

Workshop on the Economic Benefits of PETs

Brussels, 12 November 2009

Introduction

This is a report into the proceedings, including presentations and subsequent question and answer sessions, of the European Commission's Workshop on the "**The Economic Benefits of PETs**", which took place on 12 November 2009 at the Hotel Crown Plaza Loi in Brussels. This Workshop is part of an ongoing study launched by the Commission into the economic benefits of Privacy Enhancing Technologies (PETs).

The main focus of the Workshop was to present the Interim Report into the study on PETs, which is currently being carried out by London Economics. The Workshop was attended by about 50 experts in the field of PETs, bringing together a broad spectrum of stakeholder expertise including developers, data controllers, public authorities, users/consumers and government. The aim was to highlight, discuss and deliver.

To highlight through practical experiences the transposition of PETs into the public and private domains, to discuss the practical workability of PETs from an economic perspective and to debate how PETs can be delivered and ultimately how it will be of benefit to all, institutionally, commercially and in our private lives.

Growing in importance

The European Commission has over recent years been increasing its funding into the development of technologies which aims to making breaches of certain data protection rules more difficult and/or helping to detect them.

Over the last few years, growing concerns about privacy violations as the result of the disclosure of personal information have been increasing. A recent Flash Eurobarometer survey (No. 225 – Data Protection) showed that close to two-thirds of EU citizens are concerned about how organisations actually handle personal information, in fact nearly 82% of respondents were not convinced by security provisions in relation to online data transmission, and more specifically to the transfer of personal information over the Internet.

Therefore the growing importance and primacy of data security and therefore of Privacy-Enhancing Technologies (PETs) in particular, is becoming more and more apparent. PETs include technologies such as encryption or anonymisation tools, as well as more complex technologies, such as P3P or automatic use-by dates for personal data. These technologies have an important role in improving the security of digitally stored personal information, and in providing not only a secure platform for data protection but more importantly providing a secure data environment for doing business and general online communications, both in the public and private sectors.

In particular, the Commission has been highlighting the importance it places on Privacy Enhancing Technologies (PETs), encouraging consumers to use PETs through awareness raising campaigns. The Commission has been steadily investing in data protection and privacy projects, studies on PETs' economic benefits and standards for using PETs.

The EU's contribution to research into PETs in the current Seventh Framework Programme (FP7) will go beyond the funding allocated under the previous Sixth Framework Programme (FP6), which reached more than €18 million on PET research alone. Under the Seventh Framework Programme, twenty-four new projects were launched from 1 January 2008 in the areas of Information and Communication Technology Security, identity management, and privacy and trust, across all of which PETs is playing an increasingly important role.

As part of its investment into new technologies and in particular the issues of public and private security linked to information and data retention, the Commission launched a project to study and analyse the economic benefits associated with PETs. London Economics were duly commissioned back in June 2009 by the Directorate General for Justice Freedom and Security (DG JLS) to carry out the study, and its subsequent Interim Report contains the first four months analysis of a nine month project, the basis of the Workshop in question.

Introducing the Workshop

This Workshop was co-hosted by the Directorates General for Justice Freedom and Security, and for Information Society and Media (DG INFSO). After introductions and opening presentations from Marie-Hélène Boulanger (DG JLS) and Dirk van Rooy (DG INFSO), London Economic's Gavan Conlon (Divisional Director) and Moritz Godel (Economic Consultant) presented their Interim Report for DG JLS on the economic benefits of PETs. After a short yet animated question and answer session, the first of three discussion panels was launched. Each panel was comprised of three presentations followed by a discussion session.

Panel I

Moderated by Niovi Ringou (DG JLS), the first presentation “**Why the adoption of PETs takes so long**” was given by John Borking, Director of the Borking Consultancy; this was followed by Jonathan Bamford, Assistant Director of Data Protection Development at the UK Information Commissioner's Office whose presentation was entitled “**The Business Case for Investing in Proactive Privacy Protection – the UK experience**”, and finally before the question and answer session wrapping up Panel I, Katalyn Egri, Head of Department of International Affairs at the Hungarian Data Protection Authority, presented “**Application of PETs and experiences in Hungary**”.

Panel II

Moderated by Hana Pecháčková (DG JLS). The first presentation, “**Lessons for Future PETs Standards: Looking Back at P3P 10 Years on**”, was presented by Ari Schwartz, Vice President and Chief Operating Officer of the Centre for Democracy and Technology. Bojana Bellamy, Director of Data Privacy at Accenture then presented “**Embedding data privacy into corporate DNA: from PIAs to PETs**”. The

final presentation of Panel II came from Yoram Hacoen, Head of the Law, Information and Technology Authority of the State of Israel (ILITA) “**The regulator’s role with PETs**”.

Panel_III

The final panel was again moderated by Hana Pecháčková (DG JLS), with the first of the final three presentations coming from Jonathan Weeks, Deputy Director of Legal Affairs at Intel EMEA Headquarters, the title of his presentation was “**Integrating Privacy Enhancing features – beneficial to all**”. Carole Pellegrino, a Public Affairs Manager at SAGEM Securite, then presented “**A reflexion on the labellisation of biometric products**”. The final panel presentation of the day was given by Stephan J. Engberg of Priway – Security in Context “**Without PETs Democracy and Markets won’t work**”.

OPENING REMARKS

“Promoting data protection through PETs”

Marie-Hélène Boulanger – DG JLS, European Commission

Marie-Hélène Boulanger began by highlighting the fact that rapid technological developments are challenging the protection of personal data and of an individual’s privacy, and of the extent of control an individual has over the use by others of their personal data. It is in this vain that the Commission hopes to ensure that technology becomes a tool to strengthen data protection and the privacy of the individual, rather than witnessing an increase in privacy invasive technologies.

