, K. (2007), "Privacy-Preservation Techniques in Data Mining", in Acquisti, A., Gritzalis, S., Lambrinoudakis, C. and De Capitani de Vimercati, S., *Digital privacy: Theory, Technologies and Practices*, pp. 187-226.
- Taylor, C. R. (2004), "Consumer Privacy and the Market for Customer Information," *RAND Journal of Economics*, 35, 4, 631–651.
- Telang, R. and Wattal, S. (2006), "Impact of software vulnerability announcements on the market value of software vendors - An empirical investigation", Working Paper, Carnegie Mellon University.

The META Group (2005). *Privacy enhancing technologies*. <http://tinyurl.com/6h3qru>.

Troncoso, C., Danezis, G., Kosta, E. and Preneel, B., (2007), "PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance", proceedings of the *Workshop on Privacy in the Electronic Society 2007*, pp. 99-107, ACM.

Troncoso, C., Danezis, G., Kosta, E. and Preneel, B., (2008), "PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance", Presentation at the workshop *Secure Vehicular Communications: Results and Challenges Ahead*, Lausanne February 20-21, 2008. Available at: <http://tinyurl.com/yc5acan>.

Tsai, J., Egelman, S., Cranor, L. and Acquisti, A. (2007), "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study". Paper presented at the *6th Workshop on the Economics of Information Security (WEIS)*, June 2007. Available at: <http://weis2007.econinfosec.org/papers/57.pdf>.

Van Zandt, T. (2004), "Information overload in a network of targeted communication", *RAND Journal of Economics*, 35(3), 542–560.

Varian, H. (1996), "Economic Aspects of Personal Privacy, in *Privacy and Self-Regulation in the Information Age*", NTIA report.

Varian, H., (2000), "Managing online security risks", *New York Times*, 1 June 2000. Available at: <http://tinyurl.com/y9u596m>.

Wang X.S. and Jajodia, S. (2007), "Privacy Protection with Uncertainty and Indistinguishability" in Acquisti, A., Gritzalis, S., Lambrinoudakis, C. and De Capitani de Vimercati, S., *Digital privacy: Theory, Technologies and Practices*, pp. 173-186.

Ward, M. R. (2001), "The economics of online retail markets", in *The International Handbook on Emerging Telecommunications Networks*, Edward Elgar Publishers.

Westin, A. F. (1967), "Privacy and Freedom", Antheneum.

## Stakeholder consultation documents

### European Commission DG Justice, Freedom and Security: Study on the economic benefits of privacy enhancing technologies (PETS)



Insert Name of Recipient,  
Insert Organisation Name,  
Insert Address,  
Insert Address,  
Insert Address.

17 March 2010

Dear INSERT NAME,

#### Study on the economic benefits of privacy enhancing technologies

London Economics have been commissioned by the European Commission Directorate General of Justice, Freedom and Security to undertake an analysis of the economic benefits associated with the deployment of Privacy Enhancing Technologies (PETs) by both public and private sector organisations.

#### What are PETS?

In recent years, innovative information and online communication services have been improving people's lives. Simultaneously, there has been a substantial increase in the volume of individual *personal data exchanged* when people purchase goods and services, establish contact with one another and communicate their ideas online. However, these personal data exchanges bring about risks. People have become vulnerable to identity theft, discriminatory profiling, continuous surveillance and fraud.

Privacy Enhancing Technologies (PETs) can potentially minimise these risks by helping people better protect their privacy and personal data online. Privacy Enhancing Technologies are any technology or software products that enhance privacy protection of databases in (for example, cookie cutters, encryption tools, automatic anonymisation software, or P3P (Platform for Privacy Preferences)).

#### Primary focus of our study

The specific focus of the study is to:

- assess to what extent the deployment of PETs could yield economic benefits; and,
- on the basis of the analysis undertaken, assess:
  - whether the deployment of PETs results in a economic benefit to the deployer (data controller);
  - the effectiveness of PETs; and
  - whether cooperation/joint action (such as Public Private Partnerships) of data controllers with national authorities or international organisations would enhance these economic benefits.

#### Research being undertaken

The analysis has a number of workstreams and involves undertaking

- a review of the academic and policy related literature;
- a consultation exercise in 12 EU Member States<sup>1</sup> with national authorities established for the purposes of ensuring data protection (insert name of national authority).

<sup>1</sup> Austria, Germany, the Netherlands, Denmark, Estonia, Spain, Italy, Ireland, Malta, Czech Republic, United Kingdom and Hungary



European Commission DG Justice, Freedom  
and Security: Study on the economic  
benefits of privacy enhancing technologies (PETS)



- business associations and federations (such as (insert business associations(s))); and consumer associations (such as (insert consumer associations(s)));
- a series of case studies in the 12 Member States (consisting of 2 public sector organisations and 2 private sector organisations per Member State) to better understand the following
    - the deployment process and use of PETs;
    - the changes in business or service delivery process that have arisen as a result of the deployment of PETs;
    - the costs (one-off and on-going) of the use of PETs;
    - the various types of cost savings arising from the deployment of PETs
    - other indirect benefits to the data provider; and,
    - benefits to the individual benefiting from the PET deployment by the business or the public administration
  - a large scale survey of businesses and public sector bodies to gather more extensive information on PETs.

**Your participation**

London Economics are contacting you as part of the consultation exercise. Insert Consultant Name (e-mail address and phone number) will contact you again in the near future in the hope of arranging a suitable time to have short discussion with you about the incidence, costs and benefits of Privacy Enhancing Technologies in (insert your country).

We are seeking to understand whether you are aware of any information sources on the costs and benefits of PETs that might be of assistance to us in our research. In addition, we would appreciate if you could provide some specific examples where the provision of a service has taken place in (Insert your country) in conjunction with the deployment (or partial deployment) of PETs by either private or public sector organisations. The contact details of the organisations or individuals that we might be able to contact in relation to these examples would be greatly appreciated.

We have enclosed a short questionnaire to assist ahead of the consultation and we envisage that the discussion will require no more than 30 minutes of your time.

If you have any queries in relation to this project, please feel free to contact Dr Gavan Conlon (London Economics) on +44 20 7866 8176 (gconlon@londecon.co.uk) or Hana Pecháčková (Desk Officer, Legal Affairs and Policy Directorate D5 - Data Protection) on +32 2 29 88676 (hana.pechackova@ec.europa.eu). Your assistance and support to this project are invaluable and London Economics is looking forward to working with you very soon.

Yours sincerely,

Dr Gavan Conlon,  
Divisional Director,  
London Economics



European Commission DG Justice, Freedom  
and Security: Study on the economic  
benefits of privacy enhancing technologies (PETS)



Topics to be considered during the stakeholder consultation

SECTION 1: Contact details

Please complete your contact details below.

Name:   
 Organisation:   
 Position:   
 Phone:   
 E-mail:

SECTION 2: The risks to privacy and the protection of personal data

1. Are the risks to privacy and the protection of personal data associated with online activity increasing? Please answer on a scale of 1 to 5, where 1 is "Decreasing significantly", 3 is "About the same" and 5 is "Increasing significantly".

a. What is the specific nature of the risk to privacy and the protection of personal data?

b. Are there any specific privacy and data protection issues or risks that are becoming increasingly prominent?

c. Do you think that consumers and/or businesses are aware of the general or specific risks associated with the maintenance of privacy and the protection of personal data?

2. Privacy Enhancing Technologies (PETs) can potentially minimise some of these risks by helping people better protect their privacy and personal data online. Do you think that the deployment of PETs is an effective means of minimising the risks identified? Please answer on a scale of 1 to 5, where 1 is "Not at all effective", 3 is "Neither effective nor ineffective" and 5 is "Highly effective".

3. Do you think that the deployment of PETs is currently widespread in (insert your country)? Please answer on a scale of 1 to 5, where 1 is "Not at all widespread" and 5 is "Very widespread".

European Commission DG Justice, Freedom  
and Security: Study on the economic  
benefits of privacy enhancing technologies (PETs)



4. Has the deployment of PETs changed significantly over the past 5 years (insert your country)? Please answer on a scale of 1 to 5, where 1 is "No significant change" and 5 is "Very significant change".

5. Are there any specific factors that are limiting the deployment of PETs (insert your country)? For instance, on a scale of 1 to 5, where 1 is "Not at all applicable" and 5 is "Entirely applicable".

The fixed costs for businesses associated with the implementation of PETs

The ongoing costs for businesses associated with maintenance/upgrading of PETs

Businesses unaware of PETs

Organisational Size

Limited applicability for many business types

Lack of information on how to go about deploying PETs

The sophistication of the technology involved

Perceived staffing/training barriers

The value for money associated with the deployment of PETs

The lack of understanding of PETs amongst businesses

The perceived lack of economic benefits amongst businesses

Consumer acceptance of current privacy and data protection risks

Refusal of consumers to pay for PETs

Lack of political imperative

Other 1 – please state

Other 2 – please state

Other 3 – please state

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**SECTION 3: The economic and no-economic benefits of privacy enhanced technologies**

6. To what extent could the deployment of PETs yield **economic** benefits to data controllers<sup>2</sup>? For instance, on a scale of 1 to 5, where 1 is "Very insignificant benefits" and 5 is "Very significant benefits" .

6a. What do you think are the main **economic** benefits that could be realised?

<sup>2</sup> A data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed



European Commission DG Justice, Freedom  
and Security: Study on the economic  
benefits of privacy enhancing technologies (PETs)



7. To what extent could the deployment of PETs yield non-economic benefits to data controllers? Please answer on a scale of 1 to 5, where 1 is "Very insignificant benefits" and 5 is "Very significant benefits" .

7a. What do you think are the main non-economic benefits that could be realised?

8. Do you think that these benefits are concentrated amongst any particular stakeholders (i.e. Small and medium sized enterprises, public sector organisations)?

9. What are the factors that are potentially limiting the realisation of these benefits? For instance, on a scale of 1 to 5, where 1 is "Very limiting" and 5 is "Not at all limiting".

The effectiveness of PETs  
Perceived technological barriers  
Perceived staffing/training barriers  
Lack of cooperation action between data controllers and national authorities  
Limited usage amongst other organisations  
The size of the private sector firms (data controllers) involved  
Lack of awareness  
Other 1 – please state  
Other 2 – please state  
Other 3 – please state

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

10. What are the three key activities that might be undertaken by national authorities/ business associations/ consumer associations (delete as appropriate) to ensure the realisation of these potential benefits?

11. How should PETs be deployed in order to increase protection of personal data resulting in an economic advantage to a deployer (data controller)? How feasible and effective might this be?

European Commission DG Justice, Freedom  
and Security: Study on the economic  
benefits of privacy enhancing technologies (PETS)



---

SECTION 4: The impact privacy enhanced technologies

---

11. Can you think of any information, research or evidence that may be available in relation to the deployment of PETS? This information may relate to data processing cases with or without the deployment of PETS and could involve either public or private sector organisations. ☐

12. Can you think of any data processing cases that have occurred with or without the deployment of PETS (full or partial) that might warrant further analysis or consideration? These data processing cases may apply to either public or private sector organisations. ☐

13. Would you be able to provide any information on the outcome of these cases? ☐

14. We would like to get in touch with some of these organisations to discuss the impact and outcomes associated with PETS. Would you be able to provide any contact details/ organisation information in relation to these data processing cases? ☐

---

Thank you for your cooperation!

---

## rNPV of pharmaceuticals – model parameters

The following table contains the parameters of the model used in the GENOMatch case study (case study I) presented in Section 5.2.

| Table 26: rNPV of pharmaceuticals – model parameters |                  |
|------------------------------------------------------|------------------|
| Parameter                                            | Value            |
| Preclinical                                          |                  |
| Duration                                             | 1                |
| Annual Cost                                          | \$2,000,000      |
| Likelihood of Reaching Revenue                       | 10%              |
| Phase I                                              |                  |
| Duration                                             | 1 (1.5 in CASE2) |
| Number of Subjects                                   | 60               |
| Cost Per Patient                                     | \$12,000         |
| Animal Studies Phase 1                               | \$500,000        |
| Annual Overhead (Other Costs)                        | -                |
| Likelihood of Reaching Revenue                       | 25%              |
| Phase II                                             |                  |
| Duration                                             | 2                |
| Number of Subjects                                   | 200              |
| Cost Per Patient                                     | \$12,000         |
| Animal Studies Phase 2                               | \$1,000,000      |
| Annual Overhead (Other Costs)                        | -                |
| Likelihood of Reaching Revenue                       | 35%              |
| Phase III                                            |                  |
| Duration                                             | 3                |
| Number of Subjects                                   | 2,000            |
| Cost Per Patient                                     | \$6,000          |
| Animal Studies Phase 3                               | \$1,500,000      |
| Annual Overhead (Other Costs)                        | -                |
| Likelihood of Reaching Revenue                       | 72%              |
| Approval                                             |                  |
| Duration                                             | 2                |
| FDA Fees (PDUFA II)                                  | \$309,647        |
| NDA/BLA Preparation Fees                             | \$1,000,000      |
| Annual Overhead (Other Costs)                        | -                |

| Table 26: rNPV of pharmaceuticals – model parameters |         |
|------------------------------------------------------|---------|
| Parameter                                            | Value   |
| Likelihood of Reaching Revenue                       | 81%     |
| Financials                                           |         |
| Patient Population                                   | 750,000 |
| Annual Revenue Per Patient                           | \$250   |
| Peak Market Penetration                              | 50%     |
| Patient Population Growth Rate                       | 0       |
| Ramp to Market Peak                                  | 2       |
| Discount Rate                                        | 15%     |
| In-licensing Royalty Rate                            | 5%      |
| Manufacturing and Marketing Offset                   | 60%     |
| Year Patent Protection and Revenues End              | 21      |
| Annual Ramp Overhead (Other Costs)                   | -       |
| Annual Peak Revenue Overhead (Other Costs)           | -       |

Note: Figures in the report were converted into € using an exchange rate of 1.374.

**Source: Stewart (2004)**

## Exploratory case Studies

The Annex contains a summary of the case study evidence we collected during the initial stages of the study. This part of the study was exploratory in nature and intended to provide a high level overview of the type of PETs used by data controllers across the EU. This research formed the basis for the detailed case studies included in section 5.

This annex starts with a description of how case studies were identified and classified, followed by a discussion of some of the issues that the studies highlighted. These included the role of e-Government and the costs involved in PET deployment as well as other drivers such as fear of legal liability, sanctions and data loss. Some measurement issues involved in conducting cost benefit analyses using case study evidence are then described.

### Case study identification

The terms of reference require us to examine “various data processing cases with and without deployment of PETs” in order to identify and, where possible, to quantify benefits of PETs for data controllers. Consequently, we have considered a wide range of processes that involve the use of digitised personal data, including cases where no, or only weak, PETs are used, or where PETs are used ineffectively.

The stakeholder consultation exercise described in the last chapter involved an assessment of the experiences of the various Member States with regard to privacy issues and privacy enhancing technologies. This fed directly into the identification of a number of case studies. Having provided detailed background on their national contexts, national data protection authorities, business associations and consumer associations were asked to provide additional information that might assist in the selection of cases representative of their country experiences. In order to accurately reflect the economic dynamics involved with privacy issues and PETs, four types of case studies were collected, covering:

- the supply of privacy enhancing technologies themselves;
- privacy issues faced by citizens and their resultant demands for privacy;
- organisations’ experiences of PET deployment and associated costs; and
- the benefits of privacy enhancing technologies, encompassing economic and non-economic benefits.

PETs were identified on the basis of the definition provided in Section 2. The case studies thus cover not only pure PETs (such as privacy-by-design applications), but primarily relatively low-level PETs at the data-security end of the spectrum. While we do not claim that the selection of PETs in the case studies reflects the true distribution of these technologies in the market, the preponderance of relatively simple technologies, such as encryption and information access management is in accordance with stakeholder perceptions.

The problem with some of these technologies is that they are sometimes used in applications that are inherently privacy-invasive. Improving the security of data transmission or data storage by encryption, de-identification and information access management enhances privacy by

“preventing unnecessary and/or undesired processing of personal data”. However, other elements that are characteristic of pure PETs, such as data minimisation and transparency, are missing in many of the applications we found. Some of the applications we looked at thus represent examples where PETs could be used more effectively, or where stronger PETs could be used instead of weaker ones.

Twenty case studies have been conducted to date across ten Member States. This was done in a case study process involving iterations combining several rounds of telephone interviews to collect primary evidence and cross-country comparative analysis, details of which will be outlined in the rest of this Annex.

## Case study overview

In light of the approach to identifying case studies outlined above, an appropriate framework was required to organise and analyse the information collected. This is shown in Table 27 overleaf. Case studies are organised on the basis of:

- the type of organisation studied;
- their motivation for collecting personal data;
- the costs and benefits involved; and
- the resulting adoption rates of PETs, where applicable.

If fields are highlighted in a given row, an indication is made with regard to the information provided within the case study. The mode of analysis of the case studies ranges from “mini” cost-benefit analyses in which a case is made for or against PETs, to analyses of particular technologies and privacy issues. A refinement of the analytical framework will be an important task during the later stages of the project.

At a high level, it was observed that twelve of the data controllers stored personal data for efficiency purposes, or put another way, for operational/business process reasons. Most of these were engaged in some form of e-Government activity seeking to improve the transmission of information between citizens, businesses and public administrations. Ten data controllers collected personal data for the production of goods and services. These examples are concentrated largely in the private sector, for example, among market research firms, for whom personal data is a key asset. Some other production examples come from the public sector, where personal data is used in for social goals, for instance, to improve educational outcomes in the eSchool example from Estonia, or for the provision of employment services in an example from Malta.

The costs of PETs deployment to data controllers tends to be low more often than it is high, either because the PET itself is cheap or because governments are involved in making it cheaper for the data controller in some way. For example, governments may pay for the majority of infrastructure costs, which are often the most expensive component of information security systems. Where government is involved, there seems to be widespread take-up of PETs, which may partly be related to cost but is also related to the fact that every individual and firm has to interact with



public agencies, so the use of technologies that make these interactions easier seems to be a natural choice for users.

Many data controllers adopt PETs because they are worried about the risks associated with personal data, either through data loss itself or through sanctions that might be imposed by national authorities. There is less emphasis on the benefits to be achieved through PETs. However, the improved efficiency of public administration is associated with cost savings while private sector benefits include increases in output, quality and competitive advantage. While protecting privacy as a principle was also mentioned in several instances, the economic benefits of this are difficult to measure. The rest of this chapter provides an analysis of some of the key issues coming out of the case study evidence.

Table 27 Exploratory case studies: overview

| Case No.            | Types of organisation involved |              |         |       | Motivation for storage/transfer personal information |            | Costs of PETs to data controllers |                | Benefits of PETs |                             |                |              |             | High adoption rate |
|---------------------|--------------------------------|--------------|---------|-------|------------------------------------------------------|------------|-----------------------------------|----------------|------------------|-----------------------------|----------------|--------------|-------------|--------------------|
|                     | Public                         |              | Private |       | Efficiency                                           | Production | Fixed costs                       | Variable costs | Cost saving      | Increase in output/ quality | Comp advantage | Reduced risk |             |                    |
|                     | National                       | Sub-national | Large   | Small |                                                      |            |                                   |                |                  |                             |                | Of data loss | Of sanction |                    |
| CZ01                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| DK01*               |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| DK02                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| DK03* <sup>1)</sup> |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| DE01                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| DE02*               |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| EE01                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| EE02                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| ES01                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| IT01                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| IT02                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| MT01                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| MT02                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| MT03                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| MT04                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| NL01*               |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| AT01                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| AT02                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| UK01                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |
| UK02                |                                |              |         |       |                                                      |            |                                   |                |                  |                             |                |              |             |                    |

Note: Key: dark red shading indicates relatively high costs and light red shading indicates relatively low costs. 1) We are aware of two live applications of the PET (RFIDsec) in DK, one by public libraries, one by a furniture manufacturer. \* These case studies were selected for further analysis and are discussed in detail in the main report in Section 5.

Source: London Economics

## e-Government and PET deployment

Table 27 shows that thirteen PETs applications in the public-sector and nine in the private sector.<sup>107</sup> The split between larger and smaller organisations within the private sector is relatively even. The largest deployment of Privacy Enhancing Technologies tends to be initiated by government agencies. Examples include *FinanzOnline* offered by the Austrian Federal Ministry of Finance implemented to improve the efficiency of tax collection; the Estonian eSchool programme and the Maltese government's Common Database.

The technologies involved aim almost exclusively to facilitate communications between various arms of government and private individuals/industry, i.e., the motivation for storing and transmitting personal data comes from a desire to improve public administration processes. This is achieved through a reduction in invalid communications with government agencies (e.g. incorrectly completed tax forms) and an increase in the pace with which officials receive and treat personal data relative to what was possible under the postal system.

The deployment of PETs through these government information systems may be one of the fundamental drivers of PETs in society today. Take-up rates appear to be high in the Austrian *FinanzOnline* case, with the number of users increasing tenfold over a period of six years; the number of people undertaking their sales tax filings using this system has risen by close to 70% over five years and the number of people filing income tax returns through the system has almost doubled over the same period.

The fact that large e-Government systems backed by PETs exist may be the reason why private data controllers are encouraged to “piggyback” their interactions with their customers using these secure communication channels. Some respondents were keen to accredit adoption rates directly to the security of these systems but it is difficult to make this point from an economic perspective. Firstly, as an empirical exercise, it is difficult to untangle e-Government technologies from the PETs embodied within them. Secondly, it is not clear whether the privacy features of these technologies are particularly valued or whether their general functionality is paramount. There is reason to believe that the latter is the more important driver of take-up and that privacy *per se*, is not the reason for the take-up of PETs, which is the message echoed in each of the above chapters.

