DELIVERABLE D3.4A – Ethical Brief on PETs

HIDE PROJECT

Project funded by the European Commission-FP7

Contract: 217762

Co-ordination and Support Action (CSA)

Start date of the project: 1 Feb 2008

Duration 36 months

1° Reporting Period

Deliverable:	D3.4a *Intermediary*
Title:	Ethical Brief on PETs
Due date:	30.07.2009
Actual submission date	30.07.2009
Lead contractor for this deliverable:	Cesagen
Contact:	p.mccarthy@lancaster.ac.uk
Dissemination Level:	PU

Contents

1. Citizens and the Surveillance Society

Since the terrorist attacks of September 11, 2001, it has been argued that a shift in society has occurred towards an increased tolerance of surveillance and detection measures to ensure security.[1] Such trends have not been universally accepted and nor has the growth in security and detection technology innovation and deployment been smooth. The consequences of the emergence of an increasingly more surveillance and security orientated society have been numerous and raise a number of substantive ethical, legal and social questions as to their impacts.[2] For some commentators there are major concerns relating to deployments of these personal detection technologies.[3] However the perceived problems and threats to privacy that arise out of data collection and processing are not new phenomena. Concerns over the nature of privacy, threats to privacy and the balance between personal space and public interest are contested and negotiated areas rooted in the contours of western development.[4]

While security is an important driving force of a surveillance society it is not the only one. Trends towards increasing digitalisation of existing data along with growth in the collection of new data (such as biometric data) has led to an exponential growth of databases for public and private purposes. These databases in turn are becoming increasingly interoperable allowing for data sharing and comparison within member states, between member states and between the EU and external countries.[5] Within the EU the removal of barriers for the operation of the common market was identified as presupposing a need for information as elements of a digital economy to be able to cross borders as easily as other goods and services.[6] The guarantee for individuals in exercising mobility within the Union also necessitates the sharing of data between member states.[7] This is added to the need for data on individuals who travel which – while often located in security debates – are also related to issues of migration. It is clear though that there has been a 'securitisation' of these debates which has had implications on the rationale for data being collected, what types of data are collected and the uses to which they are put.[8]

These provided much of the impetus for directives on data protection initiated by the EU. Such motivations were guided by the need for there to be a common *baseline* of protections for data that would be present across the Union. New technologies have however continued to force refinements in regulatory approaches dealing with privacy and there is a clear sense that future trends in personal detection technologies will create formidable challenges to privacy and data protection regulations.[9] In this brief we examine the development and implementation of privacy enhancing technologies.[10] PETs encompass both existing technologies (such as encryption, digital signatures) as well as new and emerging technologies (such as biometric revocable identity systems). There is a diverse range in their typology, implementation, focus as well as the manner in

1 Raul 'Privacy and the Digital State: Balancing Public Information and Personal Privacy' (2002)

2 Taylor 'State Surveillance and the Right to Privacy' (Surveillance & Society 2002 (1))

3 'A Report on the Surveillance Society' For the Information Commissioner by the Surveillance Studies Network (2006); Lyon 'Surveillance Society: Monitoring Everyday Life' (2001); Zureik and Salter 'Global Surveillance and Policing' (2005)

4 Shank 'Privacy: History, Legal, Social, and Ethical Aspects' (1986)

5 Mitrou and Moulinos 'Privacy and Data Protection in Electronic Communications' (2003)

6 'GÉANT – data-sharing driver for Europe's digital economy' (2005) Public Service Review - European Union, Issue 10

7 Otjacques et al. 'Identity Management and Data Sharing in the European Union' (2006)

8 Professor Ole Waever coined the concept of 'securitization' in 1995. See Waever "Securitization and Desecuritization" in Lipschutz (ed) On Security (New York: Columbia University Press 1995)

9 Cate 'The Global Challenge to National Data Protection of Networked Digital Information' (Bilateral Conference on Cross Border Data Flows and Privacy, Washington DC, October 2007)

10 Cranor 'The Role of Privacy Enhancing Technologies' (2003)

which they are used. We can summarise the key trends providing the backdrop for the implementation of privacy enhancing technologies as,

- The development of new technologies, including importantly the use of biometrics, which raises new concerns over the nature of data being collected.
- A large increase in the amount of data being collected on citizens by the state and other organisational actors.
- Movements to make such databases and the technologies feeding data into them interoperable
- Transnational co-operation on ensuring safety and security leading to data sharing between relevant governmental actors.
- Increased 'shelf-life' of data, where it is retained, and subsequently put to uses not first envisaged during its collection.
- Automation of data collection, storage and processing by an increasing number of governmental and other actors.

2. Defining Privacy

Recent data losses by government agencies in some member states as well as by commercial entities have begun to highlight for individuals the threats that can arise from data on them being compromised.[11] This has for example led to increased awareness about crimes such as identity theft. One of the fundamental rights of citizens within the EU is the right to privacy and to have a private life. Various legal documents in the EU enshrine this right to privacy in different ways.[12] Yet aside from the legalistic concerns the right to a private life is as much a social and ethical construct as it is a legal one. What is meant by this is that privacy is a relatively fluid conception and one which is subjected to ongoing negotiations and contestations as to what constitutes a 'private' life or space. This process of negotiation has been enmeshed within debates arising out the development and application of new technologies. The visible signs of this can be seen in the regulatory patchwork and official documents framing data protection legislation as well as the shifting discourse of privacy/security in light of recent terrorist threats and attacks.