While technological development was essential, it should be combined with legislation – technology will never replace the need for legislation, but it can complement it. In the past the Commission has done some considerable work in this area, referring to the PETs workshop dating back to 2003 following the first Implementation report of the Data Protection Directive. The report made clear that the use of PETs was already an integral part of the Directive, and the Commission realised that it was necessary to take additional measures to promote the use of these technologies. The May 2007 Communication “Promoting personal data protection through Privacy enhancing technologies”, identified the need for further development of PETs (in particular through RTD projects and large-scale pilot demonstrations) and their use by industry and public authorities, involving a broad spectrum of actors, including the Commission services, national authorities, industry and consumers.

Eurobarometer surveys were conducted both in 2003 (in 15 Member States) and in 2008 (in 27 Member States) relating to data protection. Separate surveys were also conducted in relation to the perceptions of data controllers and the perceptions of citizens. However, as far as PETs were concerned, the Commission felt it did not receive strong enough results.

Wider use of PETs would improve privacy protection as well as help fulfil data protection rules. Better respect of data protection rules would also have a positive impact on consumer trust, along with a number of promising and value-added services that rely on transfers of personal data across IT-Networks. The objective of London Economic’s study is to assess the economic impact of PETs covering both the public

and private sectors and to explore to what extent the deployment of PETs could be economically beneficial and how they could be measured.

It is felt that if the economic benefits are identified, then stakeholders would in turn be encouraged to integrate PETs into their applications. For the public sector, e-government applications entail the use of ICT in the daily working life of public administrations, including electronic identification as well as other more transactional online public services such as tax declarations, e-procurement and e-social security – a way for public administrations to be more transparent, service-orientated and productive. For e-government to function well, users would need to see the security and confidentiality of their personal information is guaranteed. While deployment of PETs across the private sector could result in economic reward for the industries using them, it could create a “snowball” effect, encouraging other companies to pay greater attention to respecting data protection rules.

“Privacy enhancing technologies in the ICT research programme”

Dirk van Rooy – Head of Sector for Trust and Security, DG INFSO, European Commission

One of the principal missions of the Directorate General for Information Society and Media (DG INFSO) is to stimulate the development and use of information and communication technologies in order to establish an all-inclusive information society. There are three mechanisms or pillars:

- Firstly, setting regulation and/or policy, in order to establish a level playing field and stimulate competition and the market.
- Secondly, DG INFSO runs the research and development ICT programme, with the aim of increasing competitiveness – the EU needs rapid development, for it to be at the cutting edge.
- Finally, the promotion of wider use, referring to greater and faster uptake as well as market pull.

Therefore, trust and security are of pivotal importance, and integral to this is privacy protection.

Rapid development can sometimes be seen as a problem. Over the last 15 years a “digital wave” or “tsunami” has been running over society, which is not always ready. The growing information society is ubiquitous and service-centric, integrating everything, but it is still under development, with the privacy situation being of great urgency.

A relatively new phenomenon is “The Cloud”, which is used to explain the many privacy/security risks which we are facing as we are putting more and more data out onto a server network, yet we don’t always know into which jurisdictions – this is a new and growing challenge. The knowledge society has developed from the early days of ‘local data’ to company ‘networked information’ in the 1970s-90s where we saw the emergence of PETs, up onto a ‘ubiquitous knowledge’, an open knowledge contribution built around frameworks for identity, transparency and accountability in

the age of ambient intelligence – it is not just data but ‘sets of knowledge’ being generated everywhere.

It has been argued that our democratic values are being eroded digitally, but it is not necessarily true that to establish security we need to sacrifice liberty, justice and freedom, we simply need regulation. The Commission believe that privacy through the development of the appropriate technological measures should go hand-in-hand with legislation, if we are to achieve an appropriate level of privacy protection.

PRESENTATIONS

Presentation of the Interim Report of the study: "Economic Benefits of PETs" Why PETs? Stakeholder views and economic considerations

Gavan Conlon, Divisional Director of London Economics introduced the Interim Report which covers the first 4 months of a 9 month project. The study investigates How, if at all, PETs result in economic advantage for data controllers, it also looks at the effectiveness of PETs, and finally whether cooperation between data controllers and national authorities can enhance economic benefits.

The methodological approach was split into three stages. The first being desk-based was a literature review and development of an economic framework. The second element was built around stakeholder consultations, with responses from 8 Consumer Associations, 12 National Data Protection Agencies and 5-6 Business Associations. At the same time a business questionnaire was developed, focussed on small and medium-sized enterprises (SMEs).

We defined privacy as the concealment of personal data, as a best-fit when it comes to our general economic analysis of PETs. But the real problem was defining PETs, so we adopted a working definition.

The fundamental question is, is there a sub-optimal deployment of PETs? Different groups assess this in different ways – individuals, businesses, data controllers...etc. If deployment is sub-optimal then how can we counter market failure, or if deployment is not sub-optimal then how is the question of cost exceeding the benefits addressed.

Moritz Godel, Economic Consultant at London Economics then took to the stand, and asked the question – Are PETs good for individuals? The initial consensus is yes, as it is considered that PETs can protect individuals from a whole host of perceived data risks. The same views from data controllers were also noted, as they saw the potential benefits outweighing the potential costs. Businesses are always looking to gain a competitive advantage over competitors and protect themselves from risk or from misuse of personal data. PETs however, can also be seen as limiting the ability to use personal data.