In sum, the case studies point to the likelihood that the economic benefits of e-Government technologies cannot easily be assigned to PETs.

## e-Government and the cost of PET deployment

Regardless of the reasons for take-up, the move away from paper-based systems to e-Government systems is likely to improve the security of personal data, thereby reducing privacy risks. The assignment of economic benefits to technologies embodying PETs may therefore be a subtler issue than appears to be the case at a first pass. By government bearing the infrastructure costs associated with secure technologies, they create an ICT platform for private data controllers to build upon; this initiates a technological adoption process in which individual privacy protection

<sup>107</sup> Two of the case studies concern applications used by both public and private sector data controllers.

becomes the *status quo*. As discussed in the UK case study on market research, individuals may give away their personal data for a variety of reasons unconnected to privacy, despite being concerned about privacy issues. PETs can therefore play a useful role to individuals that may not demand privacy as actively as one might expect given their stated values (e.g. as described in Section 3.2).

In practice, the use of government-initiated privacy enhancing technological infrastructure by data controllers is likely to occur at advanced stages of PET adoption that are unlikely to be observed in most countries at the current time.

## Cost sharing and PET deployment

Direct government involvement is not the only way in which PET deployment can take place. One of the few case studies conducted with a vendor of PETs, in the Netherlands, highlighted the ability of sub-national organisations with limited budgets to collaborate with one another to deploy PETs. The study observes how organisations sharing personal data can strike cost sharing arrangements to lower the cost of PET adoption. It is interesting to note, however, that as a general rule, where the cost of PET adoption to data controllers is lower, adoption rates seem to be higher. This is seen in each of the examples in which we have adoption rates data as well as cost information. Therefore, while the Dutch example is encouraging about the capacity of private sector data controllers to initiate PET deployment, it must be stressed that at present, the firm considered in the Netherlands only has twenty clients.

## Drivers of PET deployment

### *Legal liability and sanctions*

Without a doubt, one of the key drivers of PET deployment in Member States is legal liability and sanctions. In the case of the Dutch example described above, hospitals are compelled to take on privacy enhancing technologies or face fines in the order of € 2,000 per day.

SMEs appear to be particularly driven to adopt PETs because of legal requirements; however this is also the case for some non departmental public bodies. For example, The Danish Coastal Authority anonymised its CCTV system after being required to do so by the data protection authority. Likewise, a nightclub in Denmark deployed a PET in order to implement its fingerprint-based entry system. Meanwhile, even public agencies, such as those in Italy, need to undertake costly and time-consuming consultations with data protection authorities before implementing new systems to check whether they may be any issues with privacy laws.

This is interesting because the traditional view of privacy enhancing technologies is as a substitute for privacy law (which is considered to be less effective online than it is offline). However, a number of our case studies point to the possibility that legal channels can be used to encourage PET adoption as part of the motivation for adoption is avoidance of legal liability and sanctions.

### *Prevention of data loss*

Some firms and public bodies described prevention of data loss as a motivation for adopting privacy enhancing technologies. As might be expected, this was a key concern for banking

organisations, who tend to be front runners in the field of information security because losses of personal data translate directly into monetary losses. In contrast, the likes of market research firms (e.g., the consultancy firm TNS Infratest in Germany) either do not use PETs or adopt very crude privacy enhancing technologies. This is surprising given the centrality of personal data to the businesses of market research firms. A privacy breach could potentially imply the loss of millions of Euros of revenue, while PETs can help firms to earn rents on proprietary information.

### ***Forward looking firms***

A particularly interesting driver of PET adoption comes from the pharmaceutical arena, where firms appear to be self-motivated to adopt privacy enhancing technologies. Pharmaceutical companies in Germany for example, describe how they place special emphasis on using PETs in relation to their genetic research programmes. On some level, this is out of a concern for legislation that might restrict research in the future without the use of PETs.

However, respondents to this case study also stressed that if privacy becomes a concern for research participants in the future, especially in relation to keeping their genetic data secret, they want to have the technological solutions ready and in place. The reputational benefits that might be gained in the future were identified as outweighing the cost of PETs because of the potential competitive edge pharmaceutical companies can gain on one another by being able to access a stream of research participants that contribute innovation breakthrough.

### ***Conclusion***

The drivers of firms and public agencies to adopt privacy enhancing technologies are interesting to note. Among private companies, a minority of large entities are interested in adopting PETs. These include banks, whose success fundamentally relies on their security procedures; and pharmaceutical companies, whose profitability could also rest on reputation in the future, insofar as they are able to protect participants in genetic research. However, even companies with a strong interest in data protection usually opt for tried-and-tested, but low level PETs, eschewing the (arguably more demanding) task of redesigning their business models to include privacy by design and use PETs that minimise data or provide reliable anonymity for individuals.

Among public companies and SMEs, the key drivers behind PET adoption are legal requirements and the associated sanctions. This suggests that encouraging PET deployment can either be achieved through further legal channels or via large companies/government taking a leadership role in commercialising PETs.

## **Cost-benefit analyses**

### ***Non-economic benefits***

One of the most fundamental measurement issues is that of understanding the non-economic benefits of PETs. Viewing privacy as a principle, it is far more difficult to put a valuation on it relative to straightforward economic losses and gains that might also be involved. Specifically, non-economic benefits are difficult to compare and aggregate because it hard to gauge how important the discomfort of a lack of privacy is to different people. In the Alcobendas case in Spain for example, it is difficult to pin down the value of making citizens aware of their rights. Likewise,

in the case of the PETs involved in the secure transmission of crime notifications in Italy (IT02), the differences in how much citizens' value privacy with regard to their criminal infractions are unclear.

### ***Measuring the benefits for data controllers***

So far we were able to collect quantitative information that could permit simple cost-benefit analyses of PETs only in a handful of cases. However, the legal requirements that drive the adoption of PETs poses a problem for these exercises if they are aimed at understanding *voluntary* adoption of PETs among data controllers.

On the one hand, in order to measure the economic costs and benefits of a PET for a data controller, the PET should be *separated* from the technology in which it is embodied. In the case of the Danish Coastal Authority, it is apparent that the PET was implemented as an afterthought relative to the need for CCTV. The benefits of the technology described are therefore more due to the CCTV system itself rather than the PET component. In addition, PET adoption was not voluntary.

On the other hand, legal requirements could be taken as reflecting the demands of citizens for certain levels of privacy in society. If this is the case, citizens will use new technologies contingent on their use of PETs. Where this is the case, cost-benefit analysis can evaluate new technology-PET combinations *together*.

In order to distinguish between the two cases outlined above for the purposes of cost-benefit analysis, it is important to understand how widely adopted a given technology would be in a counterfactual legal environment, i.e., how widely adopted a given technology would be if data controllers were not mandated to use PETs.

### ***Summary of cost-benefit analyses***

Given the above caveats, a summary of the costs and benefits relating to the case studies is provided below, where applicable.

| Table 28: Exploratory case studies: selected summaries                                                                     |                             |                                                             |                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------|-----------------------------|-------------------------------------------------------------|---------------------------------------------------------------------------------|
| Case study name                                                                                                            | Type                        | Costs                                                       | Benefits                                                                        |
| CZ01: Electronic system of the Single Registration Form applying for trade license and notification of changes to business | e-Government PET deployment | € 8-€ 39 per certificate                                    | Ease of obtaining licensing                                                     |
| DK01: The Danish Coastal Authority – Privacy zones in CCTV surveillance                                                    | PET adoption                | € 10,700 plus 1-year of consultation                        | € 13,500 due to reallocation of resources plus 7.5% reduction in staff costs    |
| DK03: Crazy Daisy – fingerprint identification*                                                                            | PET adoption                | PET cost plus € 100-€ 150 fee for data protection authority | Speed up processing entry into nightclub; reduced verbal and physical assaults; |

|                                               |                                                                                                     |                                                                                  |                                                                                                                                           |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
|                                               |                                                                                                     |                                                                                  | reduced staffing costs                                                                                                                    |
| DK04: RFIDsec*                                | PET design and deployment                                                                           | € 0.5 per chip                                                                   | Improvement of operational efficiency in the supply; protection against fraud and illegal activity; product transparency and safety; etc. |
| DE01: TNS Infratest (DE)                      | Data breach                                                                                         | € 28 million at risk                                                             | N/A                                                                                                                                       |
| DE02: GENOMatch (DE)*                         | PET design                                                                                          | N/A                                                                              | N/A                                                                                                                                       |
| EE01: Genome project                          | PET adoption                                                                                        | Overall annual IT budget of € 64,192                                             | Facilitation of genetic research                                                                                                          |
| EE02: eSchool                                 | PET adoption                                                                                        | eSchool packages (incl. PETs) range from € 112-€ 23 per month                    | Efficiency improvements in schools (through administration) and improved schooling outcomes expected                                      |
| ES01: Alcobendas data protection              | Local government PET adoption and awareness raising of privacy issues                               | Unavailable                                                                      | Increased awareness of rights relating to privacy                                                                                         |
| IT01: CRS – Regione Lombardia                 | PET adoption                                                                                        | < € 5 per card                                                                   |                                                                                                                                           |
|                                               | Access to social and health and other services online; and online access to patient medical history |                                                                                  |                                                                                                                                           |
| IT02: data transmission of crime notification | PET adoption                                                                                        | € 43 million over 3 years                                                        | Direct benefits of € 46.9 million per year                                                                                                |
| NL 01: PET vendor*                            | PET design and deployment                                                                           | € 50,000-€ 75,000 initial cost                                                   | Avoidance of fines totalling € 2,000 per data; benefits of collecting longitudinal health data                                            |
| AT01: FinanzOnline                            | e-Government PET deployment                                                                         | Unavailable                                                                      | Reduction of invalid filings; increased rate of processing documents; staff reduction of approx. 500                                      |
| AT02: EDIAKT II                               | e-Government PET deployment                                                                         | € 2 per head of population in the authority area in year one, € 0.15 ongoing fee | Various efficiency savings                                                                                                                |

Note: These case studies were selected for further analysis and are discussed in detail in the main report in Section 5.

Source: London Economics

## Overview summary

This Annex provides some feel for the rationale and extent of PETs deployment across the Member States considered as part of this analysis. There are differences in the reasons for adopting PETs between the various organisations depending on the nature of the organisations and the legal framework in which the organisation operates. In addition, the primary benefits associated with the deployment of PETs are varied – and can relate to business generating competitive gains over other organisations in the same market to governments attempting to generate efficiency savings through the better provision of public services. Given the range of PETs and rationale for deployment, assessing the costs and benefits is difficult, especially when attempting to isolate the role of the PETs in facilitating the operation of a particular form of online activity and the activity itself. The individual case studies are described in the remainder of the Annex.

## Austria

### AT01: FinanzOnline

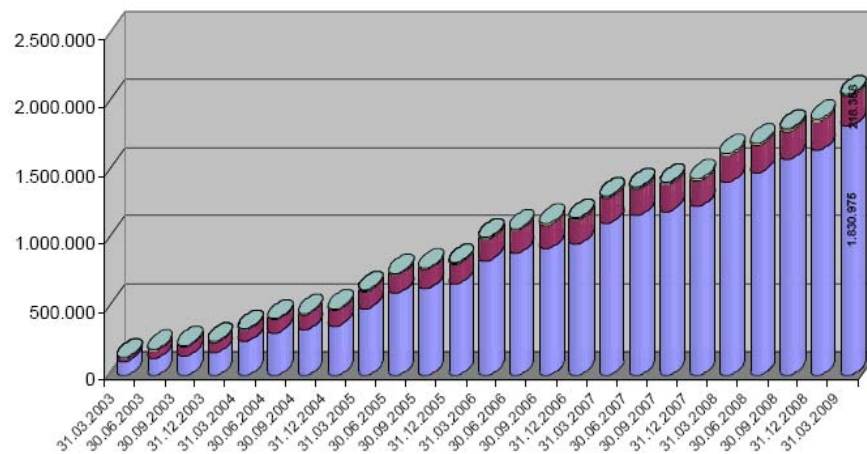
FinanzOnline is a service offered by the Austrian Federal Ministry of Finance by which individuals, businesses and local authorities can:



- file their federal taxes statements or annual accounts (E-Bilanz) online;
- receive tax assessment notes electronically (DataBox);
- file a variety of other official statements/requests; and
- manage relevant information held by the Ministry.

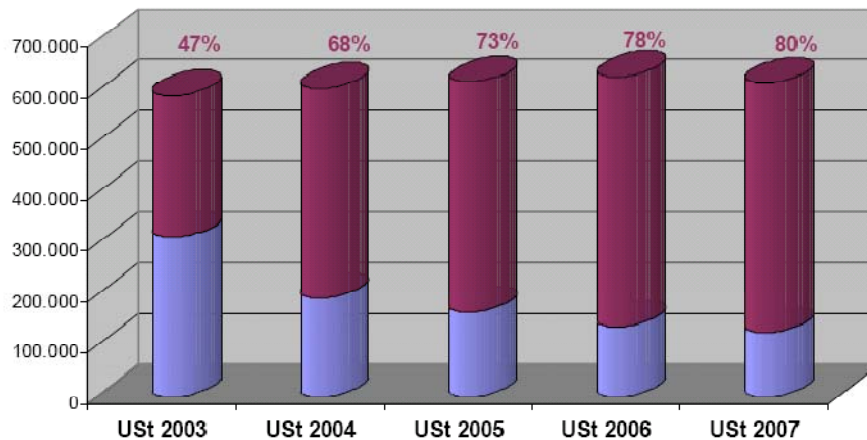
The system enjoys considerable popularity with the Austrian public. The service recorded more than 2 million users in 2009, almost a quarter of the population.



**Figure 47: Users of FinanzOnline (as of March 2009)**

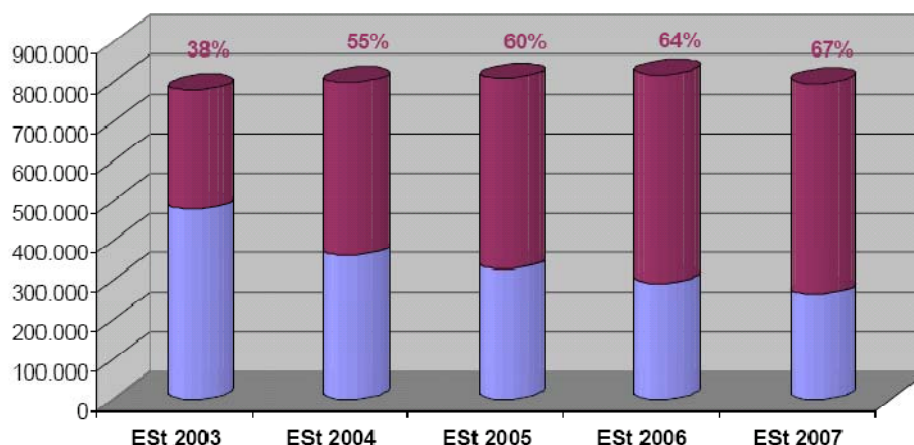
Source: Waldecker, E., 'Steuern zahlen im Internet – Ein neues Service von FinanzOnline'. Presentation at the e-government conference, Vienna, 18 June 2009

The take-up of the various services offered through FinanzOnline has been quick. Within 4 years, the proportion of businesses filing their sales tax returns online increased from 47% to 80%.

**Figure 48: Proportion of sales tax return filings via FinanzOnline (as of April 2009)**

Source: Waldecker, E., 'Steuern zahlen im Internet – Ein neues Service von FinanzOnline'. Presentation at the e-government conference, Vienna, 18 June 2009

A similar, albeit slightly less pronounced trend can be observed with individuals' income tax filings, where the most recent figures shows that two thirds of liable individuals file their returns online.

**Figure 49: Proportion of income tax return filings via FinanzOnline (as of April 2009)**

Source: Waldecker, E., 'Steuern zahlen im Internet – Ein neues Service von FinanzOnline'. Presentation at the e-government conference, Vienna, 18 June 2009

### **Benefits of FinanzOnline**

For users (citizens, businesses and the administration), the system offers a number of benefits, primarily in terms of speeding up the administrative process. Examples of benefits include:

- reduction of invalid filings through standardised online input and real-time verification; and
- increased through-put (no need for postal delivery of documents, manual intervention only in cases requiring additional checks).

The Ministry of Finance estimates that the system reduces the processing time for each tax return by 3 minutes, which leads to savings equivalent to the annual workload of 482 clerks. Similarly, the system reduces the volume of advice handled over the phone, saving 186 full-time posts.<sup>108</sup>

### **PETs used in FinanzOnline**

The personal information that is disclosed during the process is highly sensitive. PETs consequently have a crucial role within the system. In a first step, FinanzOnline was developed using only programmes and programming languages that are currently held to be secure. Further, FinanzOnline is protected by a range of PETs that can be categorised as follows:

- PETs for secure data transfer; and
- PETs to protect stored personal information.

<sup>108</sup> See Makolm, J., 'FinanzOnline - E-Taxation in Österreich'. Presentation at the E-Government Fokus conference, Bern, 27 October 2006.

Several PETs secure the transfer of data to the system. Users are assigned unique IDs to access the system and access is further secured by alpha-numeric 8-10-digit password. With the Secure Socket Layer Protocol 3.0 (SSL), the system uses a high standard of encryption (168 bit). SSL ensures that the data exchanged during a session are complete and uncorrupted.

The system also monitors sessions and closes them if it detects potential sources of insecurity, for example long periods of inactivity by the user (time out), during which data might be visible contrary to the user's wishes. Finally, the FinanzOnline server uses a security certificate, by which users can verify that they are communicating with the correct server.

Once data are received by FinanzOnline, they are protected by another suite of PETs. They include an array of firewalls, user authentication and active scanning software to detect unusual operations.

In addition, the Ministry of Finance deploys technologies that allow the tracing of attacks against the site. In conjunction with the threat of criminal sanctions, such programmes act as a deterrent against attackers.

### **Conclusion**

FinanzOnline is a classic case in which providing a service that was hitherto paper-based online brings substantial cost savings. The popularity of the system with the Austrian public can be seen by the high take-up rate.

PETs in this context are an integral component of the service: few people would entrust their financial information to a system they consider insecure. The Ministry of Finance has been able to win the trust of Austrian taxpayers by deploying a number of state-of-the-art PETs as part of a user-friendly application that brings genuine benefits in terms of speed and convenience for taxpayers, as well as considerable cost savings for the administration. The fact that – as far as one can see – the PETs that are used are off-the-shelf technologies with a track record of success in other online applications (e.g. electronic banking), shows that data protection in many cases is not primarily a technological problem, but rather a question of integrating known technologies into well-designed applications that work with users to deliver services in which security is an integral part of their overall utility.

However, the fact remains that the Austrian Ministry of Finance collects large amounts of highly sensitive personal data. PETs have not been used to develop a less privacy-invasive model of tax collection.

## **AT02: EDIAKT II**

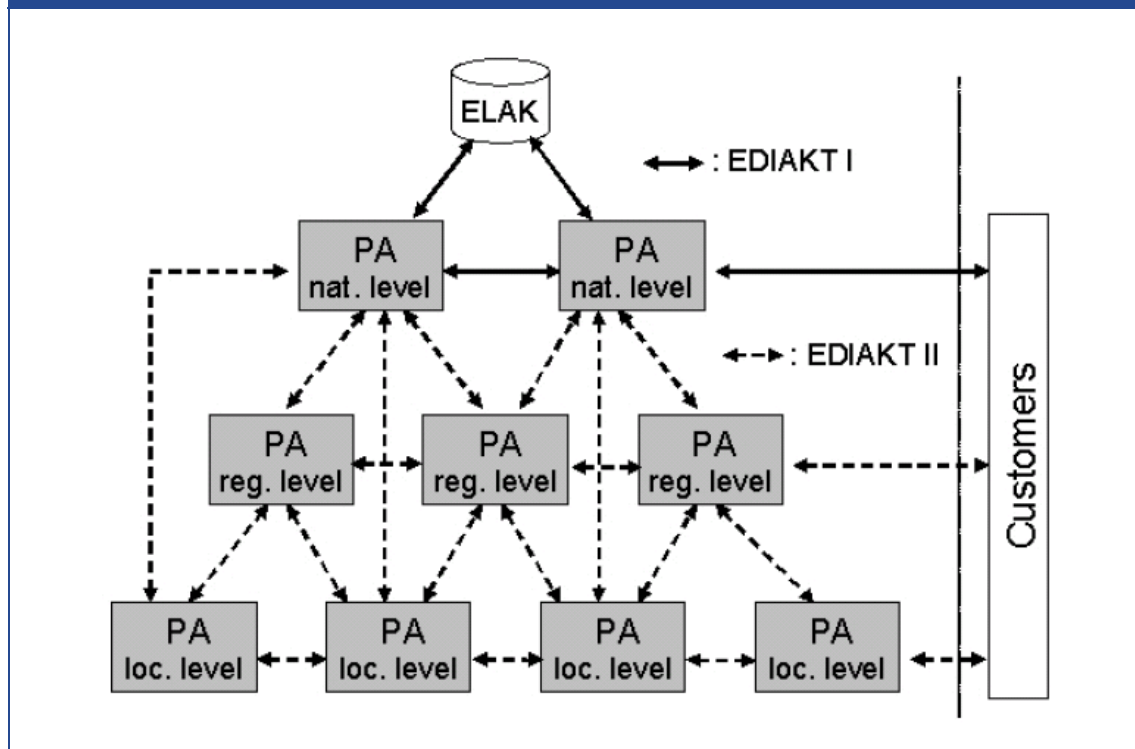
EDIAKT II is an XML-scheme defining the universal structure and attributes of the electronic file system used by the public administration in Austria. It allows the exchange of administrative objects (files and processes) between different agencies within the Austrian administration at the federal, regional and local level.<sup>109</sup> The system was introduced in 2005, building on an earlier

---

<sup>109</sup> See <http://www.ag.bka.gv.at/index.php/EDIAKT:Deckblatt>.

version that was limited to the federal government level and businesses that use its services. The chart below shows the flow of EDIAKT messages between public authorities and customers in Austria.

