PETS 2nd Focus Group meeting report

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

Cesagen 2nd Focus Group on Privacy Enhancing Technologies

Introduction

One of Cesagen's allocated tasks within the HIDE project is to lead a workgroup exploring the ethical impacts of Privacy Enhancing Technologies (PETs). As part of the activities comprising the work of the project in this area Cesagen will organise and host three focus groups with participants from government, NGOs, industry, the public and academia. The second of these focus group workshops was held in London, UK on the 16th October, 2009. The final deliverable of the focus groups will be the delivery of an Ethical Brief on Privacy Enhancing Technologies.

An intermediate version of the Ethical Brief on Privacy Enhancing Technologies was produced by Cesagen in 2009. This was circulated prior to the focus group to participants and formed the immediate backdrop for the planned discussions of the focus group.

The ethical brief identified and suggested that there are **two different technical approaches**, and explored 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.

An aim of the focus group was to discuss the validity of categorising approaches to PETs in this manner, whether it may be refined or altered, as well as adding to, if necessary, and exploring the ethical and social issues that have been identified with each approach and specific implementations highlighted in the ethical brief as examples.

Participants were encouraged to ground their discussions in relation to the following key issues for the focus group

1. Consider the definition employed in the ethical brief with respect of technological approaches to the implementation of PETs. Can this be refined? Is it suitable? What are further examples of specific

PETs that may fit into the framework? Are there specific technological examples that prove to be exception to the categories outlined? What other relevant technological examples exemplify issues, approaches and reflect the objectives of the European Commission?

2. How do these approaches, and examples of each, interact with the position and objectives set out by the European Commission in its Communication on PETs?

3. How do these technological implementations and the objectives of the European Commission in respect of PETs interact with the key social and ethical issues identified in the ethical brief? Are there additional concerns to be included, how can the existing ones be further refined and clarified in relation to technological implementations, the legal context in the EU and the objectives set out for PETs within the European Commission's Communication on PETs.

Framing the entire focus group, and framing the work of Cesagen in this area are 3 objectives set out by the European Commission in a Communication on PETs (May 2007). These 3 objectives are 1. Support the development of PETs, 2. Encourage the use of PETs by data controllers and 3. Encourage the use of PETs by consumers. The second focus group was divided into two sessions, a morning session which was a more traditional speaker/presentation/question format where the aim was to provide sufficient information on the background and context of PETs and the social and ethical issues involved. Following this the afternoon session was a focus group discussion moderated by Prof. Juliet Lodge.

The focus group consisted of,

Michiel van der Veen (Philips, General Manager priv-ID Biometrics), Prof. Juliet Lodge (University of Leeds), Prof. Emilio Mordini (CSSC), Sonia Massari (CSSC), Dr. Paul McCarthy (Cesagen), Katja Jacobsen (Cesagen), Dr. Antoinette Rouvroy (CRID) and Dr. Maria Veloso (Centre for Biomedical Law), Mr Pete Bramhall (Hewlett Packard), Dr. Sotiris Ioannidis, Vlad Niculescu (Zuyd University), Mary Collins (IBG) and Ms. Laureene Neeves (Cesagen).

The three invited speakers for the focus group were Mr. Pete Bramhall, Mr. Michiel Van der Veen and Dr. Sotiris Ioannidis.

Presentations Session

Mr Pete Bramhall:

Mr. Bramhall's presentation synthesised a number of important themes. He began by highlighting, specifically in the case of the UK, but with relevance to other European countries, the growing assumption that individuals are more concerned about issues related to privacy. However he qualified this by suggesting that threats or damages to privacy led to complex redress procedures and complex methods of protecting individual privacy. This led he indicated to people not engaging with mechanisms allowing or aiding in the protection of their

privacy to any substantial degree. Furthermore he detailed the findings of TrustGuide which suggested that there were high levels of mistrust from people in ICT applications and systems.