Taken together we hold the view that each of the trends and elements noted previously, either solely, or in combination has led to an increased public *awareness* and *concern* over the nature of data being collected, its uses, and who is allowed access to this data.[13] Yet it should not be taken that this awareness or concern outside of official and technological literature has coalesced around perceiving the benefits of PETs. We are concerned that such a 'design turn' in responding to these challenges may not necessarily deal with the ethical and social issues that arise out of the development and deployment of personal detection technologies. Indeed a reliance on technological responses may simply gloss over important issues. Privacy has been a contested and debated concept and it is difficult from any review of the literature to outline a universal definition of privacy. However, from the point of view of regulation concerns over privacy have been resolved through data protection.[14] Arguably the modern notion of privacy has in regulatory terms been confined to questions of *informational privacy*.[15] Historically, approaches focused on the spatial and non-

11 'Brown apologises for records loss' BBC News, 21 November 2007

12 Most importantly the 1995 Directive 95/46/EC on the protection of personal data

13 This growing concern over issues of privacy has also been stressd by others. See for example Smith, Milberg and Burke (1996) "Information Privacy: Measuring Individuals' Concerns About Organizational Practices" MIS Quarterly, 20(2)

14 Bennett 'Regulating Privacy: Data Protection and Public Policy in Europe and the United States' (1992]

15 Clarke "Introduction to Dataveillance and Information Privacy" (1999]; Turkington "Legacy of the Warren and Brandeis article: the emerging unencumbered Constitutional right to informational privacy" (1990)

interference aspects of privacy were the primary drivers in negotiating the meanings of privacy.[16] In the example of space the articulation of there being forms of divisions between 'private' life and 'public' life can be seen as early as the Ancient Greeks. Such principles that individuals have a right to a private life, a space secluded from public scrutiny continues to hold resonance in declarations and conventions describing fundamental freedoms and rights for individuals especially where there has been conceptualised as the space of the 'family' or the 'home'. The right to 'be left alone' is attributed to the 1890 article by Warren and Brandeis which itself was a response to changes in media, reflected by journalism and new developments associated with photography.[17] In essence the concerns expressed were the ways in which new technologies were rendering intimate details accessible to the public.

The risks associated with such developments are the perception of their potential ability to render intimate details knowable. In essence particular technologies were perceived as rendering private spaces into public ones. Important is the observation that such drives occur within society as a result of technological developments. Whereas it was photography in the 1890s or networked information systems in the 1990s legal responses have attempted to shape and reflect societal and individual concerns about what is public, what is private and what is acceptable or not in terms of intrusions. It is also a feature of privacy discourses that the notion of personal space has been subject to revisions as a result of technological and social development.[18] As such a personal space as we might conceive of it currently may refer not only to geographical spaces (for example legal restrictions on unauthorised access to one's home) but also as well to the personal spaces associated with the body or bodily functions (the 'naked' scanner controversy illustrates these notions of privacy). Increasingly it is also about virtual spaces where identity may only be constructed through projection of and collection of data on multiple digital identities.[19] Indeed one of the principal rationales for the implementation of biometric technologies has been the promise of being able to link all of these multiple digital identities to one unique identifier.

The articulation of concerns over these aspects of privacy within the EU can be seen in article 8 within the Convention for the Protocol of Human Rights and Fundamental Freedoms echoing sentiments expressed in Article XII of the International Declaration of Fundamental Human Rights. Both reaffirmed the right to a private family life with article 8 extending this to communication except in instances such as the ensuring of security, economic well-being or national interest of the state which is reasonable and not arbitrary. Similarly the convention raises the protection of personal information to the status of it being a fundamental right. The level of concerns expressed over informational privacy has been spurred on by developments in IT and the expansion of the 'virtual' world. In particular the emergence of the Internet has increased concerns over informational privacy in tandem with significant growth in data collected on individuals. If as Agre suggests that "...control over personal information is control over an aspect of the identity one projects to the world" and that the right to privacy is to be free from restrictions and or constraints in the construction of this identity, then the notion of digital identities, whether these be located offline or online require consideration.[20]

However while the right to privacy is often seen as a fundamental element of citizenship it must be placed against the argument that modern states, including supra-national ones such as the EU are only possible in many ways through the collection of data on citizens. As a historical example of this the operation of the welfare state system across Europe brought with it a need for information on citizens to determine

16 Sommer "Personal Space" (2008)

17 Warren & Brandeis "The Right to Privacy" Harvard Law Review, December 1890

18 Friedman "Privacy and Technology" Social Philosophy & Policy, Volume 17, 2000; Bennett "Visions of Privacy" (1999)

19 Windley "Digital identity" (2005); Lyon (eds) "Surveillance as Social Sorting" (2003)

20 Agre (eds) "Technology and Privacy: The New Landscape" (1998)

entitlements, to deliver effective services as well as to assist in their administration. As Lyons has argued modern societies are surveillance societies due to the fact that data on citizens is often a prerequisite for the organisation and implementation of many activities of the state.[21] Indeed these are activities that citizens actively pursue to benefit to themselves and are activities that constitute what it is to be a citizen. The pursuit of being able to engage in such activities and access such services has led to the growth in the amount of information stored on individuals by the state. It is not however solely the state of course that has required or made use of data on individuals. The commercial and private sector has similarly made use of personal data, so much so, that in some cases it is difficult to ascertain how modern societies could function without data, both personal and organisational. In much of the literature, official and academic, we are faced by recourse to the idea of balance or proportionality, or to what extent can privacy be sacrificed for the pursuit of security or the pursuit of activities necessary to engage in society. Others have though argued that resorting to notions of balance excludes an important argument that privacy may not need to be sacrificed in order to perform these functions, that PETs represent an avenue for example where we can have privacy and security in a 'positive-sum' fashion.[22]

3. The EC Communication on Data Protection by Privacy Enhancing Technologies and Data Protection Directives

The EU focus on privacy enhancing technologies is encapsulated in the Communication on Data Protection by Privacy Enhancing Technologies from the Commission to the European Parliament and the Council. Although this is not the only European document dealing with the issue of PETs, it nevertheless represents an indication of policy futures involving PETs. In the introduction to the communication a number of issues are highlighted as illustrating the need to develop and deploy PETs more widely. These are,

1. Intensive development of ICT allowing for the expansion of the provision of new services
2. These services becoming more available to citizens online within 'cyberspace' with the material for such services being personal data
3. The porous nature of borders or restrictions to transnational and international mobility of data held on citizens

It is the nature of the risks that these developments produce that form the key target for intervention of PETs. Such risks are held to be diverse and extensive and for the Communication include 'identity theft, discriminatory profiling, continuous surveillance or fraud'.[23] It is striking from even these four examples that there is a wide scope of perceived risks. Similarly these examples straddle concerns with private and public deployments as well as organisational and individual concerns. As an example fraud might be perpetrated on individuals, it may be perpetrated on companies by individuals or other organisations (licit as well as illicit) and the detection of fraud is often a rationale deployed by governments in relation to data collection on welfare services.