**Figure 50: Electronic file exchange via EDIAKT**



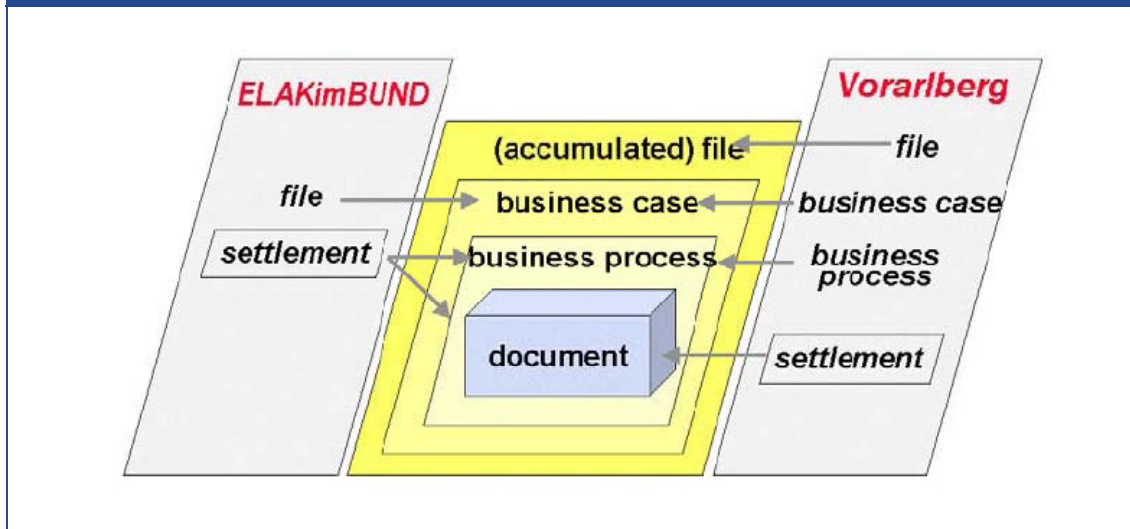
Note: PA = public administration; ELAK = electronic file system.

Source: Cimander et al (2006), 'Standardised e-Form exchange via EDIAKT II in Austria'. Available at: [http://www.egov-iop.ifib.de/downloads/GPC\\_IOP\\_in\\_EDIAKT2\\_Austria.pdf](http://www.egov-iop.ifib.de/downloads/GPC_IOP_in_EDIAKT2_Austria.pdf)

EDIAKT messages are XML objects that can contain various kinds of data, including documents in standard formats, such as .pdf, .doc, etc. Such objects are created for every administrative procedure that requires further action or needs archiving. Thus every procedure can be audited anytime by viewing the file (which is a legal requirement in Austria).

EDIAKT II objects can be visualised as cascades of data envelopes. The figure below shows two examples: on the left is a relatively simple one from the federal level, in which the outer envelope constitutes a business case, which contains a business process, which in turn contains a document. On the right is an example from the regional level in which a complex EDIAKT II file contains a business case, in which individual processes and documents are enclosed. A business process containing a document is the smallest bundle of objects that can be sent in an EDIAKT II message.

Figure 51: Two examples of EDIAKT II objects



Source: Cimander et al. (2006)

### PETs in EDIAKT II

An EDIAKT II message consists of XML strings and as such is in principle freely readable by all. The security measures for transport and storage of EDIAKT II objects depends on the procedure in question and the information contained in the object and is defined by law.

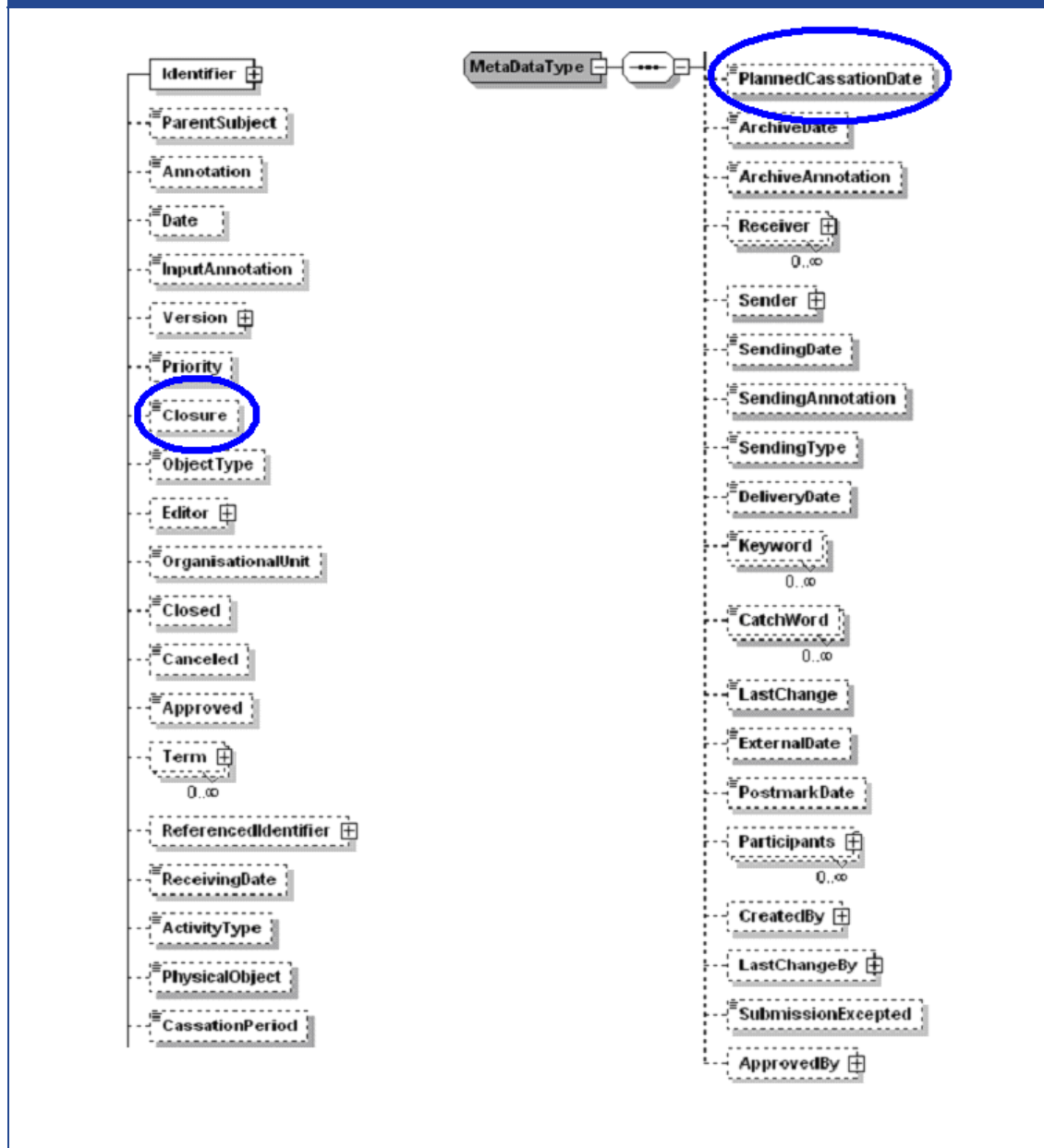
Each EDIAKT object contains metadata, which contain essential information, such as type of object, urgency, originating body, date of origination, etc., which contribute to passive data protection by assigning clear responsibilities and leaving a clear and detailed audit trail. In addition, the metadata also define more active data protection methods:

- The element 'Closure', for example, contains the protection level of the object. The protection level is defined<sup>110</sup> on a range 1 (access restricted) to 4 (top secret), and signifies that an appropriate level of encryption<sup>111</sup> must be used for all data thus classified.
- The element 'PlannedCassationDate' contains the date on which the object is scheduled for deletion. This date is determined by the cassation period (e.g. 10 years), which is typically defined by laws and regulations and depends on the object in question.

<sup>110</sup> Information Security Law, Article 2(2), <http://www.jusline.at/index.php?cpid=ba688068a8c8a95352ed951ddb88783e&lawid=390&paid=2>.

<sup>111</sup> Information Security Regulation, Article 9(5), <http://www.a-sit.at/pdfs/infosiv.pdf>.

Figure 52: EDIAKT metadata



Source: <http://www.ag.bka.gv.at/index.php/EDIAKT:Metadaten>

Moreover, the concerned IT-systems used to process the objects have to be able to restrict unauthorised access, for example by securing external access through use of electronic signatures.

### Benefits

The benefits of EDIAKT cannot be strictly separated from the benefits of the e-government applications it supports. Essentially, the benefit of switching from paper-based to electronic processing of administrative procedures is one of efficiency. Specific benefits include:

- speeding-up and standardisation of internal processes;
- easy set-up of efficient e-Government procedures;
- easier implementation of changes to the organisational structures of public authorities;
- integration of electronic forms and delivery services;
- cost savings for paper-based transport and archiving; and
- staff savings in documentation, transportation and archiving.<sup>112</sup>

As an example of cost savings from using the EDIAKT II system, the local authority of Gföhl in Lower Austria reports the speed with which files can be accessed, response-times following requests for advice and processing times for administrative actions all increased by 50%.<sup>113</sup>

A general assessment of the efficiency improvement achieved by EDIAKT I (Cimander et al, 2006) found a lower, but still impressive figure of 11% savings compared with the non-electronic case, with additional savings of similar magnitude expected from the upgrade to EDIAKT II in 2005.

### **Costs**

Local authorities can get access to EDIAKT II by joining the ELAK Government Association, which provides the EDIAKT interface as well as support with implementation and security measures. The decision to join has to be made by the local council. The one-off joining fee is € 2 per head of population in the authority area, while the annual membership fee is € 0.15 per head of population.<sup>114</sup>

### **Conclusion**

A great variety of different processes is handled via EDIAKT, only some of which involve the electronic transmission of personal data. The EDIAKT example draws attention to the fact that the protection of personal information is still in many cases dependent on institutional decisions to grant such protection. In the EDIAKT case, the assignment of protection levels is done by the government agencies, not by the individual citizen.

Another noteworthy feature of EDIAKT is the use of open standards, like XML, and open source software, which mitigates concerns about potential anticompetitive effects by creating consumer lock-in through proprietary standards.

<sup>112</sup> Cimander et al. (2006).

<sup>113</sup> See Simlinger, K. and Deimel, A., (2008), 'ELAK – Elektronischer Akt für Gemeinden – Aktenaustausch via EDIAKT zwischen Gemeinden und dem Land NÖ'. Presentation to the e-Government conference.

<sup>114</sup> Ibid.



## Italy

### IT01: CRS – Regione Lombardia

#### **Background**

The CRS, Carta Regionale dei Servizi (Regional Services Card), was initially introduced by Regione Lombardia in 2004, and it is now in use as national health services card, European health insurance card, fiscal code card (a national identification number) and national services card.

This card differs from the card distributed in other Italian regions<sup>115</sup>, because it has a smart chip that allows citizens of Lombardia to access various online services. To use online services, citizens have to obtain a PIN code, install the appropriate software on their personal computer and use a smart card reader.

The most relevant use of the card (and the services available online) to date is related to social and health services. If an individual provides consent, all the data related to the individual's health and health events (e.g. medical prescriptions, examinations, medical reports, emergency data, data relative to current treatments) will be stored in their personal file (Fascicolo Sanitario Elettronico - FSE), in order to create the individual's entire medical history. As user consent is given (as required under data protection legislation), the system is clearly inherently privacy invasive. Using the card allows for the ability to access and modify personal contact details, access all registered data and information related to health events, choose a general practitioner and book medical examinations and visits.

The CRS card also grants access to various regional services, (e.g. applying for regional grants) requiring the submission of a signed application (using the electronic signature) and to other services provided by local authorities and regions (request of a certificate, enrolling children in school etc.). Furthermore, this card can be used to access Fisconline, the online services provided by the Italian Revenue Agency.

#### **Privacy**

The creation of the file with all personal health data and information (FSE)<sup>116</sup> is optional and subject to the citizen's consent. For the FSE each health unit acts as data controller, while Lombardia Informatica (IT partner of the Region, founded and wholly owned by Regione Lombardia) is responsible for processing and treating the data (data processor). Regione Lombardia acts as a coordinator of the overall project and may treat the (anonymised) data for administrative and research purposes.

The subjects who are allowed access to personal health records (FSE) are, apart from the interested citizen, the relevant doctor when the patient is admitted to hospital and the patient's general or specialist practitioner (only after the further explicit authorisation of the patient). In

---

<sup>115</sup> A similar technology is currently in use in two other Italian regions: Friuli Venezia Giulia (where online services are currently available) and Sicilia (where online services are still to be launched).

<sup>116</sup> Detailed privacy information on the FSE is available at <http://tinyurl.com/yam5j7b>.



addition, pharmacists may have access to the record, but only if the concerned person hands in their card and limited to those data related to medicines, in order to verify possible incompatibilities. Data are treated and transmitted using data security tools: data on personal health are separated from contact details, then are digitally signed and encrypted. Authorised operators need to identify and authenticate themselves using a smart card and a PIN code before accessing the data.

When the card is used to access other services, the relevant local or central authority acts as data controller.

The Garante for Data Protection recently published the guidelines on the FSE<sup>117</sup> and, among other things, suggested that the system should be organised by modules, with the different subjects involved only having access to the part of the file directly connected with their activity (e.g. a specialist doctors only having access to data related to the treatment in use or pharmacists able to access only data on medicines and possible incompatibilities between medicines). Lombardia Informatica confirmed that they strictly adhere to the Data Protection Authority's directives and they have not encountered to date any specific problems with data protection or abuse of personal data deriving from the CRS. It is interesting to note, however, the emphasis of the guidelines on information security rather than data minimisation.

### ***State of implementation and related issues<sup>118</sup>***

As mentioned previously, the main driver for the introduction of the card was related to promoting the take up of health services. While the implementation of the health services system was centrally planned by the Region, other services have been offered by local authorities or other organisations on their own initiative.

The main objectives for the introduction of the system in the health sector were to provide citizens with better services for the prevention, diagnosis and provision of medical treatments and also to achieve efficiency and rationalisation of public expenditure in the sector, better planning and reduction in waiting lists.

As for the state of the implementation, the card has been distributed by Regione Lombardia to (almost) all citizens in the region. There are approximately 10 million cards circulating in Lombardia (covering 99% of the population)<sup>119</sup>. In the health sector, 60% of card-owners have given their consent to the constitution of the FSE, while the remaining 40% using the card to access health services, but don't have a personal file with all events recorded. Currently around 300,000 families are able to access online services from their computer, using the smart card reader.

Given the numerous actors involved, the implementation of the system took time and a series of problems arose. One main problem was connected to the integration of different systems and applications. For example, case histories are recorded using different file formats; and different

<sup>117</sup> See <http://www.garanteprivacy.it/garante/doc.jsp?ID=1634116>.

<sup>118</sup> For a comprehensive review of press articles about the CRS, see <http://tinyurl.com/ydcswaw>.

<sup>119</sup> All quantitative data presented in this paragraph were provided by Lombardia Informatica.

booking systems are in use in different hospitals. The central system had to be adjusted in order to be compatible with all the different applications. Another problem at the beginning was the incompatibility of the software with open source operating systems. Some of these problems have now been solved and we present below the adoption of the system by different categories of participants, with the main relevant issues.

The integration of the system of the different participants varies according to the category. All public hospitals and other public medical facilities (approximately 30 covering 60% of health services in the region) are connected with the system. The degree of integration for private medical facilities (around 450 due to the presence of many small laboratories covering 40% of the services supplied) is around 80% with regard to administrative database, but the capacity to upload and see clinical information is still in the early stages (with an estimated integration of 15% by 2010 rising to 100% by the end of 2013). As for online booking, at the present time it is possible to book an examination or visit online using the card in only five hospitals in the region.

Ninety-four percent of general practitioners<sup>120</sup> have adopted the system (with peaks of 100% in some provinces) and 89% have the capability to upload prescriptions online<sup>121</sup>. Almost 100% of pharmacies have integrated their facilities with the system, while there is variation between services offered. Although technically feasible, for organisational reasons it is still not possible for pharmacists to access the system and see electronic prescriptions and information related to medicines. In general data traffic is already substantial: last year 62 million prescriptions were recorded in the system, as well as 10 million medical reports.

The main limitations and challenges, at least according to the federation of general practitioners<sup>122</sup> are the following: all public and private facilities should be integrated in the system and upload information on the FSE (in most cases this is currently true only for data relative to laboratory analysis and emergency treatments in public hospitals and facilities); not all information is available in a format that ensures interoperability between systems; data should be organically arranged and presented and a patient summary, identifying the main issues for each citizen, should be developed. Also, more could be done to enhance citizens' adhesion and participation.

For what concerns non-medical services, the range of services accessible through the card depends on the different organisations (local authorities but also private organisations). The fact that the card is in use by almost all the population makes it an ideal tool for the delivery of many other services. Examples are access to library services and the integration of the card with the system managing access to all ski resorts in the Region (realised along with significant investment in hardware/software for a technological upgrade of the system).

---

<sup>120</sup> There was resistance at the beginning from a number of general practitioners to the introduction of the system for two main reasons: general resistance to technological change and upgrade of IT facilities; possible concerns that the system may be used for tighter activity controls by the Region. Also some articles reported there were concerns for the privacy in relation to the adoption of the system.

<sup>121</sup> At the present time all prescriptions have to be made and kept in paper format, but may also be uploaded online in electronic format.

<sup>122</sup> See [http://www.crs.lombardia.it/resources/rassegna/N1225e7ba816cc82cf2f/N1225e7ba816cc82cf2f/ilsole24ore\\_08\\_07\\_09.pdf](http://www.crs.lombardia.it/resources/rassegna/N1225e7ba816cc82cf2f/N1225e7ba816cc82cf2f/ilsole24ore_08_07_09.pdf).

### Costs and benefits

According to estimates provided in February 2009<sup>123</sup>, the introduction and distribution of the card, and the launch of online services, had cost nearly € 500 million. The Ministry for Innovation and Public Administration presents an estimate of the cost difference of a smart chip card (which, as mentioned above, grants access to several services), compared with a traditional health services card (with no chip and whose use is limited to health services only). According to this estimates, the cost of a smart chip card is less than € 5 higher than a traditional health services card, while the annual management cost of the PIN-Password system is around € 1-2. At this stage, there is no information on the cost savings associated with the introduction of the smart card in Lombardy.

## IT02: data transmission of crime notification

### Background

The Italian Ministry for Innovation and Public Administration, together with the Ministry of Justice and the Ministry of Home Affairs, has launched a project directed to modernise and accelerate the data transmission of crime notification between the police and the Public Prosecutor's Office (*Procura*). This project is part of an e-government plan aiming to innovate and modernise the public administration and generate efficiency savings and better services.

The project<sup>124</sup> aims to accelerate and facilitate the investigation process through the electronic data transmission of crime notification from judicial police forces to the relevant Public Prosecutor's Office. The project plan is such that, when a crime is notified, the crime notification will be automatically recorded in the appropriate register of the relevant file for the use of the public prosecutor and the *giudice per le indagini preliminari* (a magistrate with warranty and decisional functions during preliminary hearings<sup>125</sup>) will be automatically generated. When the system is operative and the project is fully implemented, the police will be able to digitally copy the crime notification and all relevant documents, and to transmit them, digitally signed and encrypted, to the appropriate *Procura* (Offices of Public Prosecutor). This system will employ a private network utilised by police forces (Polizia di Stato, Carabinieri e Guardia di Finanza) with the use of dedicated lines of communication and direct connections.

### Timeline and costs

The service was launched in January 2009, and from the end of June is active (as an experiment) in three *Procura* in Southern Italy, Napoli, Nola and Torre Annunziata. By the end of the year the system should be operative in two *Procura* in Northern Italy (Milano and Monza). It will then be extended to all judicial police forces and *Procura* in Southern Italy. The introduction of the system in all other *Procura* will depend on the availability of financial resources. It is expected that by the

<sup>123</sup> See <http://tinyurl.com/ya3txyv>.

<sup>124</sup> Information available at <http://www.e2012.gov.it/egov2012/?q=content/trasmissione-telematica-delle-notizie-di-reato-hp>.

<sup>125</sup> The GIP (*giudice per le indagini preliminari*) decides on the public prosecutor's or the different parties' requests during the preliminary hearings (preliminary phase of the criminal prosecution, directed to gathering evidence). At the end of the investigations, the GIP decides whether to dismiss the case or to proceed with the formal incrimination.

end of 2010 the system will be fully implemented in at least one of the three *Procure* in Southern Italy.

The main costs relate to the data transmission system (it was originally planned to connect police forces and *procure* using fibre optics, but now alternative, less expensive, solutions are being considered) and the need to equip all police stations with the necessary facilities (and possibly to dedicate staff specifically to the system management). Total cost estimate for the project over the period 2009-2012 is € 43 million. Part of the cost is covered by European Funds: € 2.6 million are already funded within the National Operative Programme (PON) Security 2000-2006 and the remaining € 20 million is being funded within the PON Convergence 2007-2013.