London Economics looked at why do data controllers decide to deploy PETs – they showed their initial findings through a Decision Matrix, which found both costs and benefits. On the costs side, loss of efficiency in data processing as well as the

financial cost of PET deployment. While on the benefits side one can see increased sales, competitive advantage and reduced risk of misuse of personal data.

London Economics went on to look into how widespread PET deployment is? Is the deployment of PETs sub-optimal? They also looked at potential market failures, which can limit deployment. Behavioural biases, which are believed to explain the mismatch between stated consumer preferences and observed levels of demand – a survey showed that while 63% of EU citizens were concerned about their personal data, the preference for security did not equal that of demand. And perhaps more importantly, the question of cost – Are the costs of PETs too high for data controllers?

Regarding the costs to the data controllers, evidence from London Economics' business survey suggests that costs are in fact too high at the moment, they exceed the benefits. By holding personal data, businesses believed they were often able to provide better customer relations, and knowledge of buying patterns would enable businesses to simplify online shopping for the customer. And quite interestingly businesses in general don't tend to see the holding of personal data as in anyway divisive or sinister. However, initial findings seem to suggest that businesses are split on the benefits of PETs, with almost half seeing PETs as not simply a business 'cost' but ultimately as an unwarranted expense.

London Economics also asked how effective businesses think PETs in fact were. Initially there appears to be a doubt over the effectiveness of PETs, although Moritz Godel did suggest that it was too early to quantify for the moment. He wrapped up the Interim Report presentation by addressing the question of how public-private sector cooperation can help. He concluded that that there was a need for education on the risks and remedies associated with PETs and a need for information sharing at all levels. Businesses expressed not only their wish for clear and binding international standards but were looking towards pre-packaged PETs – ready to roll.

Interim Report – Question and Answers

Caspar Bowden launched the Q&A session with a scathing attack on the Interim Report, highlighting a fundamental lack of both definition and categorisation of PETs. He went on to assess the results so far as being predictable as a result of questions which were too vague. He sited a list of terms which he suggested should be fundamental to any report on PETs, and which were missing: zero-sum, minimisation, subject access, transparency, threat model, onion routing, differential privacy..., and a "total blindness in the Report to any [...] notion of personal data". In response, **Moritz Godel** accepted there was indeed a weakness with reference to the current research on PETs from a Computer Science perspective. **Caspar Bowden** reiterated his concerns that there appeared to be a general lack of understanding on the subject and that the questions being asked were too simplistic – much of these concerns into the validity and competence of the Report to-date were echoed by a number of other speakers including in particular **John Borking** and **Stephan Engberg**.

Bojana Bellamy suggested that maybe this gave credence to the view from some quarters that we need to in fact look at PETs in a different way, with a wider view – Privacy By Design, and processes rather than pure technologies. **Ari Schwartz** agreed that there was a real need for a clear definition and that the case studies in the Report were muddled and needed more clarity.

Stephan Engberg insisted that PETs should not be categorised into one big group, as in the Report, and there was a need to differentiate between internal risk management (which is more a liability discussion) in companies and balancing the interaction between consumers and businesses. He also suggested that SMEs were not a good model to follow as they are not able to influence PETs effectively by themselves, because this is dictated by the ‘market’ and by government.

Yoram Hacoen highlighted the lack of a geographical aspect, it was too euro-centric – this was defended by the Commission, who took responsibility for the geographical parameters of the study. But Mr Hacoen did also draw attention to the fact that the Report needed to view the ‘tort’ model, as legislation should be very important in the framework of the discussion.

Panel I – Moderator Niovi Ringou, DG JLS, European Commission

“Why the adoption of PETs takes so much time?”

John Borking – Director, Borking Consultancy

John Borking began by outlining some preliminary remarks. The idea in the beginning from the ‘fathers’ of Privacy Enhancing Technologies was that they should enhance privacy, that PETs should not be purely data or information security, privacy alone is not security. PETs have to help realise the legal aspects of the Privacy Directives.

Unfortunately the interim report does not provide a solid workable definition of PETs from the outset. Borking suggested that PETs is in fact a system of ICT measures to protect information privacy by minimising personal data, or at least preventing, without a loss of functionality, any unnecessary or unwanted processing of personal data.

If we cannot do data minimization we still want, and we can process clear unencrypted data within the boundaries of the law, this is what we call Privacy Management Systems.

We are technologically able to solve the privacy problem – PRIME has proven it, as will PRIME-Life. Borking stressed that the problem is, as the Report highlighted, that there is no political imperative – governments appear to be preaching anti-trust legislation and a lower-level security; however, it is necessary to fight for PETs, and not to accept the lower-level for PETs.

In 2004 the Dutch Ministry of the Interior created a 4-pillar list of PETs:

- **General PETs measures** – this is what today’s Report is referring to, the stepping up of PETs to data and information security.
- **Separation of data** – missing in the Report, and a key cornerstone of PETs, the splitting of identity domain and pseudo-identity domains.

- **Privacy Management Systems** – processing data within the borders of legislation, for which there are already ready-to-work prototypes developed by IBM and HP for the market.
- **Anonymisation** – no registration of private data, or at least the immediate destruction of personal data on processing.

The four central questions which came to the fore were; When do organisations bother about privacy? What factors affect the decision to introduce PETs? Is there an organisational adoption problem? And are there drivers and inhibitors for PETs? The research findings were that IT awareness or maturity was really necessary in order to implant PETs. Borking insisted that we cannot go deeper into PETs if we don't have Identity and Access Management.

An American named Rogers developed a model based on an 'S-curve' which is still the standard today for explaining the adoption factors which are affecting innovation, such as PETs which is in itself an innovation. It was based on a question related to technology take-up by farmers in pre-1940s Idaho.

