

PETS 3rd 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 last of these focus group workshops was held in London, UK on the 14th May, 2010.

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 final focus group was centered on identifying elements of the ethical brief to be reworked and edited for the final version of the brief.

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.

While previous focus groups comprised technical presentations and overviews of different ways of implementing PETs the final group comprised of presentations focusing on the ethical, social and legal aspects engendered by the development and promotion of PETs.

As noted, one element of the ethical brief is its analysis of the legal context, which itself is framed by the European Commission "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). A highlight of the ethical brief in its discussions on PETs is that 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. With the Lisbon treaty and the observation that it guarantees Privacy as a fundamental right it could be reasonably assumed that PETs will be seen as an increasingly important means of guaranteeing this right. Likewise the Madrid Privacy Declaration (a pronouncement issued by over 100 data protection authorities and privacy related organisations) recommends

‘comprehensive research into the adequacy of techniques that deidentify; data to determine whether in practice such methods safeguard privacy and anonymity;’

It is clear from these developments which have occurred during the course of the project that there are significant points to be addressed in terms of the ethical, legal and social issues involved in PETs. The ethical brief identifies and suggests that there are two different technical approaches, and the main ethical and social implications that might arise from the development and deployment of technologies within each approach:

As such for this focus group Cesagen would seek that participants ground their discussions in relation to a number of points as summarised and detailed above, these should be to

1. Consider the definition employed in the ethical brief with respect of technological approaches to the implementation of PETs. What might be the main ethical, social and legal issues that flow from these approaches and the types of technologies characterising each approach?
2. In regards to the European Commission's objectives, what ethical, social and legal considerations could be made in respect of them? Are there particular issues that are not addressed by the Commission's objectives and documents that the Ethical brief should aim to highlight?
3. What specific changes and alterations can be made to the intermediate version of the brief? Both to capture ongoing developments related to Privacy and reflect the particular ethical, legal and social concerns raised during focus group discussions and presentations.

The third 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,

Prof. Ruth Chadwick (Cardiff University), 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, Prof. Irma Van Der Ploeg (Zuyd University), Prof. Raphael e Vries (PRIVILEGE), Prof Mireille Hildebrandt (UBE), Mary Collins (IBG) and Ms. Laureene Neeves (Cesagen).

The three invited speakers for the focus group were Prof. Ruth Chadwick, Dr. Antoinette Rouvroy and Prof. Mireille Hildebrandt.

Presentations Session

Prof. Ruth Chadwick

Prof. Chadwick delivered the first presentation of the focus group which sought to explore current challenges to privacy and what role PETs might have in meeting these challenges. As an introductory note Prof. Chadwick pointed out that it should be mentioned that her comments on PETs emerge from her work in the field of genomics. It was put forward that her presentation would demonstrate that useful insights on the issue of privacy could be derived from a comparison between how privacy is debated in the field of biometrics/ICT and how it has been (and still is) discussed in the field of genomics. Prof. Chadwick also in the opening to her presentation asked the question about what changes to privacy are occurring what the relationship between ethics and privacy might be in the future due to current and future challenges.

Prof. Chadwick then suggested that privacy could no longer be guaranteed. In support of this she listed three types of challenges to privacy,

- Intentional, i.e. intended
- Side effects of new technologies
- Cultural changes; the new exhibitionism (social networks)

In terms of intentional challenges to privacy Prof. Chadwick pointed towards increased surveillance as a result of the desire to ensure security. Intentional violations of privacy could be seen as emanating from governments and importantly corporations. Some of the arguments made which seemingly allow for intentional violations of privacy such as the supposed trade-off between security and privacy but also being able to use commercial services. An example from the medical field was where disclosure of information was seen as being important in terms of how it might benefit another. The next set of challenges that Prof. Chadwick discussed were those arising out of being side effects to developments in existing technologies or as a result of new technologies. Of concern here was also the massive increases in the collection and storage of information as a result of wider and more general trends in computing and ICT. Such developments and advancements have allowed for new forms and ever increasing scales of data mining for example. Prof. Chadwick particularly highlighted the growth in forensic databases, such as the UK's National DNA database and highlighted the issue of third parties having access and their implications in terms of the potential types of information that might be gleaned or disclosed from them. Prof. Chadwick also gave the example of mobile phone usage and made mention of the next generation 'smartphones'. Prof. Chadwick gave the example of how Nokia are experimenting with biosensors in phones, suggesting more ways in which potential medical information will be accessible and recordable in a wider variety of settings. The final challenge to privacy Prof. Chadwick outlined centred on cultural challenges with the specific example of 'The new exhibitionism' being detailed. Examples of this trend were given such as