The main economic benefit is associated to the electronic transmission of the documents: the current procedure involves the physical delivery of the documents by police officers (for obvious security reasons). Moreover it will also be possible to reduce the need for paper documentation. Further benefits are associated with a general increase in efficiency. The system will also prevent possible loss of documents and speed up access to files.

### **Privacy Issues**

The system will use a central database hosted by the Ministry of Justice, which will gather all the relevant information and documents. Concerns for privacy and security were reported<sup>126</sup> in an interview by Armando Spataro, Milan's *procuratore aggiunto* (deputy prosecutor). Mr Spataro underlined the inherent risks of a system in which all police forces have access to summary data on crime notification. The Ministry of Justice ruled out such a possibility: paper documents are copied in electronic format, digitally signed and encrypted, and they are then transmitted to the relevant *procuratore* with a key identifying the receiver. Only the relevant *procuratore* has access to the file and can grant access to the file to the assistant prosecutor that will work on the case. Other parties do not have access to the file, and the system administrator themselves can only work on the encrypted data. The system is able to trace access to the file, and it is therefore possible to control for unauthorised access.

The example only rudimentary PETs are used (encryption) and the state of privacy protection depends heavily on human actors that manage data access. However, it is difficult to see how stronger PETs could be used without compromising functionality.

---

<sup>126</sup> See <http://www.repubblica.it/2009/01/sezioni/politica/giustizia-7/intervista-spataro/intervista-spataro.html>.

## Czech Republic

### CZ01: Electronic trade licence registration



As of 1<sup>st</sup> July 2008, several amendments to the Trades Licensing Act came into effect simplifying the process by which trade licenses are issued in the Czech Republic. The amendments of the Trades Licensing Act, inter alia, do not require entrepreneurs to apply for trade licenses or change to business in person. The amendments introduced the possibility of using the Single Registration Form (SRF) to handle communications with the trade licensing office via the Internet.

#### ***Filling in the application form or notifications of changes to business using electronic SRF***

The SRF software, which is used for data entry and checking the completed form, is available to the public free of charge<sup>127</sup>. After a successfully downloading and installing the SRF application, forms can be directly sent to the applications registrar of the Trade Licensing Office or via the licensee's secure "data box". Given that firms are mandated to share information with the government, the use of data boxes is beneficial because it helps to limit misuse of personal data insofar as firms have credible records of their interactions with government.

There are three ways of sending the SRF to the trade licensing office. These possibilities are explained in detail in the next paragraph.

#### ***The costs the electronic SRF for entrepreneurs***

The cost of using the electronic SRF, and the privacy enhancing technologies behind it, depends on the way in which the SRF is sent to the Trade Licensing Office. Essentially, there are three ways of using the system:

- Using an electronic signature and sending the SRF directly to the applications registrar of the trade licensing office. In order to verify the electronic signature, accredited certification is required by law. The costs of this certification range from CZK 200 (approximately € 8) for the simplest versions to more than CZK 1,000 (more than € 39) for the most complex product licenses<sup>128</sup>. Validity extends for the period of 12 months.

<sup>127</sup> Download, installation, as well as functionality of the SRF's application is secured under SSL protocol.

<sup>128</sup> The exchange rate used 25.540CZK/EUR as on October 7th 2009 according to Czech National Bank.

However these costs cannot be entirely assigned to the use of the electronic SRF since the electronic signature is used in communication with other official authorities or business partners.

- From 11 November 2009 it will be possible to send the electronic SRF through the licensee's data box<sup>129</sup> to the data box of the trade licensing office. Establishing and using data box is free of charge for businesses. The costs of data boxes are incurred in their entirety by the Ministry of Interior.
- In addition, entrepreneurs that do not have access to ICT can still use the services of The Trade Licensing Office in person without filling in the SRF on the computer.

In sum, entrepreneurs do not bear the cost of the SRF if they use the latest "data box" technologies, which is entirely subsidized by government. They therefore serve to benefit through the new system or remain at least as well off as they were under the old system, in which applications for trade licenses were made in person.

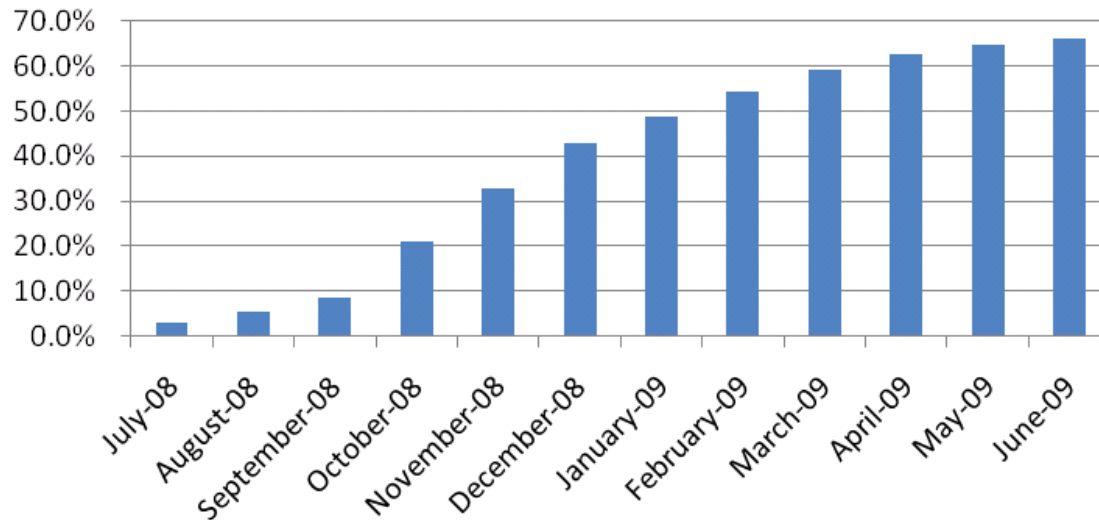
### ***The benefits of the electronic SRF***

Clearly, there are a number of economic benefits associated with the SRT – both direct and in relation to elimination of opportunity costs. The electronic SRF saves time for entrepreneurs who would otherwise have to visit the local trade licensing office as well as other bodies that used to be involved in the administration of trade licenses. Once submitted, data from the electronic SRF are automatically transmitted from the Trade Register to information systems of the Finance Office, Employment Office and Social Security Administration.

Figure 53 demonstrates the take-up of the electronic system. The average use of SRF in all localities has increased every month since its introduction and has now been adopted by more than 60% of applicants – and now becoming a part of standardised procedures, replacing paper-based substitutes.

---

<sup>129</sup> The data boxes are envisaged to be the main communication point between a citizen and public administration.

**Figure 53: Average usage of SRF filled in through electronic system**

Note: % of all SRF submissions.

Source: The Trade Licensing Office and Ministry of Industry and Commerce

In December 2008 there had been 28,783 filings using electronic SRF resulting in approximate cost savings<sup>130</sup> of:

#### For the Trade Licensing Office

- CZK 122,000 associated with 40,663 paper copies that would be needed under the old system (assumptions: on average 1.2 A4 copies per form; CZK 3 per one duplex copy of A4).
- CZK 93,600 for 3,600 consignments would that would need to be sent to other authorities involved in the administration of trade licences (assumptions: CZK 26 per consignment).
- Other cost savings resulting from the fact that the electronic SRF are more likely to contain all information necessary for validating an application in comparison to previous paper forms. This has resulted in significant cost saving from not having to contact applicants to resubmit their applications.

#### For other public authorities

- At least CZK 728,000 savings given a minimum of 10 minutes to extract data from paper forms (assuming CZK 129 per hour cost).

<sup>130</sup> Assumptions provided by The Trade Licensing Office and Ministry of Industry and Commerce.

**For entrepreneurs**

- CZK 1,856,503 resulting from time savings (assumptions: additional 0.5 hour to fill in and handle in the old form, CZK 129 per hour wage).

Given these estimates, we have estimated that the total savings for December 2008 to be approximately CZK 2,800,000 (€ 109,631). The cost savings are also increasing over time since an increasing proportion of applications are being undertaken electronically (see Figure1).

If we assume that there will be net benefits in the amount of CZK 2,800,000 every month from the beginning of the project for 10 years and discount these benefits<sup>131</sup>, we can calculate the present value of benefits.

$$PV_{\text{benefits}} = 12 * \text{benefit}_{\text{p.m.}} * \frac{(1+i)^n - 1}{i * (1+i)^n}$$
$$PV_{\text{benefits}} = 12 * 2,800,000 \text{ CZK} * \frac{(1 + 4.73\%)^{10} - 1}{4.73\% * (1 + 4.73\%)^{10}} \approx 262,886,000 \text{ CZK}$$

This simplified calculation gives us the present value of benefits of almost CZK 263 million equivalent to approximately **€ 10.3 million** in present value terms.

**Summary**

A single registration form and the PETs used to support it, enable firms to receive information from the Trade Registry; fill out forms and check the accuracy of filings; and verify information held in other public registers. The system thus fulfils a PET function by improving the accuracy of data held in electronic databases.

**Denmark****DK03: RFIDsec****Background**

The Radio Frequency Identification (RFID) tag has long been predicted a bright future as a replacement of the traditional bar code. The basic RFID tag is a chip that transmits its identification number through a radio signal. This signal is picked up by any receiver with the relevant frequency,

---

<sup>131</sup> We used yield to maturity of the ten year bond of the Czech government, ytm=4.730%p.a.



regardless of whether the signal was intended for that receiver. Compared to the traditional bar code, RFID tags have the advantages that multiple signals can be read at the same time and that the tag does not need to face any particular direction for its signal to be read.

RFID technology has been implemented by both the private and public sector in recent years. Examples include<sup>132</sup>:

- RFID tags in EU passports;
- Payment cards with RFID tags for public transportation e.g. Oyster Cards in London;
- Payment methods for toll roads which allows holders to move through a toll area without having to stop to pay e.g. Bro-Bizz in Denmark;
- Item tagging of grocery products e.g. by the Metro Future Store in Germany; and
- RFID tags in waistbands provided for children in amusement parks which allow parents to locate lost children e.g. the LEGOLAND KidSpotter.

The success of the implantation of these measures has been mixed. For instance, consumer groups have strongly opposed item tagging when introduced (for instance Metro Future Store in Germany and in Marks and Spencer in the UK).<sup>133</sup> As pointed out by Engberg et al. (2004) concerns are related to 'serious risk of abuse for commercial, political, social and criminal purposes. But especially the risk of identity theft of passive proximity tags, tracking or targeting devices could easily lead to serious breaches of security and privacy'.<sup>134</sup> Such concerns arise because RFIDs can be used to track the movement of items and people and it is difficult to control who has access to this data about movements. Moreover, in some cases information about movement of items and people may be linked to personal information in which case it is even more crucial that access to the information can be limited. Finally, more advanced versions of the RFID tag are essentially small computers with an internal memory and data stored on these RFID tags may contain sensitive information.

### ***Potential benefits to the public and private sector of RFIDs***

Despite the privacy concerns, it is widely recognised that there are potentially significant benefits to both private and public sector users of RFIDs.<sup>135</sup> Such potential benefits include:

- ***Improvement of operational efficiency in the supply chain.*** For instance, RFID tags on items may help retailers keep track of stocks and ensure that no item is ever sold out. This may help make inventories more efficient both for the retailer and for the producer.

<sup>132</sup> European Parliament (2006), 'RFID and Identity Management in Everyday Life', available at [http://www.europarl.europa.eu/stoa/publications/studies/stoa182\\_en.pdf](http://www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf).

<sup>133</sup> Ibid.

<sup>134</sup> Engberg, Stephan J., Harning, Morten B., and Jensen, Christian D. (2004), 'Zero-knowledge Device Authentication Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience' available at [http://www.rfidsec.com/docs/PST2004\\_RFID\\_ed.pdf](http://www.rfidsec.com/docs/PST2004_RFID_ed.pdf).

<sup>135</sup> See for instance Engberg, Stephan J., Harning, Morten B., and Jensen, Christian D. (2004), 'Zero-knowledge Device Authentication Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience' available at [http://www.rfidsec.com/docs/PST2004\\_RFID\\_ed.pdf](http://www.rfidsec.com/docs/PST2004_RFID_ed.pdf); Teknologi-rådet (2006), 'RFID from production to consumption' available at [http://www.tekno.dk/pdf/projekter/p06\\_rapport\\_RFID.pdf](http://www.tekno.dk/pdf/projekter/p06_rapport_RFID.pdf); or European Parliament (2006), 'RFID and Identity Management in Everyday Life', available at [http://www.europarl.europa.eu/stoa/publications/studies/stoa182\\_en.pdf](http://www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf).

Furthermore, RFID tags may contain information which can help ensure efficient handling of the goods. An example is information about the type of the product. This enables producers and retailers to know the exact contents of a container or box without having to open it and thus may imply cost savings.

- **Protection against fraud and illegal activity.** RFID tags are already used to protect against shoplifting and other types of losses in the supply chain. Furthermore, the introduction of RFID tags in EU passports is an attempt to reduce potential fraud. There is also a potential to include RFIDs in large denomination bank notes in an attempt to combat counterfeiting.

### **Potential benefits to consumers of RFIDs**

Although consumer organisations have expressed concerns about RFIDs there are also significant potential benefits of the technology to end-users. Such benefits explain why consumers in some cases do not object to the use of RFIDs. Potential benefits to consumers include:

- **Product transparency and safety.** If items are RFID tagged, information about the products such as date of production, country of origin etc. may be added to the RFID tag as well as information intended for people with allergies or health concerns. As such RFID tags may help inform purchasing decisions and empower consumers. However, some have argued that this benefit to consumers may come at the expense of small retailers who do not have the resources necessary to invest in the appropriate technology. Furthermore, product RFIDs may cause an 'information overflow' where consumers find it difficult to choose between alternative products because there are too many parameters on which they may base their comparison.
- **Tracking of lost items.** Consumers might also benefit from tracking of movements of products and persons. An example is LEGOLAND Kidspotter, where parents can buy a waistband for their children that enables them to receive updates about the location of their children in the amusement park. Similarly, RFID tags in products might help track lost valuables.
- **Development of intelligent end-user appliances.** The classic example is washing machines that can determine the appropriate washing temperature/spin cycle based on information from RFID tags in the items placed in the washing machine. Other examples include a fridge that can tell you what items you are running out of and a doorframe that can tell you if you are leaving your house without your keys, mobile phone or other essential items. The development of such intelligent end-user appliances may involve considerable future benefits to consumers.

### **European Commission Recommendations**

Recognising the potential economic and social benefits but also the privacy risks entailed in RFID the European Commission has recently published a number of recommendations on the implementation of privacy and data protection principles in RFID applications<sup>136</sup>. These

---

<sup>136</sup> European Commission (2009), 'Commission Recommendations of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification', available from: [http://ec.europa.eu/information\\_society/policy/rfid/documents/recommendationonrfid2009.pdf](http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf).

recommendations are meant to enhance use of RFID tags while ensuring that 'effective measures are in place to safeguard personal data'<sup>137</sup>. Such measures are seen as crucial for public and ethical acceptance of RFID.

Broadly speaking the recommendations sets up the following principles for use of RFID in retail trade:

- consumers should be informed about the presence of RFID in the products;
- a Privacy Impact Assessment (PIA) should be undertaken by the operator (typically the retailer or the producer);
- if the PIA suggests that the tag represents a threat to privacy, it should be removed or deactivated at the point of sale unless consumers, after being informed about details of the RFID, give their consent to keep tags operational;
- even if the PIA suggests that the tag does not represent a threat to privacy, it should be possible to deactivate or remove the tag at a later stage; and
- removal and deactivation should be free-of-charge for all consumers.

The recommendations are not legal requirements but there are provisions for follow-up at Member State level to ensure that actions are taken to attempt to implement them.

### **RFIDsec**

A common solution has been to 'kill' the RFID tag at the point of sale but this may not always be an appropriate solution because some RFID tags need to stay active for any benefits to be realised (for instance RFID tags in smartcards for public transportation).

An alternative solution is provided by the Danish company RFIDsec. They produce secure RFID tags with two key features:

- control of the chip can be transferred to the consumer at the point of sale; and
- the chip has a so-called 'secure mode' where receivers generally cannot communicate with it but the person who controls the chip can communicate with it.

These features imply that the RFIDsec tags can survive after the point of sale but if they do so only authorised people can communicate with it. Thus the chip can remain a communications channel after the point of sale while at the same time conforming to EC recommendations about RFID technology. Furthermore, the chip contains memory for storage of information and this information is secured by a strong encryption. Access to the information is only provided to authorised persons.

RFIDsec started in 2005 and had its product fully developed for sale by end of June 2009. Currently the product is being tested in a number of pilot projects around Europe and it has been fully implemented in two cases in Denmark:

---

<sup>137</sup> Ibid. paragraph 7.

- A furniture producer inserts RFIDsec into their furniture. This helps them identify counterfeit and stolen products and determine which products are covered by warranty. In this case RFIDsec was chosen over non-secure RFID technology because of the strong encryption entailed in the product and because it was considered the solution with most future potential because of the PETs included in the product.
- Libraries use RFIDsec instead of bar codes in order to obtain benefits such as productivity improvements and improved consumer satisfaction. Such benefits could not have been obtained with traditional RFID technology without compromising privacy. For privacy reasons traditional RFID tags need to be 'killed' if a book is taken out of the library implying that the library would not be able to communicate with the chip when the book was returned. On the contrary, the 'secure-mode' of RFIDsec enables the library to communicate with the chip whenever it is in the library but ensures that no one can communicate with the chip when it is outside the library.

### **Barriers to RFIDsec**

RFIDsec has all same potential benefits as the traditional RFID but without compromising privacy and thus has a greater potential for public and ethical acceptance. However, at the same time the technology faces a number of barriers.

Firstly, current RFIDsec costs about € 1 per chip whereas comparable non-secure RFID<sup>138</sup> cost about € 0.50 per chip. While part of the price difference reflects the higher security level imbedded in RFIDsec, most of the price difference is probably due to the fact that production of RFIDsec tags still is relatively limited. Comparable non-secure RFID tags are produced on a much larger scale and therefore at a much lower cost. The relatively high variable costs associated with RFIDsec may limit take-up of the technology.

Secondly, at the current time there is a very low willingness to pay for privacy and in fact RFIDsec does not consider privacy a marketing parameter.

Thirdly, a barrier to the use of RFID is that producers typically bear the full cost of installing the tags but do not receive the total gain from the tag. Instead benefits are split among producers, retailers and consumers although producers may only be able to pass on the cost to a limited extent.

Fourthly, most consumers and producers have never heard about RFIDsec (or RFID) and therefore do not know the potential benefits. Consequently, consumer groups may be suspicious of all types of RFID tags and the potential of the technology, even of RFIDsec tags, may not be fully exploited unless secure RFID tags are adopted as an industry standard.

### **Conclusion**

There appears to be great potential benefits to consumers and businesses from the RFID technology. However, although the technology and the potential have been known for many

---

<sup>138</sup> The basic RFID tag with no internal memory costs much less but since RFIDsec tags have an internal memory and therefore a wider applicability the price of the tag should be compared to non-secure RFID tags with internal memory.

years, it is generally acknowledged that the full potential of the technology so far has not been exploited. One of the reasons is that consumer groups have raised concerns about privacy issues. The European Commission has recently published recommendations on how to use of RFID technology without compromising privacy. Currently, the most common solution to privacy problems is to 'kill' the RFID tag at the point of sale. This removes the possibility of obtaining benefits from the RFID technology after the point of sale.

Danish RFIDsec provides an alternative solution. Their product ensures that the tag can be used after the point of sale without compromising privacy. The product has been implemented by a furniture producer hoping to battle counterfeit and in libraries hoping to achieve improvements in customer satisfaction and productivity. Nevertheless, the price of a RFIDsec tag is about double that of a comparable RFID tag. The price difference is partly due to the cost of the PETs included in the product and partly due to the lack of economies of scale in the current RFIDsec production. The price difference is likely to be a barrier to the spread of RFIDsec. Furthermore, there currently seems to be a quite low willingness to pay for privacy in the supply chain and among consumers while awareness of the product and the benefits is limited.

Authorities might be able to affect the take-up of RFIDsec tags and other secure RFID tags through recommendations as those put forward by the European Commission or through legislation, financial support or providing scale through purchases of secure RFIDs for the public sector.

## Germany

### DE01: TNS Infratest (DE)



#### Background

TNS Infratest is a German market research and polling company. It is part of the British WPP/Kantar Group. The company enjoys a high profile in the Germany market, thanks mainly to its political opinion polling, but it is active across the entire spectrum of market and social research and consulting.

Detailed information on individuals' circumstances, habits and outlook represents a very important asset for market research companies and TNS Infratest collects, stores and analyses a large amount of such information. As of 2009, TNS Infratest offered access panels comprising 90,000 German households.<sup>139</sup> Some of the datasets kept by TNS Infratest are extremely detailed. They contain individuals' full name and address, date of birth, education, marital status, household income, as well as information on dependents, housing situation, bank accounts, health insurance,

<sup>139</sup> See [http://www.tns-infratest.com/das\\_unternehmen/fakten\\_und\\_zahlen.asp](http://www.tns-infratest.com/das_unternehmen/fakten_und_zahlen.asp).

and even details on cars and other consumer items (mobile phones, computers, etc.) owned by the individual. A screenshot showing the range of personal information recorded on the TNS Infratest system is shown below (in German).