Within the communication there is recognition of the *potential* for PETs to be of benefit to data controllers and consumers. This is to be achieved through supplementing the effective implementation of existing data protection legislation and reducing the amount of personal data processed and collected which can be used to

21 Lyon (eds) "Surveillance as Social Sorting" (2003); Lyon "Surveillance Studies: An Overview" (2007)

22 See for example, Cavoukian "Biometric Encryption" Biometric Technology Today (2007)

23 "Communication on Promoting Data Protection by Privacy Enhancing Technologies" (May 2007)

identify individuals. The definition of what are PETs then becomes a critical one. The communication itself acknowledges that a number of definitions exist. Within the text of the communication PETs are defined (through reference to the PISA project) 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 […] PETs can help to design information and communication systems and services in a way that minimises the use and collection of personal data […]."[24]

The Communication finally sets out a number of objectives in relation to PETs

A. Support the development of PETs,
B. Support the use of PETs by data controllers
C. Encouraging the use of PETs by consumers.

These objectives are linked with the Communication's recommendations that PETs will ensure greater compliance with data protection directives. PETs can then be seen as a response to new technological developments. This is a recurring theme as the initial EU Data Protection Directive 95/46/EC was followed by further directives expressly responding to further developments in IT, e.g. the emergence of electronic communication. That such directives have not been able to deal with all of the perceived challenges to privacy arising out of recent technological developments provides the basis for understanding the emergence of privacy enhancement technologies as a policy paradigm within the EU. Guiding the directives are the principles put forward by the OECD in 1981.[25] These principles as adapted within the directives state that information must be collected with the consent of the individual for a specified purpose and it must be processed in a manner which is proportionate to the requirements of the purpose for which the data was collected. Finally in terms of data sharing it must be ensured that the data will be treated with the same protections under the directive within the country to which the data is transmitted to. Furthermore, directive 95/46/EC makes clear the distinction between data controller and data subject. It establishes a number of responsibilities for the data controller as well as guidelines for the collection of data from data subjects. The directive establishes the conditions under which data can be processed which are,

> (a) processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed, or
>
> (b) processing is necessary for compliance with a legal obligation to which the controller is subject, or
>
> (c) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or
>
> (d) the data subject has unambiguously given his or her consent, or
>
> (e) processing is necessary in order to protect the vital interests of the data subject.

The distinction between personal data and other data is likewise relevant to our discussion of PETs. Article 2 of the Data Protection Regulation states

---

24 "Communication on Promoting Data Protection by Privacy Enhancing Technologies" (May 2007)

25 "OECD, Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" (1981)

> 'personal data' shall mean any information relating to an identified or identifiable natural person hereinafter referred to as 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity'

It is in within regulatory frameworks that the implementations of PETs are perceived as having the greatest potential. Whether these provisions encapsulate privacy or the social contexts described in the introduction sufficiently enough to make them meaningful forms the discussion in the following section of this brief. The European Court of Human Rights has extended privacy rights into the workplace, the home or over beliefs, lifestyles etc.[26] The focus on *data protection* and informational privacy significantly frames and shapes the future contours and trajectory of technological development of PETs. Indeed, while private sector developments for commercial applications may be separate in some ways from public sector requirements, the recourse to the argument that PETs will enhance data protection is the same across both.

4. Privacy Enhancing Technologies: Approaches and Key Ethical Implications

In this section we examine approaches to the development and implementation of PETs. A clear issue to address is the question of how PETs relate to the communications' objectives and to? the view that PETs will complement data protection legislation. A further question concerns the ethical and social contexts and implications of PET implementations. The MetaGroup report for the Danish Ministry of Science, Technology and Innovation outlines three functions for PETs: achieving 'unobservability, unlinkability and anonymity'.[27] In addition, differences in who implements them (i.e. users , designers or automated,) as well as the settings in which they can be used (public areas, internet) make for a wide variety of PETs. For the purposes of this brief, however, we categorise two overall approaches to PETs. These are:

a) *PETs as a means of allowing pseudo or anonymous interactions,*

b) *PETs as data minimisation systems or devices.*

It should be apparent that these categories can overlap, in that arguably the most successful data minimisation would be where there are no personal data collected and the identity of the individual is protected.

PETs as a means of allowing pseudo or Anonymous Interactions

PETs as a means of achieving, guaranteeing or ensuring continuous anonymity where required are a key development trajectory for the technologies. While the principal focus of development at least in commercial settings has been on the Internet, numerous organisations have identified anonymity as a key desirable element in many forms of data collection, retention and processing. There are a number of example technologies, existing as well as in development which fall within this approach to PETs. Like the other two approaches and as described below within this particular category we would argue that there are a number of variations in typology in the way in which technologies can be implemented. Firstly they may be front-end deployments visible to the user or back-end deployments invisible to the user and embedded within the systems managed by the data controller. However, while the term used reflects a concern with helping

26 See also Council of Europe, Recommendation No. R(89)2 of the Committee of Ministers to Member States on the protection of personal data used for employment purposes (18 January 1989)

27 Danish Ministry of Science, Technology and Innovation "Privacy Enhancing Technologies" (February 2006)

individuals to be anonymous it is perhaps more accurate to think these systems or devices as allowing for pseudonymisation. As such this approach to PETs deals with databases or systems that are already perceived as being privacy threatening.[28] Such PETs then are often deployed in order to be corrections and enhancements where existing systems are seen as being relatively weak in terms of protecting data on individuals and their identities.

Digital Signatures and Blind Signatures

In the area of communication, digital signatures and blind signatures have been suggested as means of keeping identity and information private yet authenticating the source of communications.[29] These PETs allow for the transmission of information securely (such as for example emails) by encrypting information transmitted over the Internet, allowing only for the intended recipients to read them. These technologies are heavily dependent on and made possible through the use of encryption tools and technologies allowing information to be anonymous and to remain protected if it is intercepted before arriving at its intended recipients.[30] The technology also aims to protect information from being intercepted in the first place. It can be argued that digital signatures are a relatively established set of technologies and are often now incorporated as default into mainstream and publically available email programs offered on the market.

Indeed the first software to contain digital signatures was *Lotus Notes* released in 1990 building on theoretical work on encryption dating from the 1970s and expanded in the 1980s with the development of the RSA algorithm. Digital signatures make use of public key encryption, in that there is a private key known only to the sender and a public key used during the decryption process by the recipient. Blind signatures are an extension of this in that the 'signature' remains anonymous even on decryption and was first proposed and developed by David Chaum.[31] Recipients are still able to authenticate the fact then that there is a signature but are not able to identify the sender. Potential deployments of this latter implementation of the technology might include for example anonymous financial transactions on the web, with products or services delivered immediately to the individual. For example, I may wish to browse a particular site and there may be no need for this transaction to require personal identifiable data.