John Borking referred to a series of interviews and a case analysis. These included looking at the characteristics of PETs and those factors which encourage take-up. The relative benefits need to be supported and proven, and the role of advisory institutions such as Data Protection Authorities (DPAs) is crucial to this – they must work uniformly to push PETs and break away from the chronic lack of understanding of PETs in the market place. While the negative results have shown that cost, compatibility and complexity are all hindering the development and take-up of PETs, as predicted by Rogers, PETs can be woven into business processes but not without knowledge. Following on from this, John Borking is proposing to set up a PET Expertise Centre (PreTECH) to help develop and push forward the knowledge on PETs.

The results relating internally to an organisation show that there must be a certain level of privacy regulation awareness available, it was also found that a Privacy Impact Assessment is crucial and should be made obligatory. While the negative points again point to complexity of structure and organisation and the diversity of the information systems in place.

Regarding the external organisation factors, more targeted and clear legislation is a positive attribute regarding privacy principles. Again, one of the clear factors is the role of the DPAs as a point of technical support and information.

“The Business Case for Investing in Proactive Privacy Protection – the UK experience”

Jonathan Bamford – Assistant Commissioner Director of Data Protection Development, UK Information Commissioner's Office

The UK experience in trying to push forward PETs is highlighted by Jonathan Bamford of the UK Information Commissioner's Office (ICO). It is a conundrum that citizens appear to care about privacy yet don't seem to demand that it is provided. In the same vein, organisations care about privacy but balk at the need to spend on

providing enhance privacy protection, and finally, DPAs are at fault in that they don't seem to have done enough to have fostered the uptake of PETs either. So what is being done to get PETs adopted?

The UK Commissioner's Office is increasingly interested, as part of their Data Protection Strategy, in the concept of "Privacy by design". With increasing amounts of personal information, the threat levels to individuals is increasing through the opportunities to exploit personal data and not always to protect it, technological and procedural safeguards are lagging behind. Therefore the Commissioner's Office in the UK is more interested to build in protection rather than bolt on.

The ICO in the UK have supported from the outset, some of the original articulations of PETs, it was seen that PETs could assist legal compliance, empower individuals, inspire personal and market confidence by reducing personally identifiable information.

The question is, why hasn't there been more take-up of PETs? The ICO see PETs as more something to build into a security infrastructure, part of a wider Privacy by Design concept.

There needs to be a better way of explaining PETs, such as the technological complexities of the different forms of ID management, without the general public being confused or losing interest.

The ICO's Privacy by Design report, launched in November 2008 realised that to move forward with PETs, the discourse had to be aimed at the executive level, as they control the 'purse strings', and that a number of barriers needed to be broken down such as poor executive awareness, lack of understanding between privacy and data sharing, the need for internationally recognised privacy management standards.

Many of the benefits linked to PETs remain unclear such as what are the demands for such products, and key to the whole PETs conundrum seems to be the need to engage with executive management. By doing so, executive managers will begin to understand their privacy duties more clearly and in turn be able to communicate their privacy needs clearly and demand Privacy Impact Assessments (PIAs) in system business cases. We need to create not only a popular mandate for Privacy by Design, but along side this we need to highlight not only the benefits to businesses which comply but the costs and risks of not. Finally, we need to develop a simple shared language regarding the concepts surrounding privacy issues.

Promoting PETs

Jonathan Bamford explained that the UK Information Commissioner's Office were keen to promote PETs as envisaged in the Privacy by Design Report, and to encourage their incorporation into products, and organisations to demand the value the access to those products. While the Privacy by Design Report speaks of privacy functionality as a 'deal breaker' in systems procurement, Jonathan Bamford explained that in reality SMEs for instance have different drivers to larger enterprises, and he went on to explain that the problem was basically linked to a general lack of a soundly argued case for investing in proactive privacy protection.

Spending on privacy friendly measures is dual focussed, on the one hand it is procedural, and at the same time spending must also be technologically linked to PETs. People must lock-in to PETs more proactively; they must be built-in, not simply bolted-on. Finally, the arguments for proactive privacy protection must be taken on by those who hold the purse-strings in a company or an organisation, and realise they must spend and invest in PETs in order to move forward.

The work done by the UK's Information Commissioner's Office on the business case for investing in proactive privacy protection led to formal research, which is expected to be published in the coming months. The research looked into the business case for PETs through the perceived benefits derived and the costs incurred. It was recognised that there was in fact a need to look at the wider context to the given value of PETs, as an asset to an organisation, to the individual and to other parties, including those with more malicious motives who would like to steal and use data illegally.

The research Report will cover the need to articulate more clearly the real value of privacy and the consequences of privacy failures. Moreover, it should highlight the various benefits attained by protecting ones privacy and a realistic assessment of the investment needed to provide privacy protection. In conclusion, the Report tries to examine how in fact to create a business case for PETs and how to quantify PETs – there is a real need for numbers, and a value figure to drive PETs forward.

Jonathan Bamford concluded by noting the lessons so far from London Economics' interim Report on the "Economic Benefits of PETs" highlighted that there are many strands working in parallel and for PETs to move forward, we need the driver of an economic case which must be addressed in different ways, which while challenging, cannot be ignored.

"Application of PETs and experiences in Hungary"

Katalyn Egri – Head of Department of International Affairs, Hungarian Data Protection Authority

This presentation focussed on an environment where PETs is being used – the application of PETs with eGovernment. This may help with an analysis of the wider issues and implications related to PETs and businesses in general.