the increased prevalence of physical tattoos. The explosion in terms of personal information being placed on social networks or on blogs was also cited. In relation to this Prof. Chadwick highlighted that within Genomics notions of Individual privacy vs. Group privacy could become more relevant as a result of technological advancements in that more technological capabilities could reasonable mean conclusions can be made on groups and their information used against them over and above individual concerns.

On the very notion of privacy – or rather, on ‘aspects of privacy’ – Prof. Chadwick suggested that in addition to differentiating between informational privacy and spatial privacy (as is done in the Ethical Brief) it would also be useful to distinguish between individual privacy and ‘group privacy’. Also the idea of ‘decisional privacy’ could be added to the EB. Having delineated these three challenges, Prof. Chadwick then went on to suggest some potential responses, these were listed as

- The use of PETs
- The Design turn in Ethics
- The idea of ‘open consent’ (Here Prof. Chadwick made specific mention of BarthaKnoppers’ point that if consent is no longer possible then what we need is not simply a new definition of privacy but structural governance reforms that addresses problems)

Prof. Chadwick also added to this that we need also be aware of different generational publics, and differences between the qualities of the data/information revealed in different contexts – although this is complicated by the cumulative effect in the case of biometrics where even ‘weak’ data (also referred to as *soft biometrics*) can have ‘strong’ privacy implications when added/accumulated on databases. Prof. Chadwick made some specific references to agency and choice and how these have an important bearing on the meanings of privacy. Prof. Chadwick then commented on Nissenbaum’s notion of ‘contextual privacy’. Making a distinction between internal logics (of one context) and its outside/external logic with the observation that negotiating this boundary is crucial and dependent on the perspectives of the individuals or organisations involved.. This would often be determined by the logic of the context in which information is being revealed, such as with internal goods such as medicine vs. friendship what is revealed in both cases will be limited and variable. How much choice people have in these contexts was questioned by Prof. Chadwick highlighting the problems of revelations by third parties, the cumulative effects of personal choices and what privacy futures will emerge, or whether there will be privacy dystopias.

Reflecting the Ethical Brief Prof. Chadwick returned to the issue of definitions of privacy, citing two covered in the brief, Spatial, Informational and querying whether decisional privacy could be included. Having suggested that the concept of privacy is problematic both because it seems to refer to a promise that can no longer be kept and because of the large number of different meanings it has in different context, Prof. Chadwick then moved on to the question of whether we should ‘abandon’ this notion and instead speak, for example, of ‘informational security’? Perhaps we should not speak of privacy, but of **appropriate norms of information flow** (cf. Nissenbaum). In relation to PETS Prof. Chadwick queried the terminology of Enhancing privacy, why do we call it enhancement and not protection? And when we talk about ‘enhancing privacy’ it is vital to pose the

question of whether this is imagined to happen qualitatively or quantitatively. Prof. Chadwick also referred to two approaches described in the brief that of data anonymisation as opposed to data minimisation. Prof. Chadwick flagged a particular concern in terms of the discourse of trade-offs and 'win-win' solutions as when reference is made to either 'trade-off' or 'win-win' scenarios it is crucial to be aware of the political commitments underlying these debates. Mention was made here of the potential lessons to be inferred from different contexts such as for example genomics. Also noted was the balance which needed to be found between the Right to privacy vs. norms of information flows.