It is difficult in the first instance to see how these technologies might be problematic. As a relatively simple means of automating the process of protecting information and allowing anonymous transmission of information to genuine intended recipients the technologies here both excel and are for the most part generally unobtrusive and easily used. This is even so even if it is the case that the encryption systems used to generate signatures are relatively complex and not well understood by users of such systems. Yet there are perhaps a number of issues involved in their use. Perhaps the most obvious limitation is that the range of potential uses for them is quite low. Also such systems may allow for the emergence of more sophisticated forms of fraud. If the premise of the technologies is to be a replication in virtual terms of the traditional handwritten signature then there is always a potential (and numerous encryption systems have been demonstrated to be compromised) that illicit actors may gain access. Responses to this latter issue of course lead to the emergence of more sophisticated methods of encryption being proposed, yet this 'technological arms race' may point towards fundamental issues highlighting problems such as the 'design turn' we have discussed previously. As such, as with many of the PETs in this category, there is always a link to some data

28 See for example "Pseudonymisation Impact Assessment Study" NHS, UK (September 2005)

29 Chaum "Blind Signatures for Untraceable Payments" Advances in Cryptology (1983); Pointcheval & Stern "Security Arguments for Digital Signatures and Blind Signatures" Journal of Cryptology (2000)

30 See for example "Public Key Encryption and Digital Signature " White Paper by CGI Group Inc. (2004)

31 See for example, Bleumer's article "Chaum Blind Signature"(2004) for further elaboration of the blind signature scheme

which is personal, even if this is protected, allowing for the risk of this data being compromised remaining present.

Privacy by Proxy Measures

One development in terms of pseduonymisation has been the emergence of privacy by proxy measures which includes the idea of pseudo identities and domains.[32] Other more established technologies in this field include remailers along with web based proxy systems that allow users to surf online anonymously or communicate anonymously through email.[33] In the case of remailers a number of solutions have been offered by the private sector. These systems therefore extend the idea of digital signatures by allowing individuals to remain anonymous when communicating information. One of the more well known examples of this type of PET was the Freedom system developed by Zeroknowledge.[34] The premise of this sophisticated system was to provide subscribers with up to 5 pseudonyms that could be used in a variety of situations while accessing services on the Internet or as a means of sending email. The system would even allow for anonymous emails to be replied to in the same fashion as the blind signatures technology described above. One of the principal benefits that were extolled for this system was that the company itself could not match user pseudonyms with real identities. While the system was sophisticated and high profile in terms of its ability to protect identity and enhance privacy it was a commercial failure with the service being withdrawn on 22nd October 2001. Other examples of remailers include the Helsingus system which allowed for the sending of anonymous emails.[35] However this particular service was shut-down by the provider due to legal actions by the Church of Scientology when the identity of one of the users had to be revealed. Other examples of proxy technologies include those which supplement existing web-browsers such as *FoxyProxy* developed for the *Firefox* web-browser.

In summation, while these systems have definite privacy enhancing aspects all of them have failed to be commercially viable. This would suggest that there is no market for privacy enhancing technologies in this regards where users must pay for such systems. As one commentator has noted it remains at best a niche market where much of the provision is by resource limited grass-roots providers as the proxy element of the technology means routing traffic through one or more dedicated servers that strip away personal data. This we feel has important ramifications for PETs in general and the manner they are approached in terms of their implementation and deployment in that this particular type of service does not appear to feature prominently in the mind-sets of many consumers. Similarly there are concerns over such systems being hijacked for illicit purposes. The ability to send emails which are anonymous and untraceable could potentially be used to harass individuals, be damaging in terms of controlling spam or also conceivably allow for identity theft to be perpetrated on individuals. We note some of these problems also in our discussion on FreeNet.

Other implementations focus on the generation of pseudo-identities or an *Identity Protector*.[36] This element of a system would control the revealing of the identity of the individual, generate pseudo-identities and authenticate these pseudo-identities for various domains and services within an information system. These are systems then where users can be assigned a pseudo-identity which does not reveal personal information but allows them to continue to access particular services within particular domains although the potential remains for some link to be made to the actual identity of the person to be made. Such systems then aim to

32 Hitchens "Secure Identity Management for Pseudo-Anonymous Service Access" (2005)

33 Seničar et al. "Privacy-Enhancing Technologies – approaches and development" Computer Standards & Interfaces (May 2003)

34 Edwards "Zero-Knowledge Systems Introduces Security and Privacy Tool Suite" WinInfo (January 2002)

35 Mostyn "The Need for Regulating Anonymous Remailers" International Review of Law, Computers & Technology (March 2000)

36 Hes and Borking, 2001:7

ensure that barriers are set up between users and service providers, or even indeed between different actors within the same organisation where the actual identity of the person need not be known in terms of using the service. Sometimes these systems rely on a trusted third party which does not communicate any personal information to the service provider but guarantees the proxy identity of the user for the service provider. Technologies here may also aim at levels of data separation. Considerations in documents advocating this approach generally seek to establish whether the system is to be 'identity rich', i.e. knowing the identity of the individual is essential for its use. Systems then are also examined to see whether identity is only necessary for certain elements of the system, i.e. for particular services data may be separated from identity or if there is data sharing then identifiable information may be stripped away.

An example of such services includes the provision of pseudo-domains when consumers make use of particular services online. As such at the point of connection the identity of the individual may need to be known but subsequent to this initial connection the use of pseudo-domains can be made stripping away personal data. Similarly a potentially important use of the notion of pseudo-domains would be in public sector deployments. Where governments make arguments about the use of inter-operable databases it could be established that identity may not be a necessary pre-requisite of sharing personally identifiable data in many circumstances.