There was an acknowledgement of particular threats by respondents but these were conceptualised as 'risks' with the onus on guarantees being provided by banks, governments and other providers in securing data and protecting the privacy of end users. A critical component of this being was seen as allowing for more control and transparency. Mr. Bramhall contrasted these views with the manner in which privacy is regarded by enterprises and governments. He suggested that they were partially concerned, where such issues impacted on economic efficiency, some differentiation by being seen to be doing 'the right thing' with the majority taking the lowest-cost approach to ensuring legal compliance. Mr. Bramhall then suggested a definition of Privacy, ranging from privacy, which could be seen as a fundamental right, to data protection as principles and Infosecurity which would be mechanisms, such as PETs.

He suggested that informational self-determination was an important goal, but that total privacy was in fact secrecy and would as a result not be helpful for relationships, i.e. the using of particular services. Mr. Bramhall the outlined a potential categorisation of PETs that saw them ranging along a spectrum. These ranged from direct control, with weak trust through to indirect control with strong trust levels in systems. An example of the weak-trust scenario was given in the case of the PRIME project. Here the focus is on end-to-end individual control over data, who it is released to, who can access it, anonymising certain transactions and providing tools so the user can trace and identify organisations etc that are accessing their data. Mr Bramhall also discussed Identity 2.0 systems or user centric identity management as another trend in this area. In the case of strong trust situations the focus is on solutions that begin at the top of an organisation and finish at the top, these were suggested as being best practices, guidelines, decision support tools etc that were embedded within the systems and mechanisms of organisations.

Two examples of work by HP in this area were given, the Accountability Model Tool and Policy Driven Automated Data Management. Both of these systems allow for real-time monitoring of data and automated decision making and support for dealing with issues of data protection. Policies for instance are derived from law, organisational procedures, data protection legislation and embedded with a rules based system aiding real-time decision making. Mr. Bramhall concluded by suggesting that current PET research is focused on delivering solutions along the entire range of the spectrum. He highlighted a number of ongoing projects and activities such as EnCoRe, MASTER, PICOS, PRIMELIFE and the W3C Policy Language Interest Group as representing these trends in research. He concluded by suggesting that PETs were ready for deployment out of the lab but highlighted that confusion still remained due to complex issues and that dialog between scientists, regulators, business, publics and social scientists would be essential for their successful implementation and uptake.

Michiel van der Veen:

Mr. Michele van der Veen gave a presentation entitled “Protecting fundamental privacy rights in commercial biometric deployments”. In this presentation he argued that biometric deployments are rapidly finding their way into commercial applications – as evidenced by a number of examples including biometric access control,

biometric payments and biometric health-ID solutions. For Mr. Van der Veen, the important point about this development is that although the commercial benefits are often straightforward, fundamental privacy rights are increasingly ‘at risk’ as a result of how biometrics is used in some of these commercial applications. This is the case in applications where personally identitfiable information is required to perform the biometric identity check.

Mr. Van der Veen then stressed that if this personal biometric information is compromised, it is crucial to understand that it is then compromised forever and thus potentially jeopardizing future biometric deployments. In other words, once a biometric is compromised, it is compromised forever. This he suggested was one of the critical concerns expressed in discussions on wider scale deployments of biometric solutions and one that the industry and providers in various ways were attempting to address. For example one method of reducing the vulnerability of biometric based systems was through the increasing use of multi-modal biometric solutions.

However, the vulnerability, Mr. Van der Veen argued, can be overcome in another potentially viable manner as well. For his presentation he demonstrated how biometrics can be deployed in what he referred to as “a positive sum manner” – that is, in a way that protect the human privacy rights while still benefiting from the advantages of biometric based identification systems. This is the main objective that priv-ID’s revocable biometric technology enables. Mr. Van der Veen then proceeded to outline how this system would operate.

Mr. Van der Veen highlighted how PrivID was making use of a system proposed by the Ontario Information Commissioner Dr. Ann Cavoukian. This is a system where the use of biometrics is done in a fashion where a random key is generated each time a biometric is given. As such rather than for example traditional 'pin' methods, where users must remember alpha-numeric passwords these passwords are replaced by biometric based encryptions. However in this type of system it is not the biometric itself which is retained but rather the encrypted template that acts as a pin or password to grant access to systems or services. The strength of such a system he stated was that for example even if the encrypted template was compromised it could be revoked and another encrypted template generated by the end-user providing his or her biometric again. This as such would allow for revocable identities.