The Hungarian Data Protection Authority looked at three cases. The first case was the "EU eAdministration Strategy 2007-2010". The Hungarian Data Protection Supervisor welcomed the initiative but it could not be set up where it enhanced the central registry or the electronic control of the data rights of the citizen.

The second case was the Central Electronic Services System, which concerned the establishment of an electronic citizens Forum, however when users gave their opinions they could be identified and therefore their political opinions could in effect be retrieved. Therefore follow-up is needed to see how the problem of identifying respondents can be solved, without being able to access their private and sensitive data.

The final case was an electronic Personal Identification System used in public administration. The DP Commissioner could not agree that the central client and identification system would be opened for larger services such as the national public transportation company, but at the moment there is certain draft legislation which would open the central electronic system for public utilities and e-payments, and the Data Commissioner welcomed the fact that it was a free choice for people to choose their eID to be readable without “contact”.

Client Gate

The electronic signature is being introduced, which is very important economically as well as the EU Directive on the basic concepts of electronic signatures. The central government portal (www.magyarorszag.hu) includes the “client gate”, which offers public administration services, and when citizens use the central system they are required to establish a client gate through registration using an electronic signature – identifying the user while also being relatively secure, and e-payments can also be initiated here.

The method of registration is by re-identification supported from the central database, actual sectoral information is avoided at this stage. The use of a sectoral identification is by randomly generated numbers which are linked to a citizen through certification by electronic signature. This allows a citizen to be unambiguously identified by a one way mathematical process linked to the two pieces of data provided. This is all provided for under Hungarian Law (Act CXL: 2004), but the right of processing must be given by the individual who must be fully informed throughout the procedure. It is the data controller who is responsible for ensuring all organisational and procedural measures are followed, and must prevent any misuse either accidental or malicious and ensure it is operated through a divided information system.

In conclusion, Ms Egri explained that the data protection guarantees allow citizens to access their information, retrieve general information, and correct or delete their own data. While investigating eGovernment services it was found that infrastructure could be widely used, while the exploitation of possibilities in the public administration sphere was not so common. There is virtually no legislation making the use of electronic signatures mandatory – being quite country specific – this may delay the spread of PETs, although PETs could be pushed forward by a partial mandatory use of electronic signatures in certain applications. Finally, it is hard for decentralised, commercial services to strengthen and access a higher market share or benefit where there is centralised database development financed by the state.

Panel I – Questions and Answers

Yoram Hacoen posed the question – Are PETs different to data security or not? The view from Mr Hacoen was that PETs are part of it. It seems that PETs are targeted at the “proportionality” aspect - is it ok to collect information, and what in fact do you do with the information. PETs are also linked to duty and the “accountability model” on data security; therefore they should not be seen as just a collection of personal data or a “minimisation” of information but more as a general case of data security. **John Borking** agreed, stating that in his view, data security and data privacy were in fact separate, with PETs reaching over data security.

Stephan Engberg of Priway firstly highlighted John Borkins ‘optimistic’ presentation. He began by suggesting that if we look at the economics of PETs we must first be clear which PETs, as the economics is not constant but different. The second point he made was to suggest that we are failing concerning the economics of security – the question should be how much should we put in. And finally, in the public sector there are not really any ‘customers’ in that there is no one really to put a value to any service provided. This in turn leads to the accumulating inefficiencies of command and control economics; therefore we need to be more clear as to what we are actually analysing.

Jonathan Bamford agreed, suggesting there was in fact a need to value not just simple business case drivers, such as a societal value, but in the public sector there are different but equally powerful drivers.

In response to **Jonathan Weeks’** question on why there seems to be a lack of knowledge of PETs, **John Borking** explained that one of the main problems is that those on the technical side and the policy makers need to learn to speak the same ‘language’ as the private sector business managers. At the same time data authorities often lack a sound knowledge of technologies and how invasive they can be. **John Bamford** took this further explaining that in his view DPAs needed to open up more and be more intuitive and responsive. The DPAs need to ask the private sector what they want, and in response the DPAs will tell them what they need.

Regarding the need for more information on privacy breaches, **John Borking** highlighted the work of the Ponemon Institute in the United States which has been collecting data from 25 large US organisations on loss of data and privacy incidents. He also recommended the Davis Tool which can calculate what the reputation damage will be if a data or privacy incident happens, and the tool can then set off the damage against needed investment – this is an example of the “language of business”. Taking the question of “language” a little further, **Caspar Bowden** highlighted the difference between “Policy makers” and “Computer scientists”, he suggests they are running parallel and quite separately, and to move forward with PETs, these two world really need to come together.

Caspar Bowden then asked Katalyn Egri whether the “Client Gate” was designated as a simply a data controller, or a data processor on behalf of parent data controllers, or a co-controller. **Ms Egri** explained that the Central Registration Authority is the data controller, and is not a data processor.

The question and answer session continued with **Stephan Engberg** who made reference to ongoing political discussions in Denmark at the moment. He wanted to know whether there was in fact one big service taking care of all citizens or numerous services for citizens such as the private sector. He insisted on the need to address the problem of economic discussions between the public and private sectors. **Bojana Bellamy** believed there was a third category to consider, Privacy Officers and CEOs of companies. She thought that PETs would not move forward easily unless the actual money men, the buyers, are brought onboard, and therefore there is a real need to streamline the topic to make it more understood. **Borking** agreed, highlighting again the PET Expertise Centre (PreTECH) to help develop and push forward the knowledge on PETs.

In response, **Yoram Hacoheh** felt that Data Encryption of Notification and Class action were the most effective options available to encourage PETs – once the CEOs understand the outcome of a data bridge then they will begin applying it.