Cookie Blockers or Cutters

In the course of surfing Internet websites it is well documented that such traffic is often engaged in continuous recording of users habits in terms of sites visited. Indeed new developments such as the Phorm system deployed by BT focus on tailoring marketing information and advertisements based on past surfing habits of consumers. Such interventions can be seen as highly invasive in terms of privacy even if such data is not directly personal as it clearly leads those with access to data to engage in profiling activities based on consumer habits while online. Cookies refer in the most basic sense to information being recorded by websites as to surfing or interactions individuals have with particular websites. These may simply be indications as to the pages on a website most frequently visited by an individual when using a website to more sophisticated profiling information based on a user's web browsing habits during an extended period of time while using the Internet. Cookies are extensive and pervasive and have often been at the centre of grassroots controversy considering the amount of data that is generated, collected and stored as a result of the use of Cookies.[37]

This controversy has been so sustained that there are a number of free standing tools available to block cookies and indeed most mass commercially available web-browser software, such as Internet Explorer, Firefox and Opera contain settings that allow for users to restrict or even block cookies being transmitted to websites during their browsing experience. The controversy over cookies has not been restricted solely to user groups. Both the US and the EU have explicitly regulated on the topic of cookies as well.[38] In the case of the EU Directive 2002/58/EC sets out rules for cookies in Article 5 which suggests that their purpose must be clearly communicated to the user and the user has the choice to block the operation itself. Exempted however are those procedures and operations which are necessary for the technical aspects of operation. This aspect of the directive has been inconsistent or non-existent in terms of enforcement throughout the EU.

Cookies demonstrate some of the wider problems with PETs and the concerns over their implementation. In this sense while amongst those who may be technologically 'savvy' there is a high degree of knowledge and in most instances a low level of tolerance for what is continuous surveillance and profiling of them by

37 Eichelberger "The Cookie Controversy" (1997); Robulack "Cookies – the end of privacy?" Net.Words (1996)

38 King "On-line privacy in Europe – new regulation for cookies" Information & Communications Technology Law (October 2003)

websites amongst those who are not technologically 'savvy' there is little empirical evidence to suggest that these same concerns are shared. However while cookies are perceived to be problematic one argument that could be made that it is not so much the technology itself but rather the purposes they are put to and the adaptations that service providers make that are the problematic aspects. Cookies for example can be designed to be anonymous as well as temporary that could for example see their design as a type of PET which could be linked with other forms of PETs described here.

FreeNet

Approaches to anonymisation may be characterised as 'soft' approaches such as those detailed above or 'hard' approaches, such as FreeNet.[39] Soft approaches require the identity of the person to be known at some point, although personally identifiable data is then stripped away. In the example of a trusted verifier, it is this actor which knows the identity. In the case of pseudo-identities or pseudo-domains it may be the automated log-on systems of the ISP or data controller which verify the initial identity of the person concerned. FreeNet is however a hard approach.

FreeNet is an anonymous web where information can be uploaded, stored and distributed without any identifiable information available as to its source. It is a distributed peer-to-peer based system, in that there is no centralised database to the system but rather information is shared throughout the network with participants unaware as to which information, or parts of information is stored at any one time on their systems. What this means is that FreeNet is completely anonymous, in the sense that there is no identifiable author of a document, there is no way of knowing where a document is located or where it originated from, but there is also crucially no way for participants in FreeNet to determine what files are locally located on their own computers. FreeNet is focused on guaranteeing freedom of speech and expression but its hard approach to privacy brings with it its own set of problems. For example there are no means of removing documents on the part of user and it may be the case that racist, radical or otherwise illegal as well as individually offensive files might be stored on individuals' computers without their knowledge. There is no way to trace the origins or creators of files. While the system is anonymous we can ask is it too anonymous, free speech arguably carries with it a certain set of responsibilities and indeed these responsibilities are regulated within various member states, such as for example holocaust denial in Germany and Austria. FreeNet's aversion to any form of censorship might be imbalanced in terms of rights as opposed to responsibilities for free speech, privacy and a right to be left alone.

The issue of trust is critical we would argue in the implementation of these forms of PETs. We are immediately faced with the problem of how these technologies would be adopted outside of commercial settings. Security discourses pervade many aspects of data collection by the state, for example in welfare databases to combat fraud, and the need in many instances in the use of personal detection technologies to identify 'trustworthy' persons would seem to stand in contradiction to the approach characterised by these types of PETs.[40] Linked to this is the lack of trust between individuals themselves where pseudo-identities may provide opportunities for fraud or make the detection of identity theft difficult to accomplish. Here we again return to the important concept of transparency as well as communication, in terms of informing citizens, as well as data controllers, on how PETs are to operate or be deployed in such contexts. As such linked with trust and perhaps an area where trust will be dependent on the role of PETs will be a role where the technologies either visibly or invisibly protect individuals' data that has been stored, processed and

39 The Free Network Project – http://freenetproject.org/

40 Robinson, Vogt and Wagealla 'Privacy, Security and Trust within the Context of Pervasive Computing' (2006)

collected.[41] Here the function of PETs will be in protecting citizen's rights either with or without their active participation in such a process.

There is a further danger that PETs as a means of allowing anonymous interactions might indeed even serve to threaten data protection. The directives make clear that they apply only to personal data, these forms of PETs are aimed at eliminating all personal data yet it is readily apparent that data is still generated in many instances. For example in relation to cookie cutters there been responses from illicit actors as well as organisational actors to circumvent the blocking functions of cookie cutters. In the first instance the fact that PETs such as these might provide a veneer of acceptability for data, i.e. in the sense that there is the perception that the technology has done its job correctly could have important ramifications in terms of how data might be reused for purposes other than which it was first collected for. In the second instance there is a danger of a technological arms race, in that the more we aim to have devices that ensure anonymity the more there is a drive towards technologies designed to reveal that identity. PETs where anonymity can occur through user choice is another key implementation within this approach as we have seen from our examples on privacy by proxy measures. What is clear here though is the degree to which systems are utilised by consumers having to pay for them. Such systems have also been referred to as being privacy management systems yet we would stress that an important defining feature of this strand of PET implementation is the level of controls given to users.[42] Such systems need not necessarily be overly concerned with data either, a relatively simple yet effective PET in this regard may be seen in the User Access Control feature of Microsoft's Vista Operating system which provides user centric protection against viruses, phishing attacks from fraudulent websites as well as highlighting other potential damaging actions a user might take which would compromise their PC.

