HIDE

FOCUS GROUP MEETING ON

on Privacy Enhancing Technologies

ORGANIZATOR

CESAGEN—Centre for the Economic and Social aspects of Genomics- United Kingdom

DATE

30th May 2008

PLACE

Nowgen Building, Manchester, UK

PARTICIPANTS

CSSC, IBG, ZUYD

Cesagen

Focus Group on Privacy Enhancing Technologies

May 30th, 2008

11am-3pm

Venue : Nowgen Building, Manchester, UK

Directions

http://nowgen.stardotserver.co.uk/downloads/81-Directions-to-Nowgen-2008-pdf

Time: 11am-3pm

On the day please contact Katja on 070951188032 should any problems arise in finding the venue.

Overview

The Homeland Identification and Technology Ethics project is a Co-ordination action promoted by the Commission within the 7th Framework Programme. As part of the core activities of the project a series of technological orientated focus groups are planned which explore significant issues in relation to the ethics of particular technologies. These 4 technological areas are technology convergence, outsourcing security, interoperability and Privacy Enhancing technologies. The activities on PETs are organised by Cesagen and this focus group is the first of 3 planned on exploring the issues that are involved. The ultimate objective of the work of the focus groups is to use the insights, data and discussions generated therein in aiding in the writing and presentation of an ethical brief on Privacy Enhancing technologies that will serve as an informative and balanced appraisal for PETs for the Commission, policy makers as well as the general public. Along with the focus groups a number of additional research activities will be undertaken in bridging the gaps between focus groups and providing an additional research and disseminative framework from which a report can be produced. These are described below.

Discussion Notes

Please note that the ideas presented in these discussion notes do not necessarily reflect the views of participants in the HIDE project or the focus group convenors. These notes merely serve to frame the objectives of the Commissions Communication on Privacy Enhancing Technologies within one potential framework of themes and issues. Each of these may be rejected in total, in part or accepted for discussion during the course of the focus group. A copy of the Commissions' communication has been sent with these discussion notes.

We would also like to note that the Commission's communication on PETs attached along with these discussion notes is relatively specific in its objectives and remit. A part of the discussion presented here centres on a wider conception of PETs. As such an important element of our discussions will be whether this broader conceptualisation is necessary to meet the objectives set out by the Commission, and if so how such a broader view can be integrated into these objectives. These are presented in bullet point format in the text below, part of the remit of the focus group will be acceptance or rejection of these as outlined above.

Background and Wider Context of the HIDE Project

Security and security policy has quickly emerged as a critical European mission due to events external to Europe as well as internal. The threats of terrorism, home grown as well as foreign, increased mobility among citizens and non-citizens, immigration, emigration and the continuing dynamics of ensuring safer societies for European publics have meant that the development of security policies has increasingly become part and parcel of the landscape of European political action. While such is the case for member states individually, increasingly it has also become a feature of common action promoted by the Commission, council and other European bodies. Indeed the reform treaty contains within it a number of important developments concerning the development of a common security policy for the EU. While there are many aspects to security policy one of the more controversial, or highlighted aspects to such policy is the increasing development of particular types of technologies to support the implementation of such actions.

The most visible of these technologies have been biometric ones even if it remains the case that many biometric technologies predate by a significant margin their increasingly sophisticated deployment within certain security policies. Similarly currently it is reasonable to suggest that security technologies

themselves are comprised in part only of biometric technologies and also it is clear that biometric technologies encompass a wider definition of security above and beyond their use in securing the spaces of and between states. A feature of this last trend has been the increasing use for example of biometrics technologies within consumer settings, such as banking and computing. This would suggest then that a focus on these technologies considering them only from their use by states is limited in its capacity towards understanding the interactions between citizens and such technologies in the conduct of their general and daily lives. Security then arguably can be said to be an increasing feature of modern life at various levels, ranging from personal, to societal to supranational.

How we define security has important bearings on the discussion as state-centric definitions of security, while remaining important, are increasingly only a part of a totalising discourse of security ranging from to state to individual. This is not to suggest a 1984 like situation where security is an imposed pre-requisite by the state on individuals. The situation is much more complex in that security has become in some ways a commoditised product as well as a matter of political expediency. The creation of secure spaces, political, social as well as individual has been accompanied by a proliferation of security related technologies which in the process of securing also monitor, record, observe and detect hence generating a wealth of data. As such one of the prime ramifications of such a proliferation of security technologies has been the growth of both the amount and types of data which is collected on individuals, groups and societies. This data, the amounts of it collected, the nature of the data being collected, its processing and sharing between different systems and actors during the course of analysing it provides much of the impetus behind developing and deploying privacy enhancing technologies. While it is true as a result that some of this data is collected without our active participation or awareness, much of this data is collected with our knowledge and understanding that such data is collected and will be processed according to respective data protection legislation.

The mission statement and context of the HIDE project is on promoting a dialog based on a deep and wide contextualisation of biometric and other security related technologies. Its chief premise as incorporated into the title of the project is on the idea of a European Homeland Security. Immediately as is discussed in other areas of the project a number of questions arise, mainly comprising the nature of a European identity and a European homeland whose security is to be guaranteed through the use of technologies and the adoption of a common security policy. These wider questions are of course important as the focus on privacy enhancing technologies as noted by the Commission is on the uses of such technologies in conjunction with existing and potential legislation on data protection towards guaranteeing fundamental freedoms and rights enshrined in European documents for European citizens. As such privacy enhancing technologies are seen as occupying an essential place in terms of

empowering citizens in what can often be an overpowering wealth of technologies which record, monitor, survey, detect and identify.

The Role and Impact of Privacy Enhancing Technologies

The Commission has set out three objectives related to Privacy Enhancing Technologies these being

1. Support the development of PETs,

2. Support the use of PETs by data controllers

3. Encouraging the use of PETs by consumers.

The series of focus groups planned by Cesagen as a part of the HIDE project seeks to engage with and explore each of these objectives. In discussing these objectives a key function of the focus groups will be to propose and explore potential issue and thematic frameworks which have a bearing on these objectives and PETs more generally. A potential framework proposed here in these discussion notes technologies is one which sees its interactions between a number of themes. This framework sees the importance of defining such technologies in tandem with key ethical impacts that might be expected to derive from the differing applicatory definitions of PETS that may be used. For the purposes of this discussion then 3 types of functions are seen to be performed by PETs, these being

1. Empowerment
2. Guaranteeing Rights
3. Balancing Interests

Linked to these are three ethical concepts that we believe interact and are interdependent with the three functions described above, these are,

a. Privacy
b. Autonomy
c. Social Justice

A feature of the growing debate on security policy and the security related technologies designed to implement secure societies has been public concerns over the use of such technologies. Such concerns arguably rest on issues of trust, privacy and the need to balance the interests of ensuring security versus ideals of liberty. The Commission has recognised the dilemmas involved, as have member states individually and as such the notion of privacy enhancing technologies has become a feature of policy documents as a means of ensuring and enhancing particular rights for citizens within the rubric of increasingly

security orientated policies in a number of areas. The Commission has set out a number of objectives in relation to PETs as described above. Our focus group aims to explore each of these objectives as well as support them through an assessment of the ethical impacts of PETs. The creation of such a dialogue on PETs is we believe an important one to address. Yet a focus on PETs as consumerist technologies may be wise in terms of garnering industry and citizen support through their actions as consumers but this may also be limited. While the use of PETs by data