Figure 54: Screenshot personal information held by TNS Infratest

| Attributname                            | Wert des Attributs                               |                            |
|-----------------------------------------|--------------------------------------------------|----------------------------|
| Postleitzahl Wohnort                    | 806                                              | <a href="#">Bearbeiten</a> |
| Bundesland                              | Bayern                                           | <a href="#">Bearbeiten</a> |
| Staatsangehörigkeit                     | Deutsch                                          | <a href="#">Bearbeiten</a> |
| Anrede                                  | Frau                                             | <a href="#">Bearbeiten</a> |
| Geburtsjahr                             | 1967                                             | <a href="#">Bearbeiten</a> |
| Schulbildung                            | Abgeschlossenes Studium (Universität oder FH)    | <a href="#">Bearbeiten</a> |
| Sprachkenntnisse                        | Deutsch                                          | <a href="#">Bearbeiten</a> |
| Sprachkenntnisse                        | Englisch                                         |                            |
| Status Krankenversicherung              | Mitglied gesetzlicher Krankenkasse               | <a href="#">Bearbeiten</a> |
| Krankenkasse / Krankenversicherung      | BEK Barmer Ersatzkasse                           | <a href="#">Bearbeiten</a> |
| Pflicht- oder freiwillig versichert     | Freiwilliges Mitglied                            | <a href="#">Bearbeiten</a> |
| Mitversicherte Personen                 | Keine Person mitversichert                       | <a href="#">Bearbeiten</a> |
| Zusatzkrankenversicherung               | Leistungen im Krankenhaus                        | <a href="#">Bearbeiten</a> |
| Fahrzeuge im Haushalt                   | PKW                                              | <a href="#">Bearbeiten</a> |
| Autos                                   | 1                                                | <a href="#">Bearbeiten</a> |
| Marke des/der Autos im Haushalt         | BMW                                              |                            |
| Modell                                  | BMW Dreier- Reihe                                |                            |
| Baujahre des/der Autos im Haushalt      | 2004                                             |                            |
| KFZ Versicherungsverträge im Haushalt   | Weiß nicht, keine Antwort                        | <a href="#">Bearbeiten</a> |
| Art KFZ-Versicherungsschutz im Haushalt | Vollkasko                                        | <a href="#">Bearbeiten</a> |
| Kundenkarten                            | Lufthansa Miles & More (Blau)                    | <a href="#">Bearbeiten</a> |
| Kundenkarten                            | Payback                                          |                            |
| Kunde bei Geldinstitut                  | DAB Bank                                         | <a href="#">Bearbeiten</a> |
| Kunde bei Geldinstitut                  | ING-DiBa                                         |                            |
| Kunde bei Geldinstitut                  | Postbank                                         |                            |
| Versicherungen im Haushalt              | Hausratversicherung / Haushaltversicherung       | <a href="#">Bearbeiten</a> |
| Versicherungen im Haushalt              | private Haftpflichtversicherung                  |                            |
| Versicherungen im Haushalt              | Berufsunfähigkeitsversicherung                   |                            |
| Versicherungen im Haushalt              | Rechtsschutzversicherung                         |                            |
| Internetfähigkeit                       | Internetzugang vorhanden                         | <a href="#">Bearbeiten</a> |
| Online Provider im Haushalt             | T-Online                                         | <a href="#">Bearbeiten</a> |
| Geräte im Haushalt                      | Digital-Kamera für Einzelbilder                  | <a href="#">Bearbeiten</a> |
| Geräte im Haushalt                      | DVD Brenner                                      |                            |
| Geräte im Haushalt                      | DVD Laufwerk                                     |                            |
| Geräte im Haushalt                      | DVD-Player für den Fernseher                     |                            |
| Geräte im Haushalt                      | Flachbildschirm                                  |                            |
| Geräte im Haushalt                      | Kombigerät (Drucker mit Fax und/oder Scanner)    |                            |
| Geräte im Haushalt                      | MP3 Player (Portable)                            |                            |
| Geräte im Haushalt                      | Spielekonsole (PS 1 oder 2 / X-Box etc.)         |                            |
| Anzahl Handys im Haushalt               | 2                                                | <a href="#">Bearbeiten</a> |
| Mobilfunknetz                           | O2 (Genion / Citypartner) (früher Viag Interkom) |                            |
| Art Mobilfunk Handy 1                   | "Postpaid" / Mobilfunkvertrag abgeschlossen      |                            |
| Mobilfunknetz                           | O2 (Genion / Citypartner) (früher Viag Interkom) |                            |
| Art Mobilfunk Handy 1                   | "Postpaid" / Mobilfunkvertrag abgeschlossen      |                            |
| Status Erwerbstätigkeit                 | Vollzeit-erwerbstätig                            | <a href="#">Bearbeiten</a> |
| Beruf                                   | Sonstiger Angestellter                           | <a href="#">Bearbeiten</a> |
| Persönliches Nettoeinkommen             | Zwischen EURO 3.500 und EURO 4.000               | <a href="#">Bearbeiten</a> |
| Haushaltsnettoeinkommen                 | Zwischen EURO 3.500 und EURO 4.000               | <a href="#">Bearbeiten</a> |
| Art des Fernsehempfangs                 | Kabel                                            | <a href="#">Bearbeiten</a> |
| Wohnsituation                           | Miete                                            | <a href="#">Bearbeiten</a> |
| Wohnfläche                              | 50 - 79 qm                                       | <a href="#">Bearbeiten</a> |
| Anzahl Personen im Haushalt             | Eine                                             | <a href="#">Bearbeiten</a> |

Source: Datenschleuder #93 (2008), p. 61

### **Vulnerability**

In 2008, the German computer security magazine *Die Datenschleuder* revealed this database to be unsafe.<sup>140</sup> Following an anonymous tip-off that provided the researchers with the login details for an active account of a panel member that had registered his or her personal information with TNS Infratest, they were able to copy the personal information of 41,002 individuals.

While the database that secured the access to the database (an ID and a password were required for login) and the connection (it used the https protocol) was protected by PETs; once logged in, any user was able, with very little effort, to view and extract every profile in the database.<sup>141</sup>

### **Potential loss**

Such data is very valuable. It is clearly of value to the company who builds its business methods around the data, but also for third parties, including criminals, who may sell the data on or use them for fraud, theft or blackmail. The Symantec Global Internet Security Threat Report 2008<sup>142</sup> reports that full identities are worth up to \$60 apiece when offered for sale on underground economy servers, and up to \$1,000 if they contain bank account credentials, which was a distinct possibility in this case. Based on these figures, the potential loss due to the lack of security on the TNS Infratest server could be as high as \$41 million, or € 28 million.

### **Conclusion**

The case illustrates a fundamental truth about data protection: the system of protection is only ever as strong as its weakest part. In this case, it might have been virtually impossible for someone on the outside to get access to the personal information recorded by TNS Infratest, as access seems to have been protected low-level PETs. However, once logged into the system, the whole database could be copied easily, with no further protection afforded to individual datasets. The example also illustrates the particular dangers faced by businesses that use personal data as a resource in a way that makes it central to their business model. Very strong PETs are not an option in this case, as data minimisation and anonymity is not achievable without loss of functionality. Stronger data security, for the moment, appears to be the only solution in such cases (although it is conceivable that less privacy-invasive market research methods can be devised).

---

<sup>140</sup> 'Im Unfragetief', *Die Datenschleuder*, 93, 2008, pp.60-61, available at <http://ds.ccc.de/pdfs/ds093.pdf>.

<sup>141</sup> Individual profiles could be accessed via unique urls, which were numbered consecutively. The researchs determined the valid addresses by trial-and-error and then used a simple Python script to bulk-download the entire dataset.

<sup>142</sup> Symantec Global Internet Security Threat Report - Trends for 2008, Volume XIV, available at: [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_Internet\\_security\\_threat\\_report\\_xiv\\_04-2009.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_Internet_security_threat_report_xiv_04-2009.en-us.pdf).



## Estonia

### EE01: Genome Project

#### *Introduction and background*

The Estonian Genome Project (EGP) is a research venture of the University of Tartu founded by the Government of Estonia in 2001. The EGP started collecting tissue samples from gene donors in October 2002. In October 2009 the gene bank contained data contributed by 37,536 gene donors. The number of donors is small relative to the population (1.304 million); however, the number is growing rapidly and people are becoming more aware of the importance of genome research. The aim of the EGP is to create a database of health, genealogical and genome data representing 10% of Estonia's population.



The database will make it possible for researchers both in Estonia and outside to look for links between genes, environmental factors and common diseases (cancer, diabetes, depression, cardio-vascular diseases, etc). The results of this research are likely to lead to new discoveries in genomics and epidemiology, and will be instrumental in increasing the efficiency of health care.

Outcomes of the research are in areas as follows:

- health data
- lifestyle data
- demographic data
- genetic data
- biological material: DNA, plasma, white blood cells

#### *PETs and security*

There are three types of information, which genome bank holds:

- personal data
- “phenotypes”
- DNA sample (genotype)

Phenotype and DNA are anonymised that means that the identifying data is removed to protect people's security. The links between the data are held in a secure coding centre and other data is held separately. To ensure confidentiality of a gene donor, the personal data of the donor is separated from genetic data and each blood sample and each set of health data is given a unique 16-digit code. It is prohibited to connect the database of the Gene Bank to the Internet.

The most important PETs used to secure the personal data are anonymising and encrypting tools. Encryption is indispensable for transferring the data securely between different applications.

The privacy enhancing technologies are being bought and developed in coordination with the Public Procurement Act and there are approximately 5 companies who are able to produce such technologies.

The gene donating process:

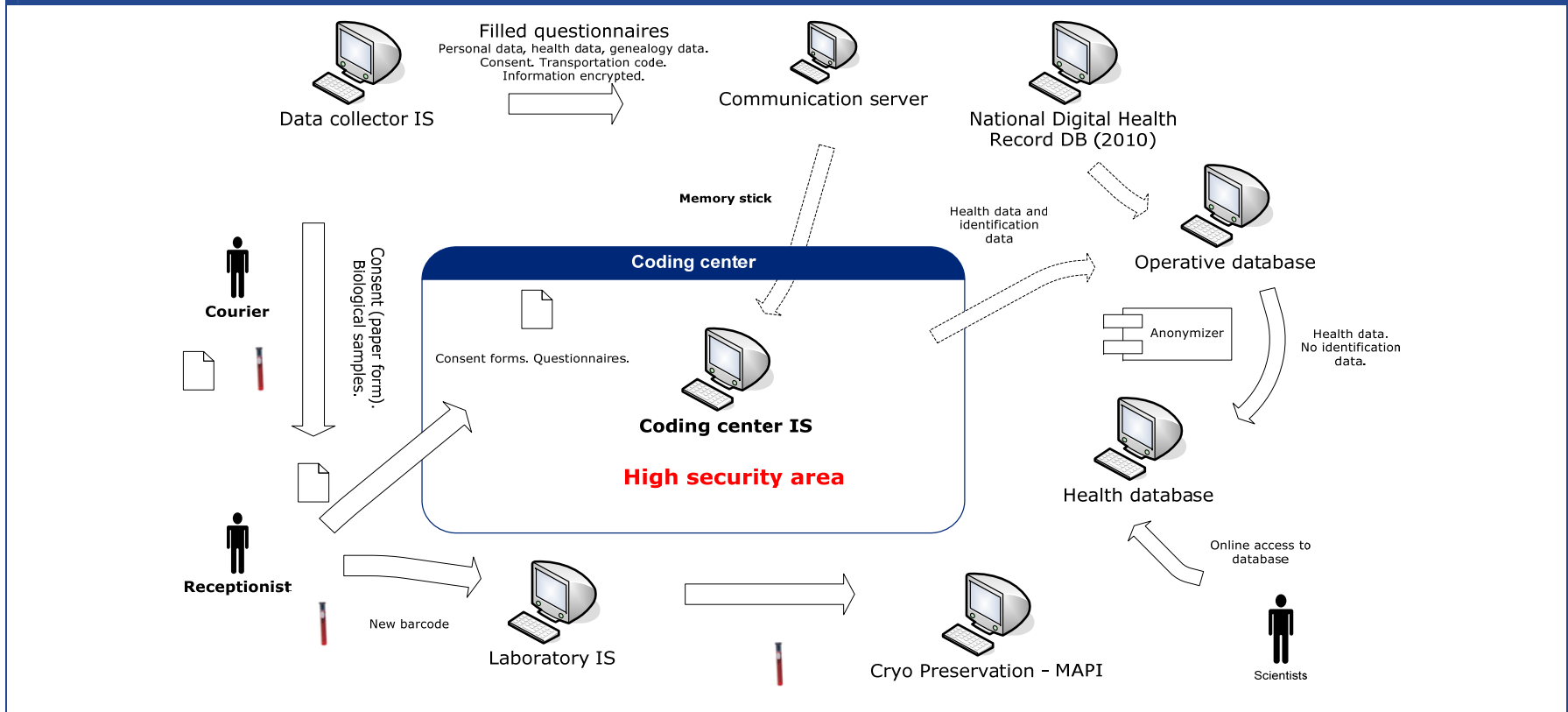
- After donating gene samples for the research, blood samples and donors signed consent form are delivered to the Gene Bank by special courier.
- Completed questionnaires are sent to the Gene Bank electronically, in encrypted form.
- In the coding centre of the Gene Bank, information in the personal data section of the questionnaire is extracted and replaced by a 16-digit code.
- Health data is separated from donor's personal data and stored in the Gene Bank's database.

The procedures:

- DNA, the carrier of the genetic information, is extracted from the blood sample in the laboratory of the Gene Bank.
- Separated DNA is placed in the storage facility of the Gene Bank. On the basis of the DNA preserved in the storage facility, it is possible to create a personal LD map of each gene donor.
- The data gathered from DNA is stored anonymously in the database and is not linked with persons ID.

NB: Data gathered from DNA will not be reachable for any counterparts e.g. judiciary, police, insurance companies, banks or employers.

Figure 55: Architecture of genome projects database system



Source: eSchool

### **Legal issues**

The legal framework for the Estonian Genome Project is laid down by the Constitution of Estonia in the following Acts:

- Human Genes Research Act;
- Personal Data Protection Act;
- Public Information Act; and
- Council of Europe Convention on Human Rights and Biomedicine.

The Human Genes Research Act regulates the establishment and maintenance of the Gene Bank and collection, processing and issuance of data.

Main provisions of the Act:

- The Gene Bank may be used only for scientific research, research into and treatment of illnesses of gene donors, public health research and statistical purposes.
- Only a gene donor and a doctor treating the gene donor shall have the right to receive personalised information.
- Blood samples and health and genetic data are the property of the Gene Bank. A gene donor shall not receive any remuneration for their processing.
- People shall be given an opportunity to participate in the Genome Project, but no one shall be obliged to participate. In order to make a person's self-realisation really free, he or she should be aware of his or her rights and obligations as a gene donor. Therefore, the law stipulates the circumstances of which a gene donor should be notified before his or her blood sample is taken (e.g. how a blood sample is taken, what is done with it, what data can be received from a blood sample, etc.). Only after that, a person can give a valid consent to becoming a gene donor.

### **Economic benefits**

The genome project is a significant research project aimed to strengthen the well being and general health of Estonian citizens on a long term basis. The database will make it possible for researchers both in Estonia and outside to look for links between genes, environmental factors and common diseases (cancer, diabetes, depression, cardio-vascular diseases, etc).

The Genome banks yearly budget for 2009 is approximately 15.5 million kroons (€ 1 million) and the budget for their IT infrastructure (development and maintenance) is approximately 1 million kroons (€ 64,000) a year. The exact cost of ensuring the security of the system is difficult to illustrate, since the safety is integrated intensely into the everyday work procedures of the Genome bank and is not recorded separately.

Longer term success of the genome project will lead to improved healthcare (better know-how and facilities) and science (advanced knowledge and research results) resulting improved better health outcomes, life expectancy, and also the economic outcomes achieved by the population. It

is difficult in this context to adequately or robustly assess the economic benefits associated with the programme.

## **EE02: eSchool**

### ***Introduction and background***

eSchool is a role based web application, allowing the distribution of learning information to authorised users. By default, eSchool provides six different roles (teacher, head-master, form-master, administrator, parent, student) and schools can modify or define sub-roles with different permissions. The application can be used in any modern Internet browser and computer operating system without further purchase or installation.

Users of the system:

- Teachers can plan their lessons, enter information about the lesson into the system, and communicate with parents.
- Students can keep an eye on their marks; set up reminders for their homework and maintain access to their record of performance.
- Parents can communicate with teachers and keep track on their children's performance, attendance and homework assignments.

### ***PETs and security***

The technology used for user authentication is the Estonian ID Card system in conjunction with an individual password and an access card. In addition, the eSchool system encrypts all data using a secure SSL protocol.

The system has two parts, a public and a private one. On the public section of the website, eSchool is gathering statistic information on users using Google Analytics. eSchool also gathers some contact information from people who get in touch with them (via e-mail, personal webpage, telephone etc).

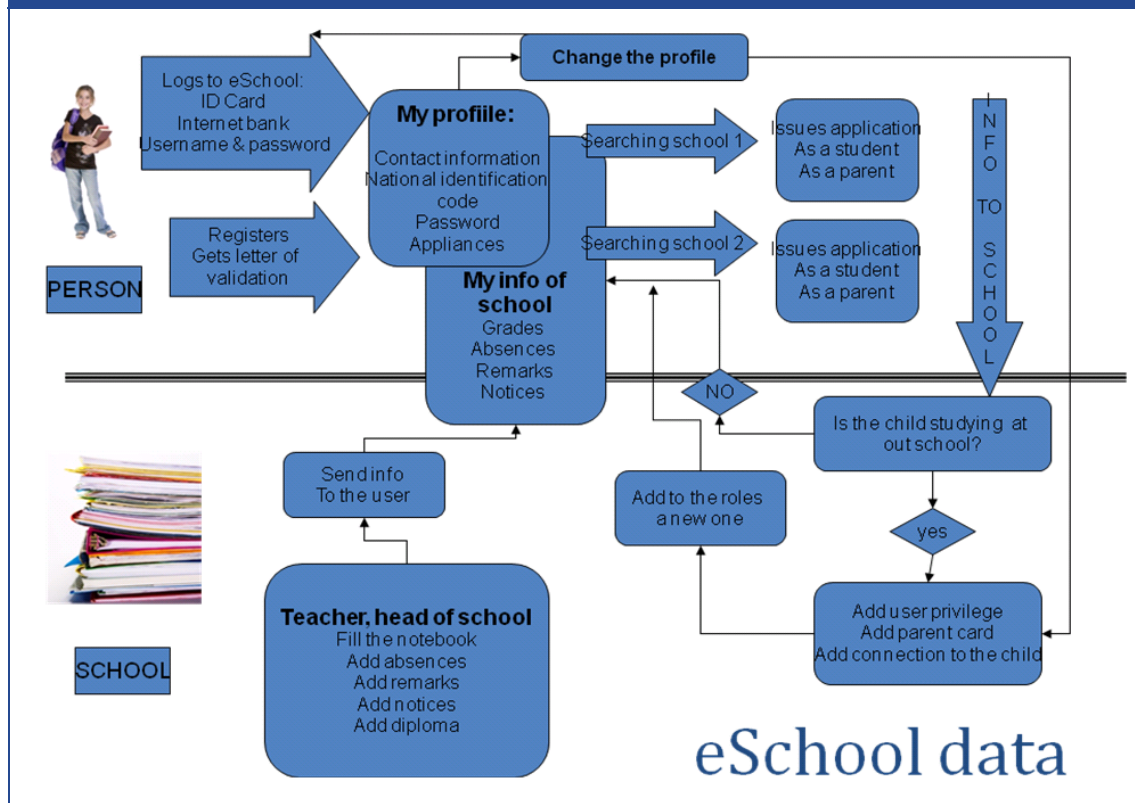
Access to the restricted section of the eSchool website is for credentialed users only and is password-protected. User authentication is handled via a dedicated service provided by a third party. After log-on, the website collects information on users' IP addresses and their activities on the site. This information is analysed and used to optimise the site's functionality. The data collected in this way is in not in any way linked to any personal data held on the system as part of the user account. Anonymised statistical information can be forwarded to third parties, e.g. the education ministry.

Personal information can only be disclosed in very restricted circumstances, e.g. for criminal investigations, or to enable the education authorities to ensure that all children attend school. Disclosure in these cases is regulated by the Data Protection Act.

Most of the personal information held on the system is collected und used by the participating schools. For this purpose, eSchool provides schools with standardised software for data entry and processing, whose proper usage is the responsibility of the schools. Schools can share information

held on the system with other parties, but this requires specific authorisation by the school's authorities.