Panel II – Moderator Hana Pecháčková, DG JLS, European Commission

“Lessons for Future PETs Standards: looking back at P3P 10 years on”

Ari Schwartz – Vice President and Chief Operating Officer, Center for Democracy and Technology

Ari Schwartz began by explaining how his NGO, the Center for Democracy and Technology, in fact helped develop in the late 1990s what became P3P, or Proactive Privacy Protection. Today P3P focuses on building metadata tools to process information, which John Borking calls Privacy Management Tools. We can't stop people using personal information but we can control it better using some of the “fair information practices”.

At the end of the 1990s Microsoft built a P3P implementation focussed on cookies for which a spec was released in 2002. When companies became blocked they decided they needed to sort this out, and our privacy rules were set up based on them. The guiding principals of P3P tied it to “fair information” practices and privacy in general.

And some things you had to do when implementing P3P, such as noticing and communication, and building choices and control into the structure as well as fairness and security. Regarding the criticisms of P3P, advocated were concerned early on because it did not appear to implement Fair Information Practices (FIPs), nor did it assure full anonymity or protect privacy on its own – in fact it was not a PET but an add-on to PETs. P3Ps were not able to prevent companies from breaking existing privacy laws. While from the industry viewpoint, P3Ps were too transparent and inconsistent with the terms of future profiling.

The economic impact of P3Ps and why they were not fully realised are borne out by the fact that they were assumed to be just too complicated – there were 18 data “categories”, 7 “purposes”, and metadata interfaces should have been built first.

In fact companies using 3rd party cookies use P3P because Microsoft built an interface to block their cookies if they didn't, therefore Microsoft is the default standard. Expectations should be managed from the beginning. A lot of money went into building P3Ps, and work on metadata standards.

“Embedding data privacy into corporate DNA: from PIAs to Pets”

Bojana Bellamy – Director of Data Privacy, Accenture

Bojana Bellamy gave a very animated and interesting presentation. She began by explaining that for her company, Accenture, and the private sector in general, the beginning and end points are that they have to invest in PETs, and therefore they will have to pass on the cost to the client – they would have to tell their clients for instance

that they have some PET technologies which will anonymise their data, but it will cost them a further 3 million!!

Maybe there is a need to look beyond PETs per say, and find a wider, more workable and inclusive concept of PETs, from technologies to processes which would give PETs a looser definition of "...any technology and process that aids and supports data privacy compliance and protection of data". Ms Bellamy explained that when she looks at the 'top' PETs she looks to PIAs (Privacy Impact Assessments) PBD (Privacy By Design), simply because these are what the private sector can better understand and so can be sold on more easily.

Ms Bellamy asked the question of whether service providers have a bigger interest in PETs than data controllers themselves. She suggested that generally people wanted to realise the commercial benefits of data, while at the same time the service providers were not so interested in data, in which case there is a greater incentive for service providers to develop minimisation techniques in order to securely send data off-shore to say India.

Accenture use PIAs, Data Privacy in System Design, and regarding true PETs they also use Encryption for emailing, and Anonymisation for application outsourcing, data testing and general guidance and practice in reporting and surveys. For this private sector service provider, the primary benefits of PETs are:

- **Preventing liability breaches** – these cover regulatory and contractual concerns;
- **Prevent data breach consequences** – breaches can become are expensive to deal with;
- **Enable global data flows** – especially concerning all the legal and financial restrictions surrounding 'Cloud Computing' and data going off-shore. Therefore anonymisation could help with data going off-shore.

The pros and cons

The benefits seem to be smarter and smoother business processes and economic gains and efficiencies in the long run. While the obvious impediment is the high cost of technologies, as well as the fact that some technologies may only be short lived – something encrypted today may be easily unencrypted tomorrow. There appears to also be a problem with enforcing data security on portable media devices, as well as problems of technological compatibility.

How do we move forward?

There is an urgent need for a standardisation of PETs and a default inclusion in new technologies. We need to be more realistic of the current economic costs to the marketplace, if we are to develop a wider interest in PET take-up. There needs to be a new synergy between Data Privacy Officers and CIOs of IT organisations, and Data Protection Regulators need to step-up to the mark and give greater compliance to PETs compliance – it needs to be seen as a 'must have'.

The regulator's role with PETs

Yoram Hacoen – Head of the Law, Information and Technology Authority of Israel (ILITA)

The final speaker of this second Panel was Yoram Hacoen of ILITA which was established in the Israeli Ministry of Justice in 2006, where they are regulators of data protection and information privacy, credit information services and digital signatures, therefore working under the umbrella of data security.

Mr Hacoen briefly pointed out that they will be hosting the 32nd Conference of Data Protection Commissioners in Israel in October 2010, at which a leading part of the conference will focus on PETs and PBD.

One of his earliest experiences of PETs was with the development of a PET CD-ROM containing the 1992 Israeli electoral roll, which was developed for telemarketing purposes. It contained name, address, date of birth, ID and telephone numbers. The PET successfully applied encryption Identified DRM, software export and functionality limitations, physical marking, and data watermarking. There was a negative security issue though, when the regulator forgot to collect back the CD-ROMs and a few years later the some of the PETs were unlocked. So while the PETs were initially successful one must be aware of the long-life capability of some PETs.

ILITA is currently involved with a number of PETs and PBD projects at the moment:

- biometric e-ID;
- e-Passport initiative (+biometric database);
- technological and administrative separation between alpha-numeric and biometric data + dedicated authority + CPO;
- false invoices;
- information transfer among public bodies;
- PBD/PET RFI.