Mr. Van der Veen then outlined an example of where this type of technology is being deployed and trialed by PrivID. He discussed how the company had developed a portable health information card utilizing biometric encryption in Africa. This system was seen as a particularly strong case for deployment in that end-users had full control over when and to whom their health information would be disclosed to. The use of biometric encryption in accessing the data also strengthened privacy due to the advantages of the system as described above.

Dr. Sotiris Ioannidis:

Dr. Ioannidis' presentation was entitled 'Privacy as a System Service'. He began by referring to research conducted within his institution illustrating the exponential growth in data readily available to anyone utilising

standard internet search engines. These included word documents, pdf's, powerpoint presentations and excel files.

Dr. Ioannidis then illustrated one of the critical issues involved in this number of files being available online in that a high proportion of the files contained metadata from which personal data and information could be extracted from. Metadata refers to saved data in files such as the names of the people who edited the document the name of the company as well as other miscellaneous but potentially damaging or valuable personal information and data. He emphasised the ease through which this information could be collected requiring only a basic level of IT expertise.

Following from this example Dr. Ioannidis then illustrated a similar example of how personal data could be extracted by referring to a number of experiments he conducted in relation to the Greek Social Security Number website. The number is a universal one issued to all Greek nationals. A website can be utilised whereby details of individuals and their SSN can be accessed by individuals themselves. By searching for data (such as for example the addresses of individuals, their date of birth etc) he was able to acquire their SSN and other useful data in a number of cases. Likewise the experiment involved testing the security of the site yet he found that through these second level attacks in the case of private individuals the SSN could be retrieved for 75.1% of them.

Dr. Ioannidis as such stated that this illustrated a fundamental issue in that privacy is an afterthought in terms of the design of many systems. But he suggested that the same was through for many design innovations in security such as file encryption which were developed 'after the fact'. The same should be seen as being true for privacy as a system service with the idea being to embed privacy within system settings as a default service. Dr. Ioannidis outlined a number of advantages, such as unified standards and disadvantages, such as a single point of failure, to such an approach.

Dr. Ioannidis then proceeded to outline a potential 'wish-list' of how privacy as a system service could be implemented. These included privacy proxies, privacy libraries and privacy policy management as examples. One key example of privacy being implemented within the architecture of systems included privacy scrubbers, gray boxes and black boxes where privacy is being protected for an individual in an unobtrusive fashion within the system itself.

As such for example the data scrubber would function in a manner which would erase any potentially identifiable or valuable information being saved within metadata tags. This would be done automatically by the system service, ensuring that individuals accidentally did not release valuable or identifiable information into the wild.

In terms of preserving privacy in the future Dr. Ioannidis stated that while ending all communication would preserve privacy it is not realistic or useful as an assumption for the ways in which modern societies have developed and function. The way forward he suggested was through the implementation of robust cryptographic measures embedded within communication systems. He concluded his presentation by suggesting that attempting to roll back what we might perceive as being privacy intrusive systems was swimming against the tide. He highlighted that we have some implementations of PETs but that we should strive to ensure that privacy

is a default, embedded within systems. Finally he concluded that the issue is multi-faceted, incorporating not only technical issues, but social, legal, economic and cultural ones with the caveat at present being whether individuals or organisations are really concerned over privacy.

Focus Group Discussion

The second session was chaired by Prof. Juliet Lodge. Dr. McCarthy was asked to summarise some of the key trends that had emerged from the morning presentations to begin the discussion.

Dr. McCarthy highlighted a number of key themes that had emerged during the presentations and questions that had followed them. He suggested that it remained an issue as to what exactly PETs were focusing on. Whether this was privacy or data protection or information security and how each of these could be defined in relation to PETs. This was compounded by the fact that defining each of these areas likewise remained difficult. He also drew attention to the division which seemed apparent between data losses that would arise out of end user activities and those that involved the 'sensor' network. This could be seen as the areas where data was being recorded on individuals without their knowledge.