**Figure 56: The technological architecture of e-school system**



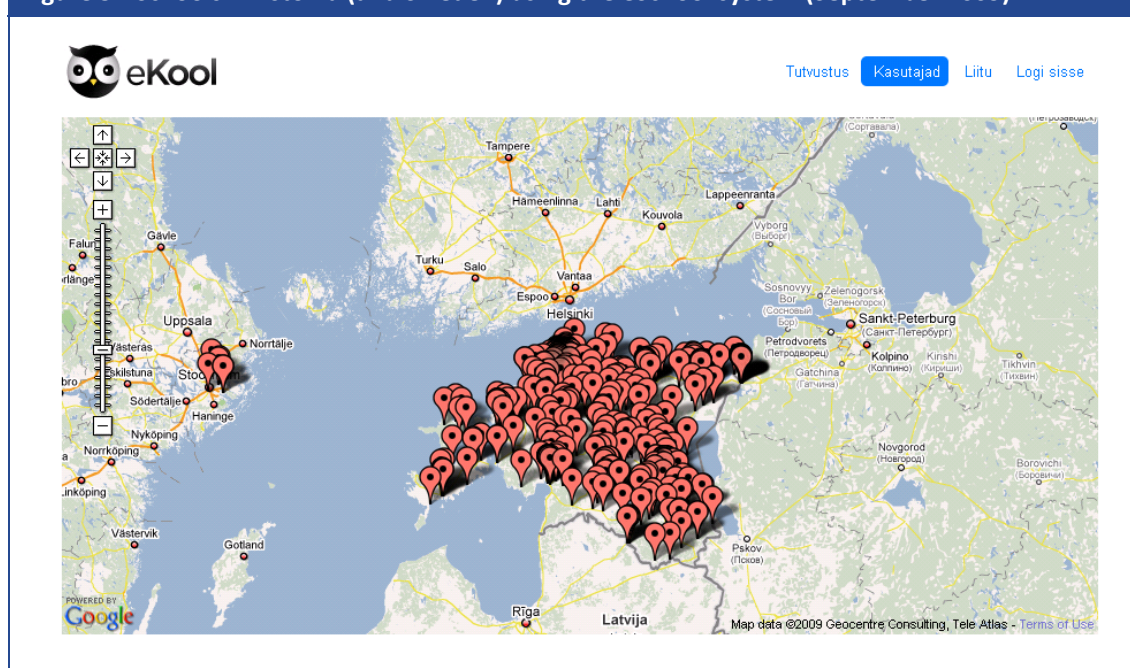
Source: eSchool

eSchool will safeguard all the contact information of the users as well as the password-protected pages of eSchool system with a SSL encryption to ensure security of data held on eSchool server.

### Propagation

The eSchool system was launched in 2002 and initially used by around twenty schools; it has grown rapidly since then, to 420 participating schools today (September 2009), which represent 70% of elementary and high schools in Estonia. The system is today also in use in Latvia and Sweden and is being tested in Argentina, Columbia and Uruguay.

Figure 57: Schools in Estonia (and Sweden) using the eSchool system (September 2009)



Source: eSchool

### Economic benefits

Costs of the system include the initial training of administrators, software rental and development, data backup and customer support. Payments are due after a 90-day free test period. There are four cost bands depending on the number of pupils attending the school. These are shown in the table below. The cost of the system is considered low by international standards.

Table 29: Please use sentence case

|                  | Option A | Option B | Option C | Option D |
|------------------|----------|----------|----------|----------|
| Price per month: | € 23     | € 48     | € 87     | € 112    |
| Price per month: | ≤ € 250  | ≤ € 500  | ≤ € 750  | € 750+   |

Source: eSchool

The benefits of the system to schools are not monitored, but they include greater efficiency in administrative processes that accrue to teachers, school administrators, pupils and parents. The education authorities derive added benefits from the statistical data the system provides. On a wider level, users of the system report educational benefits, including a reduction in truancy and better monitoring of pupils' progress and achievements. Finally, by assembling over time a rigorous picture of individual students' skills and educational achievements, it might smooth transition to the job market and raise the overall efficiency of the education system.

## Spain

### ES01: Alcobendas data protection

#### **Background**

Alcobendas is a city located in the Community of Madrid, roughly 13 km north of Madrid. The local government of the city committed to adapt their provision of services to current privacy and data protection acts.

With this aim, the Mayor of the city launched in May 2008 a new project for the protection of personal data of its citizens: “Alcobend@s protege tus datos”. The project was also aimed at informing citizens about the usage and destination of the data submitted to the government; securing such data; ensuring citizens’ rights in relation to the data provided to the government through its web site or other channels; and providing assurance that only necessary data were being requested to citizens. The project started with the ambition of becoming a reference in data protection for other organisations, including those outside the region.

The Mayor of the city received on 28 September 2009 the European Prize for best practices in Data Protection that recognises the quality in the procedures used for managing citizen’s personal information (recorded in the *Memoria del IV Premio a las Mejores Prácticas Europeas en materia de Protección de Datos*, Comunidad de Madrid , 2009).

#### **The project**

The main objective of the project was to adapt the services provided by the government to privacy and data protection regulations. It followed a strategy based on three stages.

Firstly, the project team studied extensively the current legislation on data protection. This included the national legislation but also the specific regulations of the Community of Madrid (Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid)<sup>143</sup>. This included an extensive assessment on the ways the government should guarantee the protection of data so that the fundamental right of citizen’s privacy is granted. The government official interviewed believed this was a very extensive exercise given the number of processes needed to be evaluated within local government, and the level of detail the legislation requires.

Secondly, there was an assessment of the processes for data collection and usage so that they would comply with current regulation. This involved intensive training for about 200 government officials and standardisation of the forms for collection of information on paper and its conversion to electronic formats. The rights and obligations of employees were also standardised. This included the use of secure confidentiality protocols, and guidelines on the type of software to be used for data collection (for example, avoiding the use of office software tools that do not have encrypted protection). An external audit was also conducted to assess the technological hazards of

---

<sup>143</sup> There is additional Autonomous legislation in the regions of the Basque Country, Catalonia, Galicia and Madrid.



the IT systems being used. As a result, recommendations of the audit were implemented by using state-of-the-art protection systems and firewalls.

The third strategy involved a campaign directed to citizens to inform them about their rights, the value of their personal data, and the dangers of providing information to unknown or unsecured providers (such as providing personal details for a lottery organised by a large shop).

### ***The costs and benefits***

The direct costs of the project are perceived as not very high (for example a new software application required was of the order of € 10,000). However, there are very significant indirect costs as these included the configuration of systems, reorganisation of practices, implementing secure protocols and training of staff.

Although unquantified, the benefits are perceived to be significant for the citizens because it informs and protects of a fundamental constitutional right; fulfils one of the commitments of the government with its citizens; and shows the willingness and leadership of the city in the provision of quality and innovation in the services it provides to the citizens, as well as reinforcing the trust of citizens in the local government.

### ***Conclusion***

The Alcobendas project is an example of implementation of data protection at a high scale. The project is viewed as successful because it informs and protects citizens of their fundamental constitutional right of privacy and protection of personal information. An important feature of this project is that it not only involved the deployment of secure IT systems, but it also required a whole reconfiguration of the network and a reorganisation of the internal administrative processes and working protocols. This included training of staff.

## **Malta**

### **MT01: The Employment and Training Corporation**

#### ***Background***

The Employment and Training Corporation (ETC) was set up by the Malta Government in 1990 with the objectives of:

- providing and maintaining an employment service to the Maltese labour market; and
- providing a training service to individuals seeking new jobs and to individuals already on-the-job but wanting to improve their knowledge and skills

Additional to these two primary functions, the ETC also maintains a database of all persons in employment in Malta and it is also responsible for the processing of work permits issued to foreign workers.

The ETC operates from a Head Office located in the south of Malta and it also has five regional job centres located in key areas of Malta and its sister island, Gozo. The ETC's website can be viewed at [www.etc.gov.mt](http://www.etc.gov.mt).

### ***The ETC's Operations***

To fulfil its function of providing and maintaining an employment service to the Maltese labour market, the ETC maintains a computerised register of individuals seeking employment which includes details of their qualifications, work experience and the type of job they are seeking. The ETC also captures job vacancies from employers with details on the requirements for their job vacancies and it tries to match the two. The job vacancies notified to the ETC are also displayed on its website and at its job centres which helps job seekers to apply for vacancies. Furthermore, employers may view the CVs of applicants for jobs (under certain access restrictions) which further facilitates the process of matching employers' requirements with employees' skills.

The ETC also provides career and vocational guidance and counselling services to job seekers whereby the latter are advised about their occupational preferences and suitability for roles they would like to apply for. Finally, the ETC is also responsible for maintaining the Malta-related part of the EURES database which provides details of job opportunities in the EU.

Apart from providing these employment services, the ETC maintains a computerised database of all persons in employment in Malta. Employers are obliged to provide the ETC with details of each individual they employ or whose employment is terminated, including the type of work they carry out and whether they are in full-time or part-time employment. Self-employed persons must also register with the ETC. This information provides the basis for national labour market statistics to the National Statistics Office for publication.

With respect to training services, the ETC maintains a computerised register of requests by individuals seeking training in particular areas, as well as a register of training service providers, and the Corporation attempts to match the two. The ETC is also responsible for the running of state-financed apprenticeship schemes.

The ETC operates its own internal ICT system located at its Head Office which is connected to each ETC job centre through ADSL links and comprises around 250 PC's and 6 servers. The ETC's ICT system is also connected to the Malta Government Network (known as MAGNET) which is administered by MITA (the Malta Information Technology Agency). MAGNET then connects the ETC's internal ICT system to external ICT systems such as the internet.

### ***PETs***

The ETC holds large amount of sensitive personal data, which makes data protection a critical concern. Data protection in Malta is regulated by the Data Protection Act of 2001 and fines may be levied for any violations of the provisions of the Act. The Act makes wide-ranging provisions with respect to the processing of personal data, amongst which Article 24 states inter alia with respect to security measures that:

*The (data) controller shall implement appropriate technical and organisational measures to protect the personal data that is processed against accidental destruction or loss or unlawful forms of*

*processing thereby providing an adequate level of security.*

Government parastatal organisations such as the ETC also fall within the ambit of the Data Protection Act which places responsibility on the ETC to ensure that the personal information held on its ICT infrastructure is used appropriately and only where needed to assist in its business processes. In view of its responsibilities under the Act, the ETC has introduced a number of Privacy Enhancing Technologies (PETs) to ensure that it meets these responsibilities. The PETs are of both an administrative and technical nature and include:

- The separation of modules within the ETC's database - there are different modules relating to the job seekers / job vacancies data, the employer / employees data and the training seekers / training providers data. Within each module, different sub-modules hold different parts of each data set e.g. individuals names are separated from their qualifications.
- User names / passwords providing access to the database which are also linked to individuals' rights to access particular sub-modules. The access rights define the action that particular users may take with respect to the data in each module, i.e. if they may input, amend, delete or only view data. ETC employees' access rights are deleted from the system should they not remain employed by the ETC.
- A number of audit trails which, amongst other matters, identify the PC and the user name used to log into the system, the database or module accessed and the data viewed, input, amended or deleted.
- A network intrusion prevention and detection system, antivirus technology and a security information and event management system are also used to monitor and protect incoming and outgoing data transmitted through MAGNET to and from the ETC's internal ICT system. These PETs are the responsibility of MITA and they are not handled by ETC. The corporation does not utilise these PETs on its own internal network since this is a self-contained intranet which does not require such a high degree of protection.

### ***Benefits of PETs***

The PETs described above play an important role in the operation of the ETC ICT infrastructure insofar as they allow the corporation's database to be operated in conformity with Malta's data protection legislation whilst protecting the security, integrity and quality of the ETC's data.

ETC's operations bring several benefits to the Maltese labour market insofar as it provides a vehicle through which employers' requirements can be rapidly matched against those of the individuals seeking employment thus saving a substantial amount of searching time for both the employers and employees. Furthermore, productivity gains are made by the Maltese economy since individuals would generally spend shorter periods in unemployment or in changing jobs.

A further benefit of ETC's operations in the labour market is that through the data obtained from employers on the individuals employed by them, the ETC can rapidly monitor the position in the labour market with respect to trends in the number of people in employment, their age distribution, skills etc. The rapid collection of this data is also important for the timely production and analysis of national labour market statistics by the National Statistics Office.

Finally, the information on training requirements and service providers held on the ETC's database allow it to rapidly identify areas where training is required and to set up training courses to meet this requirement thus again saving searching time for the individuals concerned and also ensuring that the labour market is rapidly provided with the training programmes it requires.

The utilisation of PETs is also important with respect to the ETC's reputation in the labour market as a trusted and reliable employment agency. Any leakage of the employer or employee information the corporation holds on its data bases would seriously undermine these individuals' confidence in the services provided by the corporation and reduce their utilisation of ETC's services. This would have serious negative repercussions both for the labour market and for the Maltese economy.

### **Costs of PETs**

The cost of the design and implementation of the PETs features contained in the ETC's internal ICT system amounted to around 5% of the costs of developing the system; the ongoing administrative costs of maintaining the PETs amounts to around € 1,000 annually.

Apart from this, there also are costs related to the PETs used on MAGNET but these costs are absorbed by the central government administration and are not charged to the ETC.

### **Conclusions**

Through its various activities, the ETC is successfully carrying out the role assigned to it by the Malta Government and this has resulted in:

- a substantial reduction in the time and effort required by individuals to find jobs and for employers to fill vacancies;
- data on the number of individuals in employment and the type of employment they are in being rapidly available; and
- an improvement in the relevance and timing of the training courses available to the Maltese workforce.

PETs have played an important part in the success achieved by the ETC since they have allowed its ICT systems to be developed in conformity with Malta's data protection legislation whilst protecting the security, integrity and the quality of the data on the systems. The benefits derived from using the PETs can therefore be considered to far outweigh the costs of designing and implementing them. Further development of the facilities offered by the ICT systems is envisaged, particularly with respect to features which will allow greater interaction with the system's external users such as employers and job seekers. This will require the utilisation of more PETs, and particularly encryption techniques, since more extensive facilities will be provided to external users.

## MT02: Dhalia Real Estate Services

### **Background**

Dhalia Real Estate Services (Dhalia) operates as an estate agency in Malta. The company was founded in 1983 by Maltese entrepreneurs and primarily services the property sales and letting market in Malta. Dhalia operates from a Head Office in a central location in Malta and has 10 branches located in different parts of the island. The organisation is supported by a team of 70 property consultants. The company's website may be viewed at [www.dhalia.com](http://www.dhalia.com).

Dhalia's operations focus upon acting as an estate agent in the property market in Malta. The company's ICT infrastructural resources are located at its Head Office and its databases hold details of more than 10,000 clients who are currently seeking to purchase, sell or let a property. The data base also holds details of clients who purchased, sold or let a property in the past.

The client details held on the database consist of their names, addresses, phone numbers and e-mail addresses, as well as the type of property they are seeking to purchase, sell or let and the property's location. Similar information is held about the properties which were purchased, sold or let in the past.

### **PETs**

Dhalia utilises a number of Privacy Enhancing Technologies (PETs) in order to carry out the activities outlined above. It is necessary for Dhalia to protect the client data described above both due to the data protection legislation in Malta and also to protect its own business activities and competitive position.

Data protection in Malta is regulated by the Data Protection Act of 2001 and fines may be levied for any violations of the provisions of the Act. The Act makes wide-ranging provisions with respect to the processing of personal data, amongst which Article 24 states inter alia with respect to security measures that:

*"The (data) controller shall implement appropriate technical and organisational measures to protect the personal data that is processed against accidental destruction or loss or unlawful forms of processing thereby providing an adequate level of security."*

The PETS utilised by Dhalia include filters and blockers, firewalls, encryption and biometric techniques, as well as administrative tools such as passwords and audit trails. By using these PETs, Dhalia can safeguard the consistency and integrity of the client data held on its databases. Thus, for example, the PETs are a safeguard against unauthorised access to the data, against data being extracted or changed by unauthorised persons and against data being deleted without proper authorisation.

### **Benefits of PETs**

The main benefit obtained by Dhalia in using PETs is that the PETs enable the company to carry out its main business activities, namely that of acting as an intermediary between individuals seeking

to buy, sell or rent properties. For this, the company uses personal data that represent a threat to privacy.

- Dhalia is dependant upon the information contained in its databases on the properties which are currently for sale or let whereby it can match sellers' and buyers' requirements in order to facilitate successful transactions between them. The loss of this information through inadequate protection of the databases would seriously disrupt the company's operations.
- Furthermore, the information Dhalia holds on its past transactions allow it to identify trends in the property market and thereby be in a better position to develop a competitive market strategy. The information on clients' past requirements also allow Dhalia to re-contact clients who may have effected transactions in the past but who may still be interested in viewing new properties which have become available.
- Apart from the above considerations, the use of PETs by Dhalia allows the company to make substantial improvements in the productivity of its staff insofar as the property negotiators and administrative staff in Dhalia's 10 branches have access through the IT system at Head Office to the properties of interest to them and can thereby more rapidly and easily match the interests of property buyers and sellers thereby saving a considerable amount of time and effort for themselves and for their clients.

Dhalia intends to further improve the service it gives to its clients by providing its property consultants with additional ICT tools such that they will be able to communicate with the Head Office IT system whilst being outside their branch office. This will further facilitate the ease with which the property consultants can match the requirements of property buyers and sellers and thus further enhance the level of service provided to clients. The deployment of these tools is however dependant upon the tools employing suitable PETs, and particularly encryption technologies, to protect the data being transmitted by the property consultants to and from the Head Office IT system.

The utilisation of PETs is also important with respect to Dhalia's reputation as a reliable and trusted estate agency. Any leakage of the customer information the company holds on its data bases would seriously damage its good reputation in the property market which is an important factor in its attracting clients and developing its client base.

### **Costs of PETs**

The costs of the PETs used by Dhalia amount to € 28,000 per year which represents the cost of the annual licence fee together with an element of cost to maintain the PETs.

The above costs are apart from the costs in terms of the potential loss of revenue and the increased operating costs which would arise if the PETs were not utilised.

### **Conclusions**

Dhalia considers that the benefits it derives from using PETs are much greater than the costs involved. This is because the company's business operations would be seriously endangered without PETs since the company is dependant upon its databases to act as an intermediary in

property transactions. Furthermore, Dhalia is in a position to obtain substantial staff productivity improvements, as well as increased customer satisfaction, through the use of the PETs. Dhalia's good reputation in the market place would also be put at risk without the use of PETs

Dhalia is thus fully committed to using PETs and the company is looking into introducing more sophisticated PETs such as intelligent auditing tools. It considers that costs, rather than technical considerations are the main limitation to the wider use of PETs. However, PETs in this example are used only to mitigate the risks. They do not eliminate them altogether, which amounts to a relatively ineffective use of PETs.

### **MT03: Computime Limited**

#### ***Background***

Computime Limited (Computime) is a supplier of Information and Communications Technology (ICT) systems and solutions in Malta. The company was founded by Maltese entrepreneurs and has been operating for over two decades. Computime primarily services the ICT market in Malta though in recent years it has also serviced clients overseas, primarily in the U.K. and in North Africa. The company has around 80 employees, most of whom are individuals skilled in providing ICT systems and solutions. Computime also possesses substantial ICT infrastructural resources located at its Head Office in a central location in Malta, namely 10 servers and the related ICT equipment and applications. The company's website may be viewed at [www.computime.com](http://www.computime.com).

In the early stages of its development, Computime focussed on installing and maintaining ICT systems and solutions provided by overseas suppliers such as SunSystems and Cisco Systems but in later years the company also expanded its business into itself designing ICT systems and solutions for its clients and into hosting data for its clients on its own ICT systems. These activities today constitute a major part of Computime's business operations.

When Computime designs an ICT system for a client, the company initially agrees the scope and specifications of the system with the client and the company's staff then proceed to configure and test the prototype system on Computime's own in-house ICT infrastructure. At later stages, test data is obtained from the client and run on the prototype system. When the prototype system reaches a sufficient degree of maturity, the system is transferred to the client's own ICT infrastructure and thereafter operated by the client.

In some instances, Computime's clients request the company to permanently host their ICT system when it becomes operational, in which case the data relating to the clients' operations – which may consist of customer, supplier and other operational data – is transferred to Computime's servers with the input of new transactional data and the output of reports and other information being carried out by the client via secure links either over the internet or through dedicated network links.

#### ***PETs***

Computime utilises a number of Privacy Enhancing Technologies (PETs) in carrying out the activities outlined above. It is necessary for Computime to protect the client data described above

both due to the data protection legislation in Malta and also to ensure that the company protects its own competitive position as well as that of its clients.

Data protection in Malta is regulated by the Data Protection Act of 2001 and fines may be levied for any violations of the provisions of the Act. The Act makes wide-ranging provisions with respect to the processing of personal data, amongst which Article 24 states inter alia with respect to security measures that:

*“The (data) controller shall implement appropriate technical and organisational measures to protect the personal data that is processed against accidental destruction or loss or unlawful forms of processing thereby providing an adequate level of security.”*

In Computime’s case, not only is client information held on the company’s databases, but in some instances Computime’s databases also hold data pertaining to the client’s clients.

The PETS used by Computime include filters and blockers, encryption techniques, data segregation, automatic data deletion, passwords and audit trails. By using these PETs, Computime can safeguard the consistency and integrity of the client and supplier data held on its databases. Thus, for example, the PETs safeguard against unauthorised users accessing the data, against company employees making improper use of the data and against data being deleted unintentionally.

The PETs thus ensure, amongst other matters, that information relating to the ICT systems being developed for Computime’s clients, and the client data held on the company’s ICT systems, cannot in any way be accessed by or divulged to the clients’ competitors which could have serious implications for the clients’ business operations.

### **Benefits of PETs**

The main benefit obtained by Computime by using PETs is that, as a result of the role played by the PETs in safeguarding the consistency and integrity of the data held on the company’s databases, the PETs enable Computime to carry out two of its main business activities, namely that of hosting clients’ data (and data relating to the client’s clients), and that of developing new ICT systems for clients, on its own in-house ICT infrastructural resources.

This has several positive repercussions upon both Computime’s business operations and that of its clients which include:

- The fact that Computime earns a substantial part of its current and potential future revenue from the two activities mentioned above; and
- The fact that, by carrying out the development of clients’ ICT systems on its own ICT infrastructure and premises, Computime is in a position to achieve several operating efficiencies to both its own and its clients’ advantage. These operating efficiencies include the fact that, by developing and testing new ICT systems on its own ICT infrastructure, Computime can test a greater variety of possible system configurations than would usually be possible if it only used the clients’ ICT infrastructure since the latter’s infrastructure would usually be less extensive and sophisticated than Computime’s.