PETs as Data Minimisation Systems or Devices

The category of PETs we have described as anonymous or pseudo-anonymous can be characterised for the most part as add-on systems that are designed to rectify flaws already present within data collection and processing systems. We have also examined the case of a 'true' anonymous system such as FreeNet and highlighted some of the potential ethical and social issues associated with it. Some commentators have described the process of PETs as the 'path to anonymity' and as a result this category of PET can be seen as the articulation of many in the field that the design and technology of PETs should be incorporated into systems from their inception. This would in turn represent a more viable path to anonymity rather than attempting to retrofit existing systems that have inherent flaws and deficits in terms of data protection. As mentioned the most successful implementation of data minimisation would be for all personal data to be removed from systems but achieving this in the face of the existing design problems inherent in many information systems may prove too difficult, expensive and may not as we have seen be technologies that generate much commercial interest once released on the market.[43]

Data minimisation approaches are often implementations of sets of technologies or refer to systems which are configured reflecting certain guidelines and principles.[44] Data minimisation may also not just be focused on the database but is increasingly being seen as a way of configuring and implementing personal detection

41 For an elaboration of the relationship between trust and risk in contemporary networked socities, see for example Bekkers & Thaens "Interconnected networks and the governance of risk and trust" Information Polity (2005)

42 Hansen "User-controlled identity management: the key to the future of privacy?" International Journal of Intellectual Property Management, 2008. See also Feigenbaum et al. on the notion of "privacy engineering" (Feigenbaum et al. "Privacy Engineering for Digital Rights Management Systems" (2002))

43 Wright "Privacy, trust and policy-making: Challenges and responses" Computer Law and Security Review, 2009

44 Rundle et al. "At a Crossroads: 'Personhood' and Digital Identity in the Information Society" STI Working Paper, OECD (February 2008)

technologies themselves. In the sense that data collected is at the point of origin minimised in such a way that what is stored reduces threats to privacy. For the majority of examples this approach centres on decisions made by data controllers dealing with the design and implementation of their systems. A linked implementation within this category is though the notion of privacy management systems which are under the direct control of individuals themselves.

Data minimisation may importantly be technologies which may be deployed impacting on data retention and the shelf life of data, which it is argued would significantly impact on a major concern expressed over function creep by removing or destroying data after a set period of time.[45] Other approaches may be combinations between pseudo-anonymous techniques such as data separation but taking this to further levels in terms of negating the amount of personally identifiable data collected from individuals in the first place. The difference here between data separation discussed previously is that there is an implicit assumption that in data separation personal identifiable data has already been collected and stored. Data minimisation approaches proceed from the question what is the absolute minimum of information that needs to be collected and stored. Arguably many biometric technologies have a level of data minimisation already built into them, at least in the instance of first generation systems as to save on costs and increase time required to process images templates are used in lieu of a full record. Where most such systems continue to be privacy intrusive however is the association of such data with more substantive data bases containing personal identifiable data. These systems may also be focused on the question of who has access to such information.

As we have noted in the previous sections of the brief there are clearly perceived limitations to the use of PETs within that might be called security or homeland security related settings. This is especially so where the need to establish who trustworthy individuals are seen as paramount goals for the operation of such systems. However this approach to PETs as we shall aim to attempt to demonstrate from our examples may be an area where PETs could be reasonably deployed without impacting on the mission functions associated with security related deployments. As described in the preceding section much of the PETs that fall into this category may reasonably be termed as ‘soft’ approaches to anonymity. In this sense the identity of the person is arguably always somewhere within the system, whether this is within the databases of the trusted entity, or within the log in computers of the ISP or the data controller responsible for the system. Similarly PETs within this category which seek to de-link data and information where these strip away elements of personal data presuppose or may always lead to the situation of the data being re-linked somewhere in the system in order to identify the person involved. In the case of data minimisation systems and devices it is arguable that this danger does not exist to the same degree as from the very outset the amount of personal data which is collected is limited. This is not to say that the risk is not present, merely that the opportunities for the risk to manifest are limited by the amounts of data which are included. Data minimisation systems and devices may conceivably then be one the principal application of PETs to be considered in public settings and contexts.

Logical Access Controls

Ensuring the security of data is arguably not only about what occurs to such data in terms of its collection and processing but also is importantly centred on who has access to data on individuals. In part many of the more substantial data losses that have occurred in the UK and elsewhere have been from unauthorised access or access to data not being conducted in the proper way. In this sense access to data in the physical sense (although remote access is also a concern) may be a very fundamental PET to consider in terms of its being deployed as a relatively simple yet effective set of protections for data. Increasingly controls over access are

45 De Hert “Identity management of e-ID, privacy and security in Europe” Information Security Technical Report (May 2008); De Hert et al. “Legal Safeguards for Privacy and Data Protection in Ambient Intelligence” Communications of the ACM (1988)

being tied to biometrics devices.[46] In this sense this approach reflects a data minimisation approach by basically restricting access to data to as people as possible. In sensitive public sector deployments such as hospitals this form of PET should be seen as a critical mission.

Similarly access control is an issue for individuals themselves. Information commissioners, such as those in the UK, have increasingly called for means to be made available to individuals to access all data held on them by public and private organisations in as easy a manner as possible.[47] While the goal of being able to review one's data is laudable, given the risks outlined above in terms of individuals not valuing their own data and its protection highly enough a strong means of authentication to access these databases by individuals concerned would be a key requirement. This particular implementation of PETs is less about the development of new technologies that might be characterised as being privacy enhancing but rather about using oftentimes what might be labelled as privacy intrusive technologies in a manner to enhance the privacy and protect the data of individuals. As such this approach should be seen as being integral to a privacy management system, with controls to be in place for both users and data controllers. It is worth noting that securing the access to data remains a high priority for member states across the EU with greatly differing degrees of success. Recent incidents in the UK highlight the paucity of current systems in some respects lending credence to the argument that individuals should be given more direct controls over access to their data.

Biometric Encryption

Perhaps one of the more interesting potential PETs is the use of biometric encryption systems. While biometrics are often portrayed as being of immense use in terms of offering secure means of identifying and authenticating people there are fears expressed at the same time as to their more privacy threatening features, especially where these are linked with surveillance deployments. This application corresponds closely to the methods suggested by the Ann Cavoukian in her emphasis on the notion of biometric encryption as a key method of ensuring privacy.[48] In this application of a PET whereas biometrics themselves have been associated with being particular privacy threatening they are turned into a type of system which provide strong sources of protection of privacy.[49] The manner in which this operates is that biometrics as unique identifiers are meant to provide secure identification, if systems are designed to utilise biometrics as a principal source of identification, and such templates generated by biometric devices are encrypted then the need to collect data can eventually become redundant as the biometric of the individual is enough to avail themselves of a particular service. In this sense the very reason for biometric technologies being popular amongst service providers and data controllers, due to the secure and reliable nature of identification and authentication they offer, becomes a key strength in them being deployed as a PET or within PET systems.