A further area was also then identified as institutions, organisations or governments making errors or breaching privacy. This he suggested was important as it was very often the case that PETs were focused on the first and the last of these issues with major difficulties in seeing any implementations of PETs that would address this area. One means of conceptualising this as suggested by the focus group was to see it as the data we generate and the data generated on us. Dr. McCarthy then reminded the focus group of the Commission's objectives in relation to PETs and asked the focus group to keep these in mind in the ensuing discussions.

Prof. Lodge highlighted that while businesses might eventually be keen on PETs, where these could be seen as economically beneficial or protecting against reputational loss it was unclear how such technologies could influence governments or other state actors. The concern here was that there was little to no impact in terms of reputational loss for these types of actors, as in effect individuals cannot change the providers of state services as they may do with commercial providers of systems and services.

In this fashion she highlighted the fact that these PETs are not technologies that every individual in the society may have access to (for economic, educational or other reasons) and that this should warrant concern, for example in terms of the privacy of vulnerable groups such as asylum seekers or the elderly. It was clear that these were substantive issues of concern and ones not easily resolved. The issue of the economic cost of PETs, who products were targeted at and who might be excluded as a result was a recurring theme of the discussions.

Dr. Van der Veen suggested though in response to some of these observations that just because not everybody might be able to use PETs may not necessarily mean that we should not promote them as valuable technologies for those that *are* able to use them. He suggested for example that we still use bikes (a socially desirable technology from the perspective of the environment) even though not every individual is capable of riding a bike. It should be stressed then that PETs even if problematic in some regards should still be encouraged to be developed and deployed. There was general consensus on this point in the focus group but the point was noted

that they could be encouraged still within a framework of critical reflection on other issues. As such it was not felt that there should be impediments on technological innovation but interactions in the form of engaging dialogs on important issues.

Dr. Rouvroy commented that privacy must be seen as a fundamental right. In fact she highlighted how within Europe at least privacy is one of the fundamental rights as set out in the European Charter on Fundamental Rights. Following from this the relationship between data protection and privacy is a complex one and that it remained problematic in that PETs might just be technological fixes to technologically created problems. As such the focus should be on protecting privacy in the first instance by strengthening protections for individuals from data being collected on them. Perhaps we need to think and talk about it differently – for, from Rovroy's perspective, privacy is not simply something that we should leave it up to technology experts and technical devices to 'ensure'. The relationship between conceptions and definitions of privacy and data protection or information security need to be tackled and addressed. Specifically engaging in meaningful dialog was flagged as an important element of this, which was a recurring theme within the focus group.

Mr. Van der Veen provocatively suggested that perhaps it is not unimaginable to think that in 10 years this discussion about privacy will be an 'old fashioned' discussion given the trend towards more and more collection, usage, storage of data in our everyday lives. One trend here for example would be developments in Ambient Intelligence will exacerbate at a possibly rapid pace due to the evolution of what may be a networked world with massive amounts of embedded sensors recording and collecting data from us. Current discussions then on privacy might be seen as old fashioned due to the pace of technological developments in these areas far outstripping the ability of regulators, social scientists or other state actors to formulate means of protecting data within the current frameworks we have available to us to deal with these issues.

This provoked a lively discussion about how realisable such a future scenario might be. It also emerged from the focus group discussions that such a future illustrated clearly the need for dialog and engagement between various actors. It also highlighted issues addressed in the brief about the nature of legislative catching up with the pace of technological innovation and deployment. This was countered by observations derived from Dr. Ioannidis' presentation which illustrated that just because legislation or technologies to protect privacy are catching up does not necessarily entail that they will not be successful. It was suggested then that this aspect was one which deserved further exploration.

Dr. Ioannidis argued that perhaps the 'small' issues we were concerned with in the focus group are in fact only 'short-term' and possibly not terribly significant issues given that historically technologies have continually led to positive developments in human lives. While some technologies of course have had negative implications Dr. Ioannidis suggested that in the greater scheme of things technology in a general sense has enabled humans to do more in and with their lives and positively contributed to human individual and social development. The concern and focus as such then should be on how to do things 'right'. Or what safeguards could be built into current developments in technologies, such as biometrics, surveillance technologies and data collection by organisations that would enable and foster technological development and innovation in a positive fashion for the benefit of society.