Apart from that, the utilisation of PETs is a crucial element in building and maintaining Computime's reputation as a reliable and trusted provider of ICT systems and solutions. The company's reputation would be seriously damaged if there were any leakage of the customer information it holds on its data bases. The company's good reputation with its customers and suppliers is a critical element in its expanding its client base, representing new suppliers and maintaining its competitive edge.

### **Costs of PETs**

The costs of the PETs used by Computime amount to a one-off cost of around € 6,000 to purchase the PETs and around € 5,000 per annum in terms of licence fees. Additionally, there is a cost of around € 6,000 per annum representing the costs of an IT specialist engaged to set up, develop and maintain the PETs. Finally, the PETs may result in an element of cost insofar as they constitute an additional layer of system controls which may to some extent slow down response times and operating efficiency.

The above costs are apart from the costs in terms of the potential loss of revenue, the increased operating costs and the reduced investment in ICT resources which would arise if the PETs were not utilised.

### **Conclusions**

Computime considers that the benefits of utilising PETs far outweigh their costs. This is because a substantial part of the company's business operations would be put at risk without the PETs which could lead to a substantial loss of revenue and business opportunities coupled with a substantial increase in operating costs. Furthermore, the utilisation of PETs is an important element in building and maintaining Computime's reputation as a reliable and trusted provider of ICT systems and solutions.

Computime is thus fully committed to utilising PETs and promoting their use. The company is considering introducing more sophisticated PETs such as Security Information and Event Management, a PET which would look out for any unusual occurrences in an ICT system. However, no stronger PETs providing anonymity are used. Since the company does not itself use most of the personal data it holds (rather, it just stores third-party data on behalf of clients) it appears that scope exists for using stronger PETs that provide complete anonymity (the extent of 'data separation' could not be ascertained). Computime considers that the main limitation to the wider use of more sophisticated PETs lies mainly in their cost rather than in any technical considerations.

## **MT04: The Malta Government Common Database**

### **Background**

The Malta Government departments and parastatal organisations engage in a large number of transactions with the Maltese public, a number of which are conducted through ICT systems operated by these entities. In many instances, the departments need to utilise data relating to individuals such as their date of birth and address which is common to all the organisations. Rather than each department creating its own database holding this information, it was felt to be more efficient for the Government to construct a database (the Common Database or CdB) of commonly

used public domain information that could be accessed and used by all the government departments and parastatal organisations on a need to know basis. A system such as entails the potential for privacy invasion on a massive scale.

The CdB project was thus launched by the Government in 1994 with the objective of creating such a database. The project was successfully implemented and today the number of users accessing the CdB is over 1400 spread in 138 government organisations.

The CdB is linked to its users through the Malta Government Network (known as MAGNET). The CdB server resides at MITA (the Malta Information Technology Agency) who also administer MAGNET.

The CdB contains information about individuals' names, date of birth, marriage or death, as well as information on individuals' parents and spouse. Details of individuals' addresses are also held on the data base. All the information is sourced from information which is in the public domain, including the Public Registry and the Electoral Office.

The information contained in the database is used by a number of government departments and parastatal organisations for different purposes. Thus, for example, it is no longer necessary for individuals to obtain birth, marriage and death certificates from the Public Registry to make applications for the benefits and services provided by the Government to the Maltese public. This is instead achieved through the use of the CdB by the government departments concerned.

This approach has been introduced in several government departments including the Public Lending Library, the Examinations Branch, the Passports Office, the Identity Cards Office and the Department for Social Security. Applications processed in these Departments no longer require the presentation of the Public Registry's civil status certificates, since the information is obtained on behalf of the clients from the CdB. Procedures have also been initiated so that other government departments will implement this approach to provide a better and more effective service to the public.

The CdB is also used by government departments and parastatal entities for several other purposes. Thus for example the Water Services Corporation utilises the CdB to calculate water and electricity bills based on the number of persons living in a household. The Health Authorities use the data base to create basic details of patients' records whilst the National Statistics Office uses it to carry out national surveys and research on matters such as the age profile and area density of the population.

### **PETs**

Data protection in Malta is regulated by the Data Protection Act of 2001 and fines may be levied for any violations of the provisions of the Act. The Act makes wide-ranging provisions with respect to the processing of personal data, amongst which Article 24 states inter alia with respect to security measures that:

*"The (data) controller shall implement appropriate technical and organisational measures to protect the personal data that is processed against accidental destruction or loss or unlawful forms*

*of processing thereby providing an adequate level of security.”*

Government Departments and parastatal organisations also fall within the ambit of the Data Protection Act which places responsibility on the Public Service to ensure that the CdB is used appropriately and only where needed to assist in the business processes of a department. In view of its responsibilities under the Act, the Public Service has introduced a number of Privacy Enhancing Technologies (PETs) to ensure that it meets these responsibilities. The PETs are of both an administrative and technical nature and include:

- validation of the data collected for entry into the CdB which is checked by both the source and user departments against pre-defined rules so as to ensure data integrity and quality. The data continues to be validated regularly even after its initial entry to ensure that its integrity and quality is maintained;
- a series of checks before government user departments are authorised to access the CdB. The Director of Civil Registration is the Controlling Authority for the CdB and is responsible to authorise all access requests. All requests received from user departments for access to the CdB are considered and the Director only grants permission under certain pre-determined conditions;
- when CdB access is granted to a government department, the Head of Department is held responsible for the way the CdB personal data is being used within his or her department. Procedures are adopted to enforce responsibility and accountability which include that no user accounts are opened without the specific approval of the respective Head of Department who is the data controller; and
- once user accounts are approved within departments, the approved users are provided with passwords which are non-transferable. Furthermore, the user’s account is closed should he or she be transferred to another department.

As the usage of the CdB developed and spread over a number of government departments, the need arose to develop a CdB printing module from which a Certificate can be printed by any department using the CdB. The Certificate is printed at the request of approved users and contains various items of individuals’ personal details. The production and use of the Certificate is protected by several PETs through which the user’s identity, printer, time of access and the data accessed can be traced. An example of the Certificate is attached in Appendix 1. The CdB Certificate plays a useful role insofar as it is in electronic format and replaces the birth, marriage and death certificates previously produced manually by the Public Registry. The CdB Certificate is also subject to much more rigorous data processing controls through the use of PETs than the manual certificates previously produced.

As noted above, the CdB server resides at MITA’s Operations Centre and it is linked to its users through MAGNET. Several PETs are in place to protect the data being transmitted by users on MAGNET including a network intrusion prevention and detection system to protect against threats of internal and external attacks, antivirus technology with advanced threat prevention to defend against malware, and a security information and event management system.

### **Benefits of PETs**

The PETs described above play an important role in the operation of the CdB insofar as they allow the database to be operated in conformity with Malta's data protection legislation whilst protecting the security, integrity and quality of the data on the CdB.

The operation of the CdB brings several benefits to both the Maltese Government and the public insofar as it provides a one-stop-shop for both the government departments and the public for personal data relating to individuals such that it is no longer necessary for the departments and individuals to obtain the data from different sources but this can be obtained in a fast and efficient manner from the CdB.

This has several implications for both the government departments and the Maltese public. Thus, for example, individuals do not now need to waste time going from one government department to another to obtain official documents relating to their date of birth, address etc. but this information is immediately available at each department through the CdB. Through this approach, waiting times and queues for individuals needing to present their personal information to government departments for various purposes have been drastically cut down. The contrast between the previous and the current situation in this respect is shown schematically in Appendix 2.

The productivity and efficiency of the government departments using the CdB has also been positively affected insofar as they have reliable and up-to-date information immediately at hand on the basis of which they can carry out several of their activities such as the issue of passports, driving licences and library lending cards. The CdB also helps departments to issue correct bills, to prepare social and economic studies and to investigate particular issues. The CdB has also assisted government departments to streamline their work practices and substantially reduce the duplication of effort by staff who were previously engaged in inputting and checking personal data in various departments. These staff could now be released to carry out more productive functions in other areas or departments.

A further important benefit arising from the use of PETs on the CdB Certificate is that this substantially reduces the risks of fraud arising, for example, from the presentation of forged personal identity documents to claim social security and other benefits.

### **Costs of PETs**

The approximate cost for the design and implementation of the PETs features contained in the CdB Certificate amount to € 48,000. Apart from this, there also are costs related to the PETs used on MAGNET which amount to approximately € 246,000 in terms of the initial purchase costs and around € 110,000 in terms of annual licence fees. However, these costs are spread over all the users using this network and the costs cannot be allocated to the CdB application in a meaningful manner.

### **Conclusions**

Before the introduction of the common data base by the Malta government, government departments and parastatal organisations collected, maintained and managed their own

commonly used personal data. This was an inefficient and expensive system which also led to inconsistencies between the information held by the departments, while also multiplying the threats to privacy. The CdB was therefore set up by Government and this has successfully:

- reduced the cost of data collection and maintenance for Government departments;
- improved the quality of Government information, since areas of information can be ascribed to individual 'Owners', responsible for assuring and maintaining its accuracy; and
- facilitated the one-stop-shop concept for personal data in Government Departments and the Maltese public.

PETs in the CdB are mostly standard security technologies, as well as administrative procedures. Privacy protection seems to depend substantially on human actors. PETs have allowed the database to be developed in a secure manner in conformity with Malta's data protection legislation whilst protecting the integrity and the quality of the data on the CdB. It is unclear to what extent the personal data collected in the CdB is strictly necessary and thus how much scope exists for using stronger PETs that would minimise the data requirements of the various government bodies and provide user anonymity. As it is, the benefits derived from using the PETs are considered to far outweigh the costs of designing and implementing them. Although further development of the CdB PETs is envisaged, this will depend on budgetary considerations rather than technical issues.

Figure 58: The CdB certificate

**CdB**  
COMMON DATABASE SYSTEM  
DEPARTMENT OF CIVIL REGISTRATION

PERSONAL DETAILS

Full Name and Surname of Person

Gender

Date of Birth

Place of Birth

Date of Death

Surname, Name and Place of Birth of Spouse

Date of Marriage

Place of Marriage

FATHER'S DETAILS

Surname, Name and Place of Birth

MOTHER'S DETAILS

Surname, Name, Maiden Surname and Place of Birth

ADDRESS DETAILS

Property number, Name and Subdivision

Street

Town and Country

FORM A - Personal/Address Details Extract printed by: MDX-AR001 on the: 03 July 2007 10:30

Signature of Issuing Officer

Security Ref No: 10001902  
Audit Id: 100706

For Internal Use only

User Details Audited

Security Ref. No.

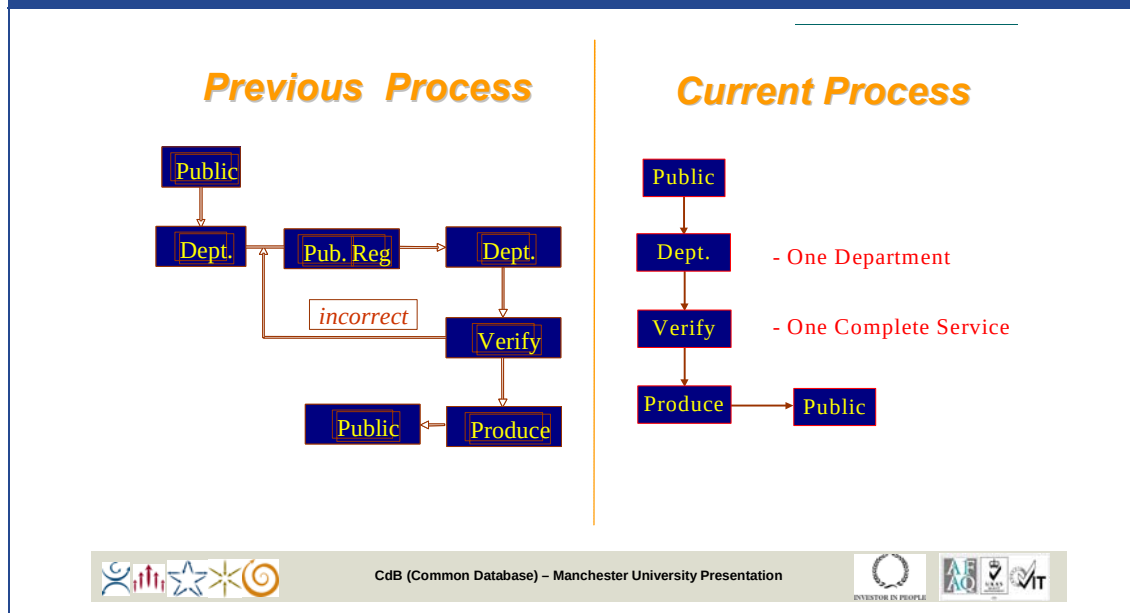
Audit Id.

Enables One-Stop Shop

Government of Malta  
INVENTOR IN PEOPLE  
MALTA  
IT

Source: Malta Information Technology Agency

Figure 59: The one-stop-shop concept



Source: Malta Information Technology Agency

## United Kingdom

### UK01: Voluntary disclosure of personal information in market research

Market research is one of the key activities that retail businesses undertake to attract consumers. Firms use insight elicited from individuals responding to surveys to inform every aspect of a product: from presentation, content, and pricing. On the one hand, consumers have an incentive to participate in these studies in order to help firms to bring out products that closely match their tastes. On the other hand, consumers may be wary of market research because it can teach firms how to exploit consumer preferences for increased profitability, e.g., through price discrimination or creative advertising. One study has found for example, that people take up loans that charge higher interest rates if direct mail solicitations are creatively designed (Bertrand et al., 2009). Clearly, the attractiveness of an advert for a loan in itself should be close to the bottom of considerations taken into account when deciding to take up a loan, however, market research using consumers can teach firms how to extract the largest profits from consumers by getting them to ignore unattractive prices. In this setting, it is important to understand why individuals relinquish their privacy to market research companies and whether this justifies the need for privacy enhancing technologies.

#### *The case of market research in the UK media sector*

This case study looks at a media consulting firm that worked with a major publications company that was looking to increase the readership of one of its newspapers. In order to gain insight from consumers on how to do this, the media consulting firm hired a data vendor that conducted a questionnaire among 1,500 members of the general public. People provided a vast array of

personal information, including: names, contact details, family details, psychological profiles and more.

In this case, the data vendor did not use any privacy enhancing technologies and was able to match personal information provided by respondents to their responses. In theory it can go on to sell this information to other firms for the purposes of direct marketing. In addition, this information is open to exploitation by employees working within the market research firm itself. Given this, the reasons that individuals still responded to questionnaires were stated as follows.

### ***Financial incentives***

Each respondent was provided with a small financial incentive of £ 2 to complete the questionnaire. This reward may be one reason why people are willing to give up personal information. However, response rates received closely match the demographic make-up of the UK. In particular, those on higher incomes and with less free time were just as likely to respond to the survey as those with more free time. This poses something of a puzzle – why would relatively well-off individuals be willing to give up their privacy at the same price as others? Three main reasons were put forward to explain this observation.

### ***Framing***

Firstly, the importance of the messages used in the questionnaire was highlighted. They emphasised how valued respondents were for taking the time to do the questionnaire, how important their insights were to the study and how beneficial any changes resulting from their contributions might be to the content of the newspaper. These messages may have suppressed any privacy issues respondents may have had in mind.

### ***Personal motivation***

Secondly, while monetary incentives are important it was claimed that most people responding to the questionnaire were genuinely interested in the topic matter – this motivated their participation. On other projects for example, people are offered the option to donate their monetary reward to charity, which most respondents do, suggesting that financial incentives may not be that important to giving up some privacy.

### ***Perceived levels of privacy***

Finally, it was noted that the use of the online medium is far more effective in eliciting responses about potentially sensitive topics – as respondents are physically removed from an interviewer, they are happy to openly answer questions on most topics as there is no-one “looking them in the eye” or talking to them over the phone in that moment, i.e., they may have a false sense of privacy.

### ***Summary***

In short, privacy considerations are not at the forefront of most respondents’ minds. For whatever reason this may be, it results in choices where privacy is traded-off for relatively small financial rewards, general interest in a topic and perhaps a false sense of privacy.

This may suggest that there is a role for privacy enhancing technologies. It appears that individuals do not take into account the significant costs sharing private information could have – small financial incentives for sharing personal information do not seem to be adequate compensation for potentially, hundreds or thousands of pounds lost through identity theft. This observation fits in with empirical evidence from behavioural and experimental economics that shows people are not able to make the best choices when faced with privacy considerations online.

## UK02: ATMs

PETs are used to protect automated teller machines (ATMs). These involve various “keys” that specify the encryption or decryption of personal information, specifically of customer PIN numbers. PIN key are used to create PIN numbers for credit and debit cards from account numbers. Terminal keys are used in ATMs to house PIN keys for the purpose of verifying customer transactions. If a bank joins a network, working keys and zone keys are used to permit customers of other banks to use its ATMs. In short, the preservation of customer privacy relies on keys, particularly on keeping PIN keys secret (while also being put to day-to-day use in verifying economic transactions).

From a simple encryption perspective, PIN keys are generally secure because of binding technological and temporal constraints placed on parties attempting to discover them. In other words, given hardware processing power, cryptanalysis generally takes too long to discover transmitted PIN information. In the mean time, this information is likely to have become useless, removing the incentive for thieves to attempt to elicit this information in the first instance. In this way, ATMs are meant to keep customer account information private.

However, there are a number of cases where fraudulent or “phantom” withdrawals have been made from UK bank accounts. These privacy violations take place despite the sophistication of banking systems because of the structure of economic incentives banks, customers and third-parties face.

Some studies (e.g. Bohm, Brown and Gladman, 2000) have posited that much of the problem lies in the legal system. In particular, UK banks are not liable for fraud cases – consumers are responsible for risks associated with PETs – which means that banks have little incentive to tighten information security systems. A spokesman for Barclays figured that 1 in 34,000 ATM transactions in the UK are phantom withdrawals.<sup>144</sup>

This contrasts with US regulations where banks shoulder the burden of information security breaches. As such, the number of ATM fraud cases is fewer in number, estimated to be worth a comparatively small sum of \$15,000 a year (Wright, 1991).

The fact that customers face legal liability over bank technologies in the UK leads to a number of other problems. Firstly, with information security risks dispersed across a large number of customers that individually only face a small probability of fraud and possess few resources to act against banks in a legal setting, little action will take place.

---

<sup>144</sup> <http://www.efc.ca/pages/media/times.07nov92.html>.



Secondly, moral hazard arises within retail banks because UK regulation is built on the premise that it is impossible for banks to be responsible for fraud (given the supposed sophistication of its PETs). Bank staff know that it is highly unlikely that they will be blamed for any information breach, therefore they are relatively free to commit fraud. Known cases include a bank clerk that issued an extra card on a customer's account to himself and proceeded to withdraw close to £ 10,000 from this account in East Sussex, UK. The clerk was only caught because he confessed.<sup>145</sup> Another case involved a maintenance engineer fitting an ATM with a computer that recorded customer account numbers and PINs in Scotland. The bank involved was heavily criticised in this case by senior members of the judiciary for failing to consider its customers' claims.<sup>146</sup>

Thirdly, with no apparent reason to systematically record instances of fraud, banks hold poor records on the problem. If they held better records they may find that fraud could occur due to the types of organisational failure outlined above. For instance, banks might find that instances of fraud are more concentrated in certain regions of the country and within certain bank, which could reflect theft by staff, as fraud cases might otherwise show no distinct pattern across the country.

---

<sup>145</sup> See R v Moon, Hastings Crown Court, Feb 92 for details.

<sup>146</sup> See A. Collins (1992), "The Machines That Never Go Wrong", Computer Weekly, 24-5.

# Business survey

## Questionnaire

### QUESTIONNAIRE

#### (I) Your business

1. Main activity: information and communication
2. Number of employees: ☐ 0-9 ☐ 10-49 ☐ 50-249 ☐ 250 and over

#### (II) Use of personal information

By 'personal information' we mean any information that can be linked to a specific individual with reasonable accuracy, that is, any data that is referenced with an individual's name, address, telephone number, email etc.

- |                                                                                                                         |                                                        |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| 3. Please specify which personal information (e.g. contact details, salaries, past purchases, etc.) your company keeps: | 4. How many records are kept?                          |
| Customers <input type="button" value="click to select"/>                                                                | <input type="button" value="click to select"/> records |
| Staff <input type="button" value="click to select"/>                                                                    | <input type="button" value="click to select"/> records |
| Suppliers <input type="button" value="click to select"/>                                                                | <input type="button" value="click to select"/> records |
| Third-parties (e.g. commercial marketing databases) <input type="button" value="click to select"/>                      | <input type="button" value="click to select"/> records |

#### (III) Costs and benefits associated with holding personal information

5. Do you currently derive economic benefits from holding personal information? (e.g. increased sales through more targeted marketing, better management of supplier relationships, etc.).  
Please rank the benefits on a scale from 1-5  

|                                                     |                                                                                                                                                                            |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Personal information on                             | 1 (No benefits) <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> (very large benefits) |
| Customers                                           | 1 (No benefits) <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> (very large benefits) |
| Staff                                               | 1 (No benefits) <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> (very large benefits) |
| Suppliers                                           | 1 (No benefits) <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> (very large benefits) |
| Third-parties (e.g. commercial marketing databases) | 1 (No benefits) <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> (very large benefits) |
6. What are the benefits you get from personal information?
7. The misuse of personal information, or concerns about the potential misuse, could harm your business (e.g. legal claims, official fines or other sanctions, loss in trust of customers). How do you judge the risk for your business?  
1 (No risk) ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ (great risk)
8. Please specify factors that limit the risk to your business (e.g. firm size, type of business, type of information held, customers are not concerned, potential loss is negligible)
9. Please specify factors that increase the risk to your business (e.g. firm size, type of business, high costs of protecting personal information, lack of awareness about means of protection of personal information, lack of technical know-how prevents better protection, lack of awareness of legal obligations in the area of data protection)
10. Have concerns (your own or your customers') about the security of personal information prevented you from developing new business activities (e.g. selling over the Internet) or processes (e.g. electronic billing)? Yes ☐ No ☐
11. If your answer to the previous question is 'yes', can you give example of an activity that you would like to undertake, but feel unable to do so because of concerns about the security of personal information?