Prof. Chadwick concluded with querying the notion of Private and Publics. Prof. Hildebrandt asked the question Where/what is public? Or indeed what is the Notion of a public space. There is an argument to be made for example that Twitter and other social networks are in fact public spaces of some kind now. Also, a question that emerges is that of what 'counts as' private space 'vs.' public space (another point that could be elaborated in the Ethical Brief) – specifically in relation to how the way in which this divide is settled will, in turn, affect norms of information flows!

Prof. Chadwick concluded here and a short Q&A session followed with focus group participants on the topics covered. Dr. Van der Ploeg began by asking whether Prof. Chadwick could elaborate on the idea of a design turn in ethics? Prof. Chadwick responded in indicating that this was already mentioned in the EB. It refers to what can be understood as a 'constructive technology' with ethical values built into the very design of the technology. PETs are (the EB suggests) an example of this. Dr. Van der Ploeg continued with asking could this be an idea for a larger context than PETs? Prof. Hildebrandt responded to this question by suggesting that this seems to be the case indeed. Nissenbaum has, for example, written on 'values in design' and Cavoukian also talks about 'privacy by design'

Prof. Mordini made the comment that privacy is multifaceted and therefore PETs are surrounded by considerable ambiguity given that there exists no prior definition of the 'privacy' that these technologies are supposed to 'enhance' – it is therefore important that we engage the underlying question of what *values* are protected by privacy? This relates to your point about public/private space. A person's *willnot to be seen* is an important point because, legally (in current Italian law), this changes whether it is a private or a public space

Dr. Van der Ploeg suggested in response to this seems to be parallel to what happens on the internet. Prof. Vries asked that Prof. Chadwick had mentioned the idea of 'broad consent' – as a lawyer noted that in some EU member states national legislation forbids this idea of broad consent. Prof. Chadwick responded that she couldn't see that there should be anything wrong with the concept. Prof. Lodge also commented that privacy is sometimes seen as a fundamental right but its conception is very difficult to maintain in light of the points raised by Prof. Chadwick and that this should be expanded in the ethical brief.

Prof. Mireille Hildebrandt

The second presentation of the focus group was given by Prof. Hildebrandt. She began by outlining the key topics to be covered in her presentation which were,

- Privacy and Approaches in terms of PETs
- Threats to Privacy
- The Computational turn
- The proposal of Ambient law

Prof. Hildebrandt began by noting that she saw two technical approaches to PETs being described in the brief. These were Anonymisation /pseudo anonymity. PROF. HILDEBRANDT made the important point that in many instances because of advances in ICT data mining allows for de-anonymisation with the further caveat that applying these types of processes of data would remove it from protection from the directive 45/96/EC which would be further problematic. The second approach was that of Data minimization. This 'PET' is, however, not a technology approach, and PROF. HILDEBRANDT suggested that we need to make use of 'smart technologies' given the complexities of today's society. Thus, she stated she was critical of whether this 'non-technology' can 'solve' the problem. PROF. HILDEBRANDT then discussed some ways in which privacy can be conceptualised. The first of these was the idea of Privacy as sovereignty. PROF. HILDEBRANDT suggested that it was this conception that thus far has guided most of the EU directives and was central to data protection legislation and the activities of data protection authorities. PROF. HILDEBRANDT noted a number of problems with approaching privacy in this manner. Firstly she noted that the very idea of data ownership itself was very problematic. How can information be owned? For example is my name something I own, either as data or information stored on me somewhere in a database. In contrast to this PROF. HILDEBRANDT noted how the concepts of data confidentiality and the notion of access control made more sense in terms of being a workable framework for understanding privacy. PROF. HILDEBRANDT stressed however that privacy cannot be reduced to any of these single aspects or more specifically that these aspects should not be conflated with privacy.