What should a data protection regulator do? DPRs need to be more aware and locked into technology (biometrics, cloud computing, RFids...). There is a real need for them to understand what PETs are there is a need for an all-encompassing, strong and agreed definition of PETs, as well as a solid understanding of the capabilities and limitations of PETs:

Pre usage PETs

- Data minimization and anonymisation (proportionality)
- Software limitation of use and DRM (proportionality)
- E-Consent mechanism (consent)

In usage PETs

- Data quality solutions (accuracy)
- Encryption (securing the personal data)
- Data watermarking and tagging (accountability)
- Usage logging (accountability)

Finally, we to identify the legitimate use of data – what can we touch and what should remain private. There is a need for consultation with non-biased experts. And we need to promote PET usage through cost reduction, find regulative benefits, and increase the cost for not applying PETs through fines, publish success stories and failure stories such as data breaches. Fines could be used to fund R&D into PETs and PBD (Spain’s data protection office collect something in the region of € 23 m every year in PET related fines). Promote PT and PBD through legislation. Talk to the industry and get involved in projects – at the grass roots is where you learn a lot!

Panel I – Questions and Answers

Caspar Bowden began by highlighting the “PET Award for Outstanding Research in PETs” (<http://petsymposium.org/award/index.php>), which he explained was an excellent opportunity to access examples of rigorous and academic study on Privacy Enhancing Technologies, and perhaps help unlock some of the mysteries surrounding PETs to the less initiated.

He then went on to suggest an excellent post-graduate text book on PETs “Digital Privacy: Theory, Technologies and Practice”, edited by Alessandro Acquisti and Stephanos Gritzalis, which again should prove an excellent guide through the mysteries of PETs.

Finally before the coffee break, Caspar Bowden brought up the subject of anomysation, and the fact that in his view previously anonymised, de-identified data, was no longer as safe as it was. However, there is currently work on “differentiated privacy” which could be more secure – keep data in its original state and simply introduce a query which can perturb any results (for further information view this years winning paper on the awards site mentioned above.).

Panel III – Moderator Hana Pecháčková, DG JLS, European Commission

“Integrating Privacy Enhancing features – beneficial to all”

Jonathan Weeks – Deputy Director of Legal Affairs, Intel EMEA Headquarters

Intel as an organisation approaches the issue of privacy on a number of levels, part of the privacy organisation at Intel is aimed at promoting trust in technology through legislation, but pure technology itself is still the prime mover.

Protecting data is expensive, both to do and when you lose it. Massive data flows require a concentrated and coordinated approach between regulators, civil society, corporations and individuals, with the essential element being technology, and adding on to this is the need for education and awareness, flexible laws, accountability and solid codes of practice.

However, we must at the same time be aware not to create global barriers – in promoting PBD we must ensure global standards other the system will grind to a halt, it would not be able to function in a globalised business world.

One of the projects currently being worked on by Intel is its Anti-theft technology (IntelAT), which is being developed to detect whether a lap top is stolen or lost, and

where necessary this system will hide data. Theft or loss of a laptop or simply the data can generate serious financial repercussions. Approximately 12 000 laptops are lost or stolen at US airports each week, that equates to about one notebook computer every 53 seconds. Intel recently sponsored a study by the Polemon Institute into the actual cost to a company of such losses, it was estimated that the average cost to a company was in the region of \$49 000, with the bulk of this cost coming not from the hardware but from the security breach.

Intel is also looking into technologies closer to PETs in the form of Privacy by Design in the Healthcare sector.

“A reflexion on the labellisation of biometric products”

Carole Pellegrino – Public Affairs Manager, SAGEM Securite.

Biometrics is a set of tools enabling authentication or identification of an individual based upon their physiological or behavioural traits. Most commonly by the fingerprint, face, iris, DNA, as well as the voice, signature, a persons gait and even via the veins – all with different performance capabilities and issues. It can be used as a PET – in Australia for instance, biometric methadone dispensers were developed to assist drug addicts.

While biometrics is one of the most secure technologies, it does however raise some potential privacy concerns including misuse and/or abuse, breach and Function Creep. And with issues specific to biometrics, *a priori* non revocability.

Biometric data falls under Directive 95/46 on personal data protection, however, there are different legal perceptions existing which create difficulties when transposing into national laws. In most countries there are currently no specific provisions on biometrics in the Data Protection laws. While in others, biometric data is considered quite sensitive when it reveals racial or ethnic origin identifiers or health data. And in some Member States such as France, biometric data is considered as “sensitive data”.

Legal proportionality across borders is becoming a complex issue. For instance, biometrics linked to time attendance at work is accepted in both Portugal and the UK, but not in France or Italy.

Why should we develop PETs for biometrics?

- Protect consumers’ privacy and enhance users' confidence
- Prevent impersonation
- Enable industry to build solutions on a solid foundation
- Develop standardised processes instead of following a case-by-case approach
- And because there exists precise and operational risks, threats and vulnerabilities which biometrics can address.

Much effort has been put into formalising the discourse on Security, including formal requirements, evaluation and certification protocols with appointed authorities. A similar effort need to be devoted to Privacy, in particular we need to develop a solid

working definition of Privacy, so we can develop objective and transparent criteria to measure the level of Security and Privacy provided by a technology.