## (IV) The role of technical means to protect personal information

Examples of technical means to protect personal information include automatic anonymisation of data after a certain period of time, encryption software or software that prevents businesses from using personal data without explicit consent, etc.

12. People might give better/more reliable information if they think it is safe to do so; on the other hand, using technologies that protect personal information could limit your ability to use the data, including in ways you have not yet thought of.

How can enhanced privacy protection through technical means affect the benefits you derive from holding personal information?

- 1 ☐ (costs significantly greater than benefits)  
 2 ☐ (costs slightly greater than benefits)  
 3 ☐ (costs and benefits cancel out)  
 4 ☐ (benefits slightly greater than costs)  
 5 ☐ (benefits significantly greater than costs)

13. Have you heard of/are you currently using any of the following:

|                                                                                                                                                                                               | never heard of it        | heard of it              | using it                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|
| a) filters and blockers (e.g. filtering email spam, filtering web content, blocking pop-up windows)                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| b) encryption tools (e.g. encrypting email, encrypting transactions, encrypting documents)                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| c) track and evidence erasers (e.g. spyware detection and removal, browser cleaning tools, cookie cutters, activity traces eraser, harddisk data eraser)                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| d) pseudonymiser tools (e.g. CRM personalisation, application data management)                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| e) anonymiser products and services (e.g. browsing pseudonyms, virtual email addresses, trusted third parties, surrogate keys, automatic anonymisation of data after a certain lapse of time) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| f) information tools e.g. (privacy policy generators, pāp, privacy policy readers/validators, privacy compliance scanning)                                                                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| g) administrative tools (e.g. identity management, biometrics, smart cards, permission management, monitoring and audit tools)                                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

14. How effective do you consider privacy protection by technical means in reducing the risks associated with holding personal information?

1 (not effective) ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ (very effective)

15. If you believe such technologies are useful, but you are not currently using them, what are the reasons for this?

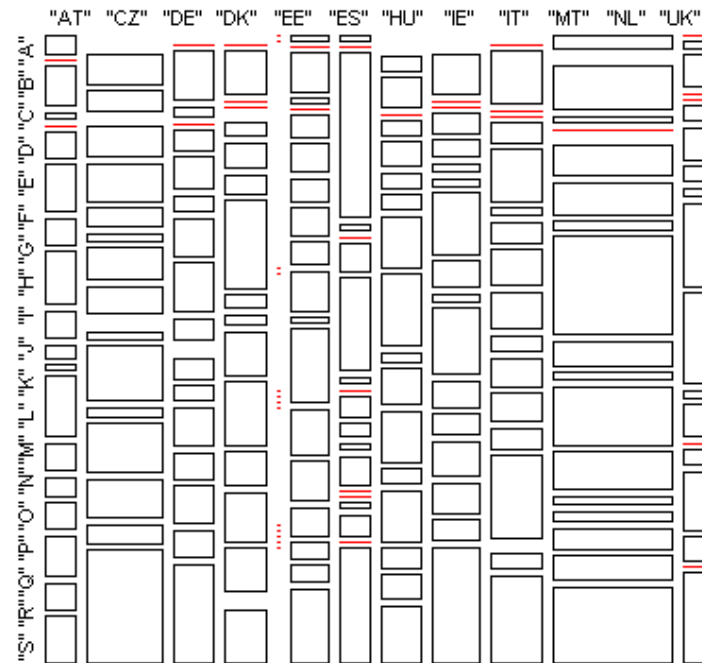
- ☐ Firm size  
☐ Limited applicability for my business  
☐ Lack of awareness about the technologies  
☐ High costs of the technologies  
☐ Limited benefits associated with data protection  
☐ Lack of necessary technical know-how  
☐ Consumers accept current level of protection  
☐ Low level of sanctions associated with misuse of personal information

16. What, in your opinion, could the public sector do to help businesses to benefit from technical means of protecting personal information? [insert text]

## Business survey supplementary graphs

### Sample distribution

Figure 60: Distribution of sectors across Member States

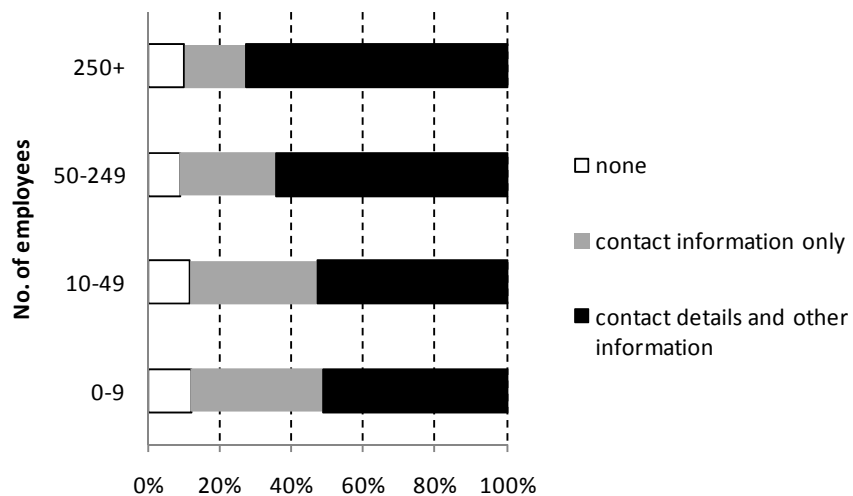


Note: Column and row labels are equally spaced, whereas the width of the columns themselves indicates the volume of observations. This means the first column represents observations on AT, the second column observations on CZ, the third column observations on DE, the last but one column represents observations on NL, etc. Thin (red) lines indicate missing values. Sectors (vertical axis) are labelled as NACE (rev. 1.1) sections.

Source: London Economics

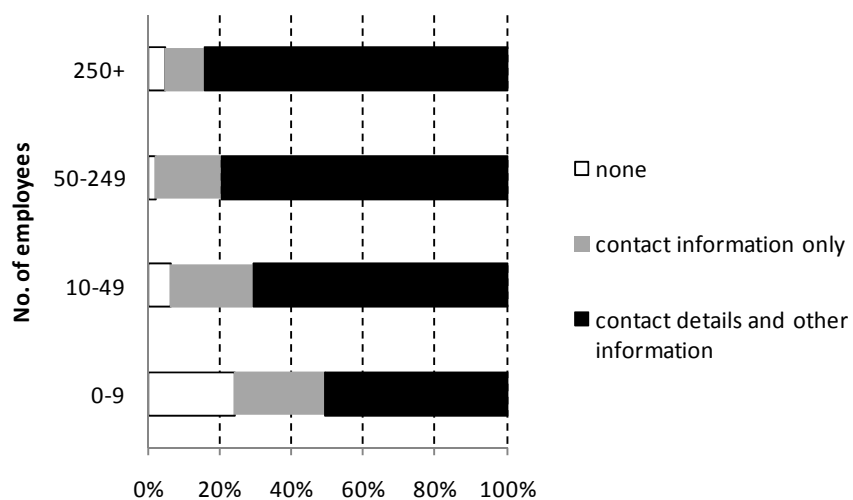
## Data use

**Figure 61: Type of personal data held on CUSTOMERS, by business size**



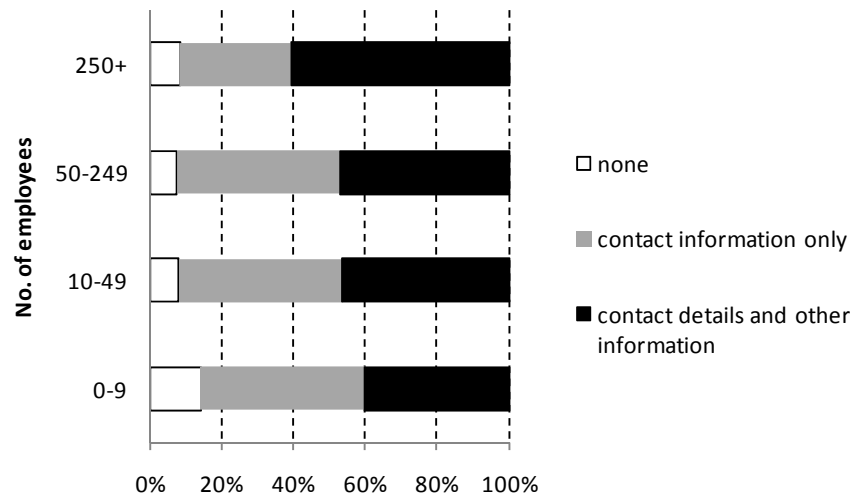
Source: London Economics

**Figure 62: Type of personal data held on STAFF, by business size**



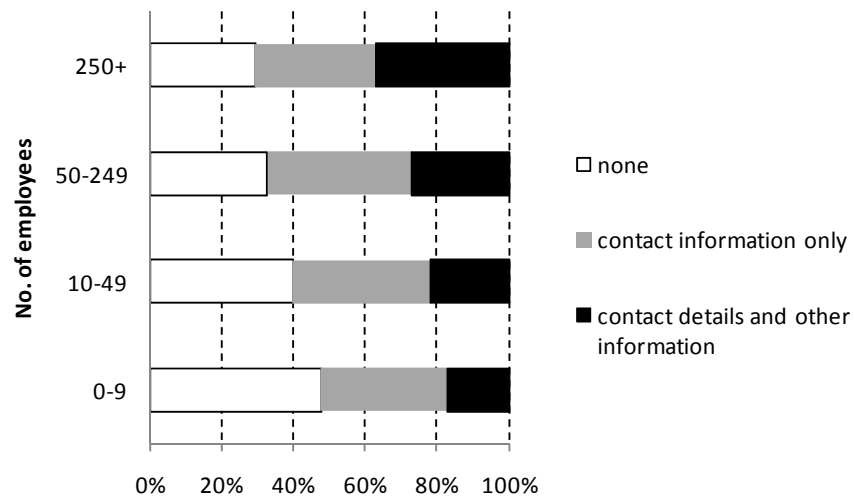
Source: London Economics

Figure 63: Type of personal data held on SUPPLIERS, by business size



Source: London Economics

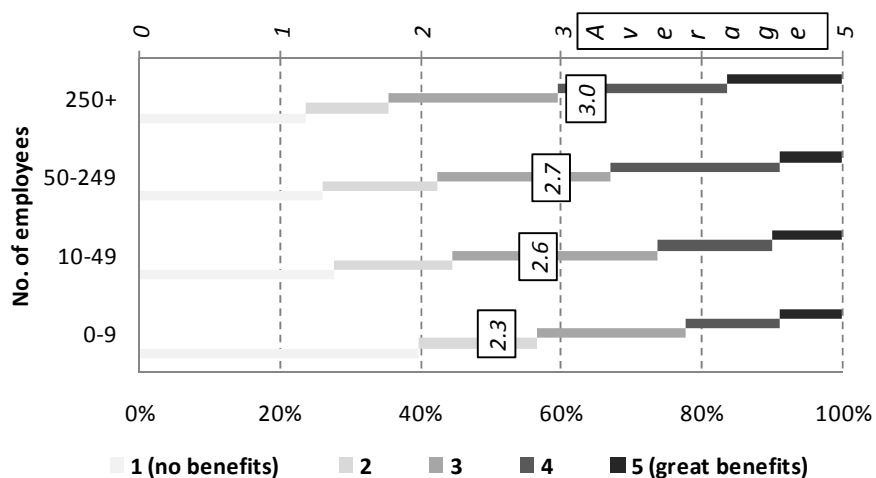
Figure 64: Type of personal data held on 3rd parties, by business size



Source: London Economics

## Benefit from holding personal data

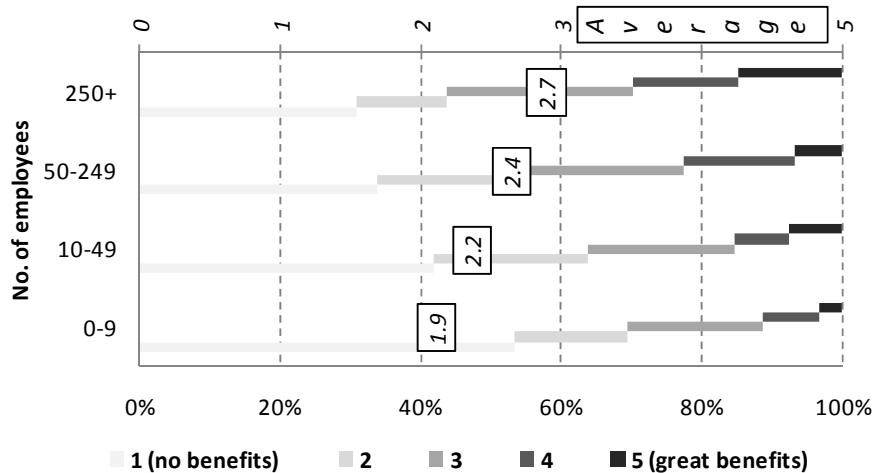
Figure 65: Benefit of personal data on suppliers, by size of data controller



Note: combined score of benefit from personal data on 1) customers, 2) staff, 3) suppliers, and 4) 3rd parties.

Source: London Economics

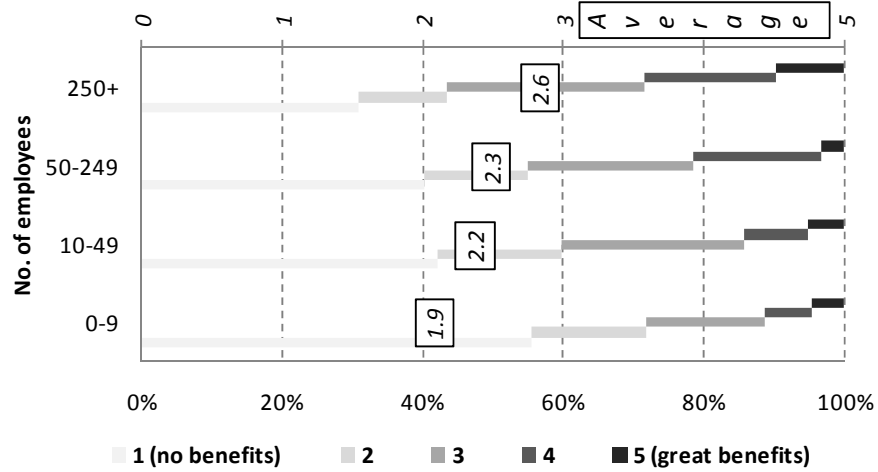
Figure 66: Benefit of personal data on staff, by size of data controller



Note: combined score of benefit from personal data on 1) customers, 2) staff, 3) suppliers, and 4) 3rd parties.

Source: London Economics

Figure 67: Benefit of personal data on 3rd parties, by size of data controller



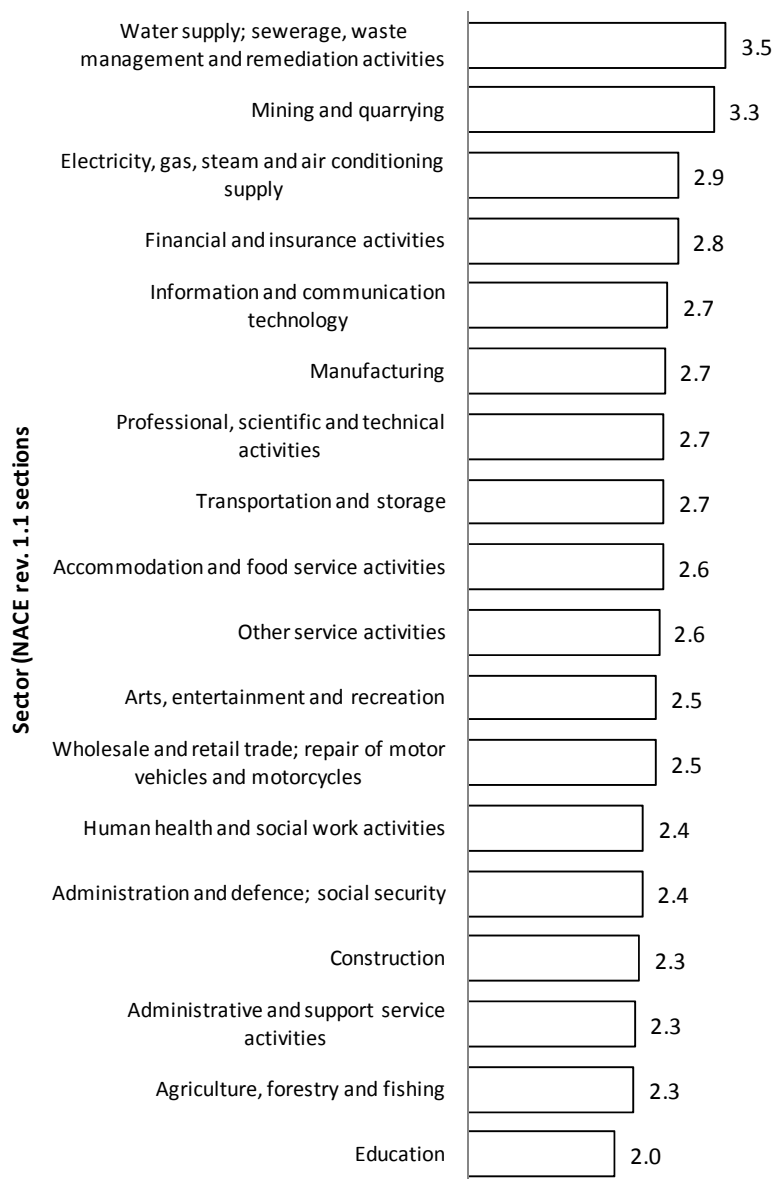
Note: combined score of benefit from personal data on 1) customers, 2) staff, 3) suppliers, and 4) 3rd parties.

Source: London Economics



## Benefits of personal data by sector

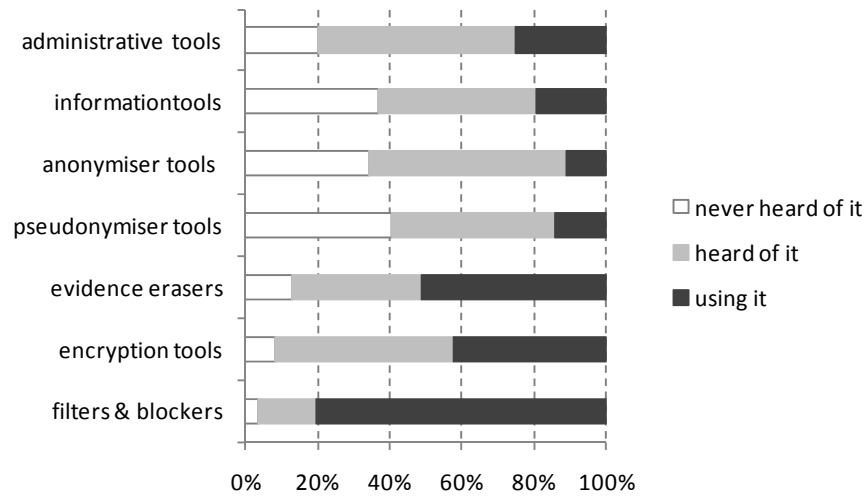
Figure 68: Average benefit of personal data by sector



Source: London Economics

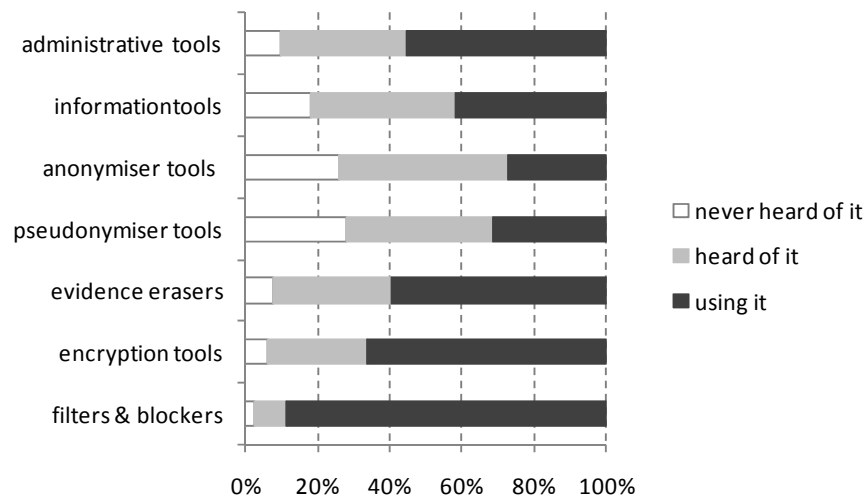
## Awareness of PETs

Figure 69: Awareness of PETs - SMEs



Source: London Economics

Figure 70: Awareness of PETs – non-SMEs



Source: London Economics