Prof. Mordini argued that what needs to concern us is the way in which the technology application (here in the application of PETs) alter the relationship between the state and the citizen – or more generally, between an already powerful actor and a less powerful actor. From this perspective it is important to point out that technology can have two effects: it can equalize a previously unequal power relations *or* it can strengthen the power of an already superior actor and thus serve to exacerbate already unequal power relations. This was viewed to be important in the specific context of the HIDE project as its wider focus is on personal detection technologies, which generally but not exclusively are deployed by state and governmental actors as opposed to the commercial interest in PETs as deployments that were discussed. Whether PETs would be beneficial or harmful in this regards was a sustained discussion point for the focus group. In balance it emerged that a critical question was to what ends are purposes PETs would be deployed for. This was seen not merely as a question of defining PETs and the contexts in which they would be used but also asking as to who would be developing and utilising the various PETs that are emerging.

The difficulty in state or governmental actors adopting or seeing the benefits of PETs were seen as a challenge by focus group participants. These challenges were perceived to be in a number of areas. Firstly the discussion returned to the issue of those who might be excluded, through a variety of means, economic, understanding, education from seeing the benefits of PETs. Secondly encouraging governments to actually utilise PETs would represent a culture shift in thinking about the nature of data collection on the part of governments. Reference in the discussion was made here to the issue of Privacy by Design. Reference was also made to embedding privacy as a system service. In relation to the latter issues of consent and autonomy were discussed as well as a pragmatic concern over whether people should be protected from themselves and how this would function within potential deployments of PETs. It was noted though that the Commission was aware of developments and trends in terms of research and potential PET applications. This was set against the issue of governmental and state actors at member state level not having as much interest as might be found in official documents supporting PETs. The issue of trust as highlighted by Mr. Bramhall's presentation was also seen as an essential ingredient in how PETs might function within governmental systems and to how publics would react.

The focus group discussion as such returned to the framing of the work of the group in terms of the EC Communication on Privacy Enhancing Technologies. It was noted that while the first objective was being met in terms of their being a wide variety of projects being funded by the Commission (with a number of examples being given in the presentations session) it was unclear what the progress on the second and third objectives were. Realising these two objectives may indeed it was suggested be difficult given the observations that the discussions in the focus group had illustrated. Reference was made to the fact that data controllers might be too general a term given the different conditions and contexts within which for example governmental and commercial actors are operating. Similarly in terms of encouraging the use of PETs by consumers it was discussed that likewise this category may be too broad and too vague. Again it was unclear as pointed out in the discussions as to whether the Communication was solely focused on commercial aspects or what the relationship between these aspects and state settings would be in the context of the development and deployment of PETs. Likewise the issue that PETs would appear for the most part to be concentrating on data protection, or information security as opposed to privacy per se (although it was acknowledged that privacy itself could be seen as having a number of ways of being defined) raised questions as to the essential purposes for which PETs

would be utilised and deployed. This was also a point seen to have bearing on who would be the principal users of PETs. If the field is to be market driven then ability to purchase may be then also be a barrier to wider use and uptake of PETs particularly for already excluded groups from the digital revolution. Furthermore those who are the most vulnerable within security and detection technologies, such as refugees, may not benefit in any way from PETs. It remained a question to be explored the extent to which PETs would impact on such settings, given that for example these groups were often the ones subjected to the most intrusive of measures, such as for example, the new Borders Agency UK scheme to use DNA testing for asylum seekers. What role PETs might place in these kinds of deployments, and how they might positively or negatively impact on power relationships between actors mediated by technologies was seen as an area necessitating further investigation.

The focus group was concluded by Dr. McCarthy, Prof. Lodge and Prof. Mordini with the recognition that dialog must be encouraged and supported between various actors and stakeholders with an interest in Privacy Enhancing Technologies.