The evaluation of biometric products is currently limited to performance evaluation such as speed characteristics and accuracy measures. Privacy and Security shall though become “a positive-sum paradigm” through the development of a number of different tools such as:

- **Common Criteria Methodology** – which is an internationally recognised methodology used for security features and performance of IT security products and services, which can be developed to fit in with biometrics.
- A second tool is **bio-encryption** – based on template protection, it converts biometric data into encrypted data so it can not be retrieved, the converted data can serve as password, anonymous identifier, or pseudo identity, however performance of converted biometric data is lower.
- Finally, a **multi-biometric approach** - two biometrics could be combined, although they would be degraded to hinder direct recognition, while the combination of the two templates would allow recognition, although this needs to be developed further to counteract the negative trade-offs between accuracy and privacy.

In conclusion, Ms Pellegrino highlighted that as many have suggested today, the current legal framework needs to be updated. And while there are tools available to protect privacy, or they can be developed, the DPAs and industry need to work together more directly – we need a precise definition not only of PETs but of the of risks, threats and targets, and we need to define a relevant certification business model.

“Without PETs in a digital world there would be no Democracy or market-driven prosperity”

Stephan J. Engberg – Priway: Security in Context

Stephan Engberg began by highlighting four successful PETs systems:

- Democratic Election
- Cash Money
- Broadcast radio/tv
- Car GPS Navigation

From this he went on to explain the need to develop and standardise a working vocabulary – terms of definition which included:

- **Privacy Enhancing Technologies** – creating anonymity and enabling services without any transfer of control, identity or data.
- **Privacy Friendly Technologies** – which help to reduce internal risk and create better data protection compliance.
- **Privacy Invasive Technologies** – eliminating privacy, and like biometrics they can be quite invasive.

But what is privacy? It is security from the viewpoint of one stakeholder, therefore businesses also have privacy. And the control of personal data is important; it is about having control of the ability to refer data to physical entities and from there the ability to transfer data between contexts.

He then turned his attention to the economics of PETs, or more precisely the economic frameworks. Looking at Ludwig Von Mises “Behavioural Economics” which suggests damage to the market comes from government regulation. Then looking at the externalities of PETs, it was suggested that PETs was the only mechanism we know of to re-empower the demand to drive the economy. According to Laissez-faire economic theory prize cartels cannot be upheld unless enforced by government regulation, and “Code is Law”. Therefore infrastructure cartels can block the market by enforcing certain interests (gatekeeper, access to data) within a small group and make all the others more vulnerable. In Europe, a lack of privacy is preventing our markets from moving ahead.

To summarise Stephan Egbergs rather technical economics based presentation. Markets cannot overcome the negative externalities of eID, while in the political context investment should be tailored to a PET National ID. Cartel standards are actually blocking competition and innovation, which should fundamentally be a responsibility of the EU. There should be greater focus on commerce and public services. Service providers cannot deploy PETs themselves; it is public administrations which actually hold the largest potential. In effect, PETs should be seen as future oriented, stabilising and driving innovation, they could be a key to unlocking the potential for the global markets.

Closing remarks – Hana Pecháčková, European Commission

Ms Boulanger wrapped up proceedings by thanking everyone for their useful, wide ranging and interesting presentations on PETs, Privacy and Security and on of course the interim Report by London Economics.

We saw today that protecting data is challenging not only in the EU, but globally. At the same time we also saw that it is necessary as it holds one of the keys to unlocking economic gains and benefits on a global scale.

The Workshop included not only interesting and sometimes rather technical theories of economics, but also controversial opinions and focussed practical examples. Not only have today’s proceedings been extremely helpful for the Commission and its ongoing study on economic benefits of PETs, but it will be a great help when looking at the future of data protection and how legislation should be adjusted to respond to the myriad of global challenges posed by new technologies. It is hoped that the results of today’s Workshop shall go a long way towards helping all see where the economic benefits of PETs lie, and how to measure them.

If the economic benefits are identified, it would be a strong incentive to all the stakeholders, including both public and private sectors as data controllers, to deploy PETs in their applications.

Closing remarks – London Economics

Beginning the closing remarks for London Economics, **Patrice Muller** (Partner in LE) thanked everyone for their contributions, criticisms and support, all of which will be taken on board. He then followed on by explaining that there was more literature which has not yet been cited, some of it because it focuses on a ‘games theoretical approach’, and in London Economics view this is not robust enough to manage the marginal changes in the assumptions, but Mr Muller assured the audience that the literature will be expanded as the project moves forward.

Then, with reference to a further criticism earlier in the day, he explained that benefits and costs needed to be looked at from two angles. Firstly, we need to look at the individual benefits for a company to invest in PETs, this is critical; and secondly, the broader externalities should be considered – whether we depend on the market for the lead, or whether the market is regulated and additional incentives are imposed from the outside.

Caspar Bowden interjected again, with a question relating to the call for tender for the project, because he felt there appeared to be a glaring lack of expertise on show from the team running the project. **Bojana Bellamy** wanted to focus on consumer empowerment. She agreed that consumers, when directly interviewed are worried and concerned about privacy related issues, as has been highlighted by numerous recent barometer type studies. She felt that consumers are generally not always capable of understanding the complexities of privacy, security, PETs etc. and it would be more useful to develop rules of accountability than directly empowering the consumers themselves – Ms Bellamy stated that she thought consent was ‘dead’ because of a lack of necessary understanding. **Stephan Engberg** disagreed, believing that the consumer should have the option of consent, not because it really matters what they actually think but what really matters is how they act. Markets will not work unless the value chains orient towards the needs of the consumer, and consumers vote through their actions.

John Borking briefly examined the question of how privacy had originally been dominated by lawyers as it was seen as a legal issue, then as we can see today technology became emperor and so by default it is the language of economics which is prevalent – privacy is therefore very much a multidisciplinary issue. But we need to begin exploring the social side as well – a good starting point is the work of Dinev in the United States.