The proponents of this system highlight how biometric encryption can allow also for a positive-sum game of making identification systems more privacy friendly without sacrificing security. In essence a part of the argument for the deployment of this system is the limitations in the 'trust model' or believing that in the face of commercial as well as national interest pressures that privacy will be protected considering the masses of data now collected on individuals. While biometric encryption might include a number of approaches and technologies (as the field is quite new) the basic premise builds on the encryption systems described previously in this brief such as digital signatures. For most PKI infrastructures, such as 128-bit encryption,

46 Manning "Using biometric measures for access control is an increasingly viable security solution" (2008)

47 Importantly, the Britisk Data Protection Act of 1998 gives individual citizens a right of access to the personal data which organizations hold about them, subject to certain exemptions.

48 Cavoukian "Biometric Encryption" (2007)

49 "Template-Free Biometric Encryption for Data Integrity Assurance" Department of Electronics, Univeristy of Kent (2005-2008)

the length of the key is for most individuals impossible to remember. The generation of the key is then tied to a much simpler input system such as a pin or password which is translated into this longer key. An example here would be the encryption systems used for wireless connections where a user enters a password which corresponds to an encrypted key. Such systems are though vulnerable to the recurrent issue of compromised, lost and improper use of passwords by non-authorised users.[50]

In a biometric encryption system however this pin or password which is an alpha-numeric input by the individual is replaced by a key which is derived from a biometric provided by the user and encoded as a template. The benefits of such a system are numerous. Firstly tying particular domains of information to a biometrically derived key would mean that illicit actors would have to target the biometric of individuals in order to derive specific keys keyed to particular databases exponentially increasing the logistical aspects of compromising individual passwords. As the biometric of an individual is immediately translated into a template and from that into a key a major concern with personal data in terms of it being biometric data being stored is immediately removed. Paradoxically – yet perhaps obviously – the use of biometrics as a form of securing data is an intensely personal usage (although there are examples of technological 'spoofing' technologies designed to circumvent this aspect) in that a user provides their biometric generally when they wish to. Such a focus, one which is one centred on user control, would for proponents of this system enhance trust and confidence in the system by its emphasis on user control over the provision of biometrics to ensure encrypted access to services and data stored on them within data controller systems.

One example of a technological device following this system and one which claims to boost both the security and the privacy by utilising a biometric data system is Phillips' recently developed '*PrivID'*. By encrypting the user's biometric this technological device protects the individual's privacy in the sense that if the data should be lost no one will be able to use the 'original' biometric; the encrypted version can be cancelled and a new encrypted version can be made. In that way the user's privacy is protected from the risk that data loss could lead to identity theft and moreover it allows the individual to renew his/her biometric identifier and in that way still be able to use and legitimately gain access to a given security system and/or a specific site.[51] The benefits of this system are that at the point of data collection encryption occurs that means other than a verification of an encrypted template no data is retained. One example of a potential deployment here is within airports, where the system could be used as boarding cards. In this instance the identity of the person has been verified but there is no need to store further data on them by trusting the biometric template encrypted on the boarding card.

Privacy By Design

One approach to privacy enhancing technologies is to understand it as a form of system design. This approach is, for example, captured in the notion of 'Privacy by Design' which (as used by the UK Information Commissioner) refers to the principle of data minimization as a crucial principle upon which a given data system is built and – in turn – as a privacy enhancing technology in the sense that by minimizing the data being collected and stored, this principle would at the same time serve to minimize the risk that any sensitive, personal data could be lost.[52] Other examples of design principles that could function as PETs are the notion that citizens' personal data must be fairly and lawfully processed and the principle that no data should be transferred to countries without adequate protection.[53]

50 Adler "Vulnerabilities in biometric encryption systems" School of IT and Engineering, University of Ottawa, Ontario, Canada (2005)

51 There are other examples of PETs understood as devices many of which are based on cryptography but other technological devices have also been developed with the aim of giving the user greater control over his / her biometric data an example of which is credential wallets.

52 See presentation by the Information Commissioner http://www.ico.gov.uk/upload/documents/pdb_report_html/index.html

53 See also Duncan "Privacy By Design"

As such this method reflects directly the principles of data minimisation as a PET itself. By applying such principles it is to be expected that the amount of personal data collected on individuals will be relatively minimal. The benefits of such an approach are immediately visible in that it is clear that the less data collected on individuals the less of a risk there are some breaches to data protection will occur as a result. The guidelines are issued as being relevant for both public and private sector deployments. As an example of how this approach could be implemented in the case of certain deployments on the part of retailers there would appear to be no reason for store loyalty cards to retain addresses or to be attached even to the individual using them, unless the company is engaged in some profiling activity related to marketing.

The critical issue in this approach to PETs is whether there will be a change in approach on the part of data controllers whether they are public or private. In many ways there is an argument based on our initial discussions that the very fact that the surveillance society requires some data collection in order to operate efficiently encourages data controllers into thinking that the more data they can collect the better they can market and sell products or the better they can deliver certain governmental or state based services. Therefore such systems will depend on decisions by data controllers, although they may be subject to agitations for change on the part of consumers and citizens. This approach may require a democratisation of surveillance and data collection procedures in the sense of controls being devolved to users, but in a pragmatic sense, given the concerns outlined in the introduction to this brief, it may be that there are definite oppositions to such trends by wide ranging and diverse groups of data controllers.

P3P

Another example of this form of PET is represented by the Platform for Privacy Preferences. This is a PET which combines front-end user directed inputs with back-end uniformly agreed upon standards and procedures. As such it may be characterised as privacy through informed consent in that individuals are expected to make choices and be aware of the ramifications of these choices. The system as such provides end-users with a series of questions or statements whose answers are compared against the provisions in place on web-sites, databases or provided services. It also provides a common report from websites using the systems as to which particular privacy policies they have implemented in their procedures. As such it allows users then to decide whether to continue using a particular service or site when they are informed as to the degree of data protection which is provided. We would argue that these types of PETs, i.e. user driven will come to the fore in terms of being deployed within commercial settings. As of yet their use within public settings is limited considering it is the choice of data controllers whether or not to implement them. However even in the case of P3P as we discuss there are limitations placed on the ‘choices’ of consumers to avail themselves from these forms of PETs. The common characteristic of these technologies is to seek methods of empowering consumers in the face of the numerous places, devices and activities where data is recorded and stored on them. The use of PETs as an empowerment for protections on the processing of such data is a critical mission yet choice is often an illusory feature. In the example of P3P the system is voluntary on the part of organisations and while some browsers are enabled for P3P it is unclear the degree to which P3P is utilised by consumers across the EU.