PROF. HILDEBRANDT then turned to her second conceptualisation of Privacy, it being seen as boundary negotiation. PROF. HILDEBRANDT noted that this was the approach she favoured the most. PROF. HILDEBRANDT noted that this could also be construed as seeing privacy as the right to freedom from unreasonable constraints on the building of one's identity. PROF. HILDEBRANDT along these lines noted that Privacy should be seen as a relational concept and that it is *not* about sovereign individuals. This she noted highlighted some problems with current data protection approaches. PROF. HILDEBRANDT asked the question as to whether Autonomy was the same or meant sovereignty. PROF. HILDEBRANDT further continued with suggesting that Autonomy and seeing it as the capacity to reflect/to develop second order beliefs and desires is a much more robust way of conceptualising privacy and again cannot be seen as sovereignty. PROF. HILDEBRANDT suggested then that measures such as sticky policies, privacy audit trails were more about sovereignty and that furthermore data security could not be seen as synonymous with privacy. With Privacy being a relational concept the questions that can arise centre on for example as to how do you deal with others. How do you manage your relationships with and to other people and what is the role of information flows between these people you know and how is it as individuals we reflect on these processes. For PROF. HILDEBRANDT she suggested that this was a critical way in which to meaningfully engage with conceptualising a potential framework for understanding privacy.

PROF. HILDEBRANDT then discussed her final conceptualisation of privacy which was to see privacy as a practice. Importantly she stressed that this should not simply be seen as the practice or attempts at shield yourself off from others or the world around. Very often PROF. HILDEBRANDT noted privacy in this type of framework was seen as a sort of negative freedom. As such it could be freedom from discrimination, although invisible social sorting might in and of itself be difficult to solve in practice. Questions here also included due process for the protection of privacy. If it was invisible then it also becomes much more problematic because it makes 'the invisible sorting' incontestable. As PROF. HILDEBRANDT put it as the fear was that "You want your privacy, well, then we won't serve you/deliver services to you", and that this could be a very likely scenario. PROF. HILDEBRANDT then noted that: "what I have said in my presentation so far can be summed up as follows: It's not the data [that's the problem]. It's the inferred knowledge!" Knowledge means we are comparable humans and our actions can make us definable. For industry, can data be seen as a resource? If it is a resource then while problematic it can easily be seen how the practice of privacy would be subsumed under the needs of commercial realities and operations.

PROF. HILDEBRANDT then turned to discuss the issue of the computational turn which she identified as having two characteristics. Critically she suggested as above the important observation is that data is a resource now. PROF. HILDEBRANDT referred to her own work on transparency enhancing tools as a means by which individual autonomy could be increased in relation to privacy without being bogged down in terms of arguments over sovereignty. These types of tools for example can perhaps not prevent but frame what knowledge is inferred from databases about individuals? PROF. HILDEBRANDT also mentioned that an important aspect here was group profiles or what the implication data mining has for the question how 'I' match knowledge or a profile as an individual rather than a collective. PROF. HILDEBRANDT also noted that protecting yourself from the state by means of the state (courts) and against the state (legislator and executive). . PROF.

HILDEBRANDT noted what kind of response could be made to this observation in terms of a social constructivist approach? PROF. HILDEBRANDT said that for example I want to know what is being inferred from my data! I worry about what knowledge is being inferred from my data *and* about how my data might match inferred knowledge derived from mining *other* data! PROF. HILDEBRANDT continued with stating "I've been treated on the basis of this knowledge (which produces particular effects), but the database could have been mined differently!" Therefore there should be a right to know on what basis I am being treated or anticipated by my surroundings (in particular when this has important (political, social) consequences. What role for state actions in this was debatable and furthermore the role of PETs potentially in solving this was likewise debatable in terms of whether they could be successful.

PROF. HILDEBRANDT stated she was sceptical of this for two reasons. The first of these PROF.

HILDEBRANDT commented was that PETs risk reducing privacy to informational security and that reduction of data worried her because the threats to our privacy that exist today do not simply have to do with/cannot be reduced to a matter of data/information. PROF. HILDEBRANDT noted that PETs are supposed to survive on the market in that one of the objectives set out by the Commission in relation to the technologies is there are to be taken up by data controllers and individual consumers. PROF. HILDEBRANDT observed that as of yet there is no incentive structure in place to facilitate (let alone guarantee) that this will happen. Here Hildebrandt refers to

the work she has done on the concept of TETs – transparency enhancing technologies/tools (FIDIS) as well as ambient law. Likewise PROF. HILDEBRANDT noted the problem that if machines define a situation as real, it is real only in its consequences and this has important ramifications for seeing privacy as a practice within which PETs might have some role. PROF. HILDEBRANDT prefaced her comments on Ambient Law in terms of it being not a Solution, but a proposal for a direction of thinking. PROF. HILDEBRANDT defined Ambient law as using the infrastructure you want to protect yourself against by *re-designing* it. PROF. HILDEBRANDT referenced the example of being a digital humanities scholar tasked with pointing out that perhaps this particular pattern has emerged (and is defined as ‘real’ by a machine), but another pattern could have been derived had the data been mined differently/had another algorithm been used! PROF. HILDEBRANDT argued that there should be a fundamental right to trustworthy ICT infrastructure (and referenced Kolinar)

PROF. HILDEBRANDT concluded here and a short Q&A session followed with focus group participants on the topics covered. Dr Van der Ploeg asked is this ‘solution’ not again only about ‘data’ which PROF. HILDEBRANDT had just warned against, arguing that privacy cannot be reduced to data? PROF. HILDEBRANDT noted that on her last slide she indicated that an important point is that an individual must be able to see the profile and the factors upon which it is based/derived (or how decisions are arrived at) --- hence, it is not only an issue solely about data

Dr. Antoinette Rouvroy

The final presentation of the first session of the focus group was given by Dr. Antoinette Rouvroy. DR. ROUVROY began by outlining that much of her presentation would rest on exploring the ramifications of the increased prevalence of a surveillance society and how and could PETs fit into the framework engendered by considering the surveillance society. DR. ROUVROY began by considering the positions of PETs in relation to a surveillance society but continued with the provocative suggestion as to whether we do in fact live in a surveillance society as the question that could be asked is that does this exist anymore or is just a necessity in availing ourselves of the digital relations that make up much of the activities of modern life? DR. ROUVROY noted that everything today in society is recorded, meaning that surveillance and indeed governance is being everywhere as a result. DR. ANTOINETTE ROUVROY suggested there is interconnectedness between technologies, all of which capture data and digitize life itself leading to the development of something which can be seen to supersede the concepts and ideas which are said to frame and conceptualise the emergence of a surveillance society.

DR. ROUVROY continued with the observation that new methods and technology of surveillance work on the statistical body. DR. ROUVROY suggested that this Prof. Hildebrandt phenomenon centres on governing traces of us without entering into contradiction with other bodies by the fact that this occurs virtually or remotely due to the fact that these traces exist on databases to which we have no immediate relation or physical vicinity in most cases. DR. ROUVROY asked at this stage though has visibility not increased? An individual’s presence on databases of all kinds, the fact that there are recorded in every more pervasive situations such as in airports or by extensive CCTV infrastructures or recorded in various places through the use for example of the Internet would suggest an increased visibility in modern societies through virtue of these technologies interacting. DR.

ROUVROY answered this question by stating that individuals are arguably more invisible than before. A part of this was the observation made by DR. ROUVROY that the power and temporality have changed too of an individuals visibility in a way which thus far has not been captured for example by legislative responses through measures such as data protection. In this type of framework the principal trend is one of governing by numbers which in itself relies on the invisibility of the parties involved such as the controlled and controller.