Furthermore in addition to the voluntary nature of adoption P3P the system itself runs into the problem of service exclusivity in terms of provision. What is meant by this is that I may wish to read the Financial Times, there are no other sources for this information and if the FT website does not make use of P3P then the illusion of choice of utilising P3P is readily apparent as unless I access this non-compliant service then I do not benefit from the protections afforded by P3P. Moves away from Net Neutrality (or the idea that content delivered on the internet should be for free for everyone) will perhaps further erode the potentials of

choice for consumers as in tandem with ISPs users of the internet will be locked into specific sets and types of content providers operating with ISPs. There are a number of potential responses though that could be conceived as dealing with these problems, the first of these is to make P3P or a system like it statutory as opposed to voluntary. This however raises the spectre of who decides what options to allow and what are the exemptions (such as matters of national interest or security). It would also mean regulating and enforcing levels of privacy for individuals, in that there is always a baseline assumption of the required privacy, would the state then be protecting us from ourselves in guaranteeing our privacy even in private commercial settings.

While P3P is a transparent application of PETs, and is to be commended for this, transparency in terms of resolving the issues attached with regulating it and other choice enablers may be a more difficult ideal to meet. Similarly allowing consumers choices does not necessarily mean they like having to make these choices. For example while the Vista UAC measure is designed to protect the computing experience of users, it is consistently cited as one of the most annoying and intrusive measures in Vista. This level of annoyance was indeed lampooned by Microsoft's rivals Apple in a series of advertisements which featured prominently in Apple's marketing of its own new operating system. Similarly the use of cookie cutters as a choice or indeed configurable firewalls (i.e. where the user is allowed to set the level of protection), especially where these are embedded within browsers are a feature which most users never avail themselves of, or certainly do not look to alter or change in terms of the level of protection from the default settings set by the technology provider. As such while PET implementations like these can be said to increase the autonomy of individuals in terms of them making decisions there are issues over whether individuals wish to actually make such decisions and the degree to which such decisions are actually informed decisions. This observation holds true not only for PETs but indeed data protection regulations and individuals' own approaches to privacy itself.

5. Conclusions

This brief has attempted to synthesise some of the key issues and technologies that have informed the first focus group on PETs carried out by the HIDE project.

The main **preliminary remarks** outlined in this working document are:

- the deep tension between, on the one hand, the fact that modern societies are considered to be "surveillance" societies (in that they need to collect personal and organizational data to operate efficiently), the increased tolerance of surveillance and detection to ensure security; and, on the other hand, increased public awareness and concern over the use of security technologies and the collection of data, and the need to balance interests of ensuring security and the ideals of liberty and privacy;
- the difficulty in outlining a universal definition of "privacy", since the notion of personal/public space is subject to revisions as a result of technological and social developments: with the increasing development of ICT, the expansion of cyberspace, and the international data sharing, guaranteeing privacy whichever definition is used in regulation may become an increasingly difficult challenge;.
- Considering the above, PETs could represent an important means of ensuring and enhancing particular rights of citizens, and serve as an example where privacy and security might coexist in a "positive sum" fashion.

The brief has analyzed the **legal context**, framed by the EC "Communication on Promoting Data Protection by Privacy Enhancing Technologies" (May 2007), and international and European data protection legislation (OECD Guidelines and EU Directive 95/46/EC). Due to the early stage of their conceptualization, and with the dynamic landscape of ICT, a variety of definitions of PETs is found in the literature, and it is reasonable to assume that these might further change over time: it is crucial to study and reflect on how these definitions may interact with the legal framework described above.

The document has examined **two different technical approaches**, and the main ethical and social implications that might arise from the development and deployment of technologies within each approach:

- **1st approach: PETs as a means of allowing pseudo or anonymous interactions**
  In relation to this group of PETs, the critical issues are: the lack of trust given the anonymity of the interactive subjects, the possible exclusionary nature due to technological complexity, the possible threat related to data protection (data is still generated in many instances and reused for other purposes; another issue is the so called "technological arms race"), and the level of control given to final users.
- **2nd approach: PETs as a data minimization systems or devices**
  PETs within this category may be deployed without impacting on security related deployments, the amount of personal data collected on individuals is minimal, with consequently less risks, the emphasis on user control enhances trust and confidence in the system; however, their deployment strongly depends on decisions taken by data controllers dealing with the design and implementation of their systems.

With regards to the **EC Communication on PETs**, the work of the Focus Group will be to analyze and discuss the general approach towards these technologies and the three objectives laid down in the EC document, to be achieved by a number of specific actions. Crucial issues to be addressed here seem to be:

- **EC general approach towards PETs**: the Commission considers that PETs, applied according to the existing regulatory framework, would "enhance the level of privacy and data protection in the Community". It is however crucial to think if the sole "technical approach" of the document is sufficient, or if it may be important to develop and add other general criteria (for instance, ethical and social implications);
- **1st objective - to support the development of PETs**: should this objective include also an action devoted to the description of some general rules related to PETs management?
- **2nd objective – to support the use of available PETs by data controllers**, **action 4.2.2** (**ensuring respect of standards in the protection of personal data through PETs**): is the described strategy of standardization adequate, or may it be necessary to address also less technical and more "ethical" standards (considering the nature of the "privacy" concept, that might differentiate greatly from individual to individual)?;
- **3rd objective – to encourage consumers to use PETs**: is this consumer-oriented approach, based on individual decisions/possibilities, correct? Or may it be important to consider a "hard" approach, involving States in the process of guaranteeing the wider use of PETs?

The agenda for the next focus groups will be to refine this document and to explore in more detail some of the questions raised by this brief within the framework of considering the objectives of the Communication on supporting the development, implementation and adoption of PETs across the EU. How this can be achieved and what are the key challenges in meeting such an objective?