DR. ROUVROY observed that other trends in this type of society were the sweeping yet more refined classifications made of and about groups. DR. ROUVROY suggested that rather than focus solely on privacy, inasmuch as privacy is related to our identity, that then identity issues might be a more worthwhile consideration than privacy issues. DR. ROUVROY commented that other features of these trends was the decline of the national as a boundary to where information might flow, data travels in the sense that inter-border flows of data and information have grown exponentially. DR. ROUVROY question and highlighted the mode of propagation of flows through text and where individual equality in the face of Privacy Enhancing Technologies would emerge as a result of being able to take advantage of PETs. Along these lines DR. ROUVROY referred to her grandmother who she reasoned would be able to receive no benefits from PETs if they are framed in terms of individuals somehow interacting with them in a proactive manner. DR. ROUVROY also noted that the definition of privacy is contingent on conditions for example related to individual autonomy and collective democracy. DR. ROUVROY noted that if privacy is a site of contestation, then perhaps we have to keep it this way? As the related observation would be that the meanings of privacy can never be satisfied in an objective manner. DR. ROUVROY also asked whether, referring to previous presentations, privacy and space are in opposition to each other. In the sense that both can really be seen as being linked yet conceptualising both has proven to be difficult in terms of legislative responses to the challenges, and supposed challenges to privacy.

DR. ROUVROY then suggested that problematizing privacy but responding in terms of keeping its problems open is better than closing them. DR. ROUVROY expanded on this by suggesting that there is a flexibility that exists in the law as opposed to the imposition of technical standards. DR. ROUVROY reiterated that privacy must remain a site of contestation and that by keeping privacy a legal issue will give law's inherent ambiguity help to ensure this, whilst making privacy a purely technical issue we will lose that crucial contestation. DR. ROUVROY noted that if it was solely to become a technical issue, an individual citizen will find it more difficult if not impossible to challenge it as if privacy is a technical standard then more often than not the logic will be that it will become defacto and accepted. The law would avoid this by continually allowing for contestation and challenges such as to say the law would be mutable against some immutable invisible technology operating to pre-defined and unchanging technical requirements.

Focus Group Discussion

After the presentations the second session of the focus group was a round table discussion chaired by Prof. Lodge and Dr. McCarthy. Dr. McCarthy and Prof. Lodge began by highlighting some of the recurring themes that emerged during the three presentations and the discussions that followed them. One of these was that in terms of understanding Privacy is there anything that really exists can be said to be private data? What was meant by this was the observation as to what Data was and what its relationship was to the real world. Another observation was what the rationale itself for Privacy Enhancing Technologies was and the related comment that

this was inextricably linked with defining privacy and defining enhancement. Or more rather what was it about Privacy as an issue that was in need of protection. Given the problems outlined in each presentation was it reasonable then to assume and ask the question are PETs here now and gone tomorrow? It was also observed that at least in the context of Privacy and PETs the debates were nearly always about Information security and less well explored the notion of intelligence and how this relates to information and data. Privacy laws and data protection initiatives was observed by some on the focus group as being more about seeing Privacy as part of trust in terms of poor governance structures as to how information about individuals is regulated? Prof Mordini suggested that Knowledge and power are correlated, but where there is power so there is resistance and that many of the debates on privacy are actually about the ramifications about power as a result of new technologies. Prof Lodge then commented so how is this to be dealt with? If Privacy is a public issue then it is not something that is solely regarding an individual but is rather a community issue of debate that is inherently political as well. Private life has expanded its borders to include public life and this trend is reflected, or would be reflected the more PETs are being built into things. For the Ethical Brief an important part to explore then would be what is it when this happens and what are the perceived implications when privacy is held within systems or defined even by the technological components that comprise these systems? Prof. Mordini played a short video demonstrating Microsofts' 'Project Natal' and the plans to commercialise it illustrating just one way in which biometrics and indeed detection technologies were moving beyond the border and moving beyond the traditional frameworks in which debates on the digitalisation of the body have thus far taking place.

The discussion again returned to this issue of power relationships. It was suggested also that PETs are in fact ethically unappreciated and unacceptable due to the fact that groups are not considered (the active technologically savvy individual using them being the main consumer in the literature and policy documents) and currently policy fails to even make mention or suggest ways in which issues of exclusion and inclusion can be dealt with. A recurrent question was where are PETs likely to make a difference and where would they'd be applicable? Refocusing on issues related to the ethical brief was the issue of effectiveness and the proposed examination it if the goal is as clear as it makes out to be or whether everything is about making the public feel secure. Or in other words the deployment of highly intrusive surveillance and detection technologies is simply governments hoping to being seen to be doing something by the electorate. Why not adopt a policy of screening individuals on blacklists more than other groups that might be more effective rather than purchasing high cost technology that is assumed to be less controversial. The point was also raised as to how we protect privacy in the distributed networked society we inhabit? Is it Privacy by design or merely access control, inclusion and exclusion of individuals in the application of PETs, does link ability require a different sort of accessibility?

Dr. Dobrisek stated that he didn't see the sharp distinction between 'real world' and 'data'. He stated his whole body has a potential to become data. Dr. Van der Ploeg added to this suggesting she like the idea of not exaggerating the difference between the real world and data as this would fit with the conception that privacy is something that we negotiate. Dr. McCarthy then asked the question what are the ramifications of 'privacy as fundamental right' or rather might we end up with 'data protection' as a right, which is not equal to privacy protection? Prof Lodge suggested whether we abandon privacy and instead talk about informational security?

Dr Van der Ploeg responded by asking how do you differentiate information from intelligence? Prof Lodge continued by observing that intelligence is what you do with information as opposed to being concerned with the existence of information in and of itself. Prof Lodge further argued that we need to be sharp about defining terms and that the ethical brief needed to be open, explicit about the principles that leads us to these definitions. DR. ROUVROY argued that protecting the possibility to contest and discuss Privacy as a structural value was vital. PROF. HILDEBRANDT argued that the consequences of leaking data in an intelligent environment or exchanging data via a broad consent was likewise a critical one which was not only a privacy interest, but a public good which might be ruled by the implicit norms of one's environment. An alternative framework would be rather being able to distance yourself from these norms but if you have no clue how people will correlate your trivial data, this ability (to distance yourself) becomes problematic/difficult to maintain in such an environment. Prof Lodge commented on this stating that implicitly PROF. HILDEBRANDT was talking about trust – and ethical obligations arising out of this trust being placed into different actors or organisations. Dr Van der Ploeg stated the need to focus the discussion on what the Ethical Brief *can* accomplish and what its limitations are. Prof. Mordini suggested that privacy is not a private issue – privacy is a public issue and that data protection protects a certain *perspective*, a specific point of view.

PROF. HILDEBRANDT suggested then that importantly the goal is not to protect data, but to protect people. So we must ask ourselves, to what extent can you protect people by protecting data? And here the knowledge that is being inferred from data traced is an important point – if PETs were deployed to create delays between data traces this could perhaps be one way of protecting people? Prof Mordini commented that the point is not privacy itself and reiterated that the point is power – or, more specifically the power relations engendered by the more widespread use of new technologies. He continued by suggesting that the EC's definition of privacy is too simplified and that this should be noted or commented on in the Ethical Brief. PROF. HILDEBRANDT commented about creating 'delays' conflicts with border management and security requirements in that delays are counterproductive to security missions. PROF. HILDEBRANDT wanted to propose a distinction to be elaborated in the Ethical Brief between PETs for controlling access (*prior*) and PETs allowing for audits, or for the following of an privacy audit trail (*post*). Cloud computing was specifically mentioned by PROF. HILDEBRANDT in that she was worried about the security of cloud computing where it would be more and more used for database storage and operations. It is for example critical to note PROF. HILDEBRANDT pointed out that currently I do not have a right to know where my data is. PROF. HILDEBRANDT noted that cloud computing makes it even more difficult to know this. Thus PROF. HILDEBRANDT suggested it would be interesting to create a PET that would visualize for individuals where their data is (where in the world, geographically) – e.g. is data (collected in Holland) now in China? The link-ability of biometric data requires a new kind of transparency that current PETs and proposed ones do not seem to be able to counter.

The roundtable ended with a discussion about the feasibility of such a PET. Dr McCarthy concluded the focus group with thanking the presenters and the participants for a lively and fruitful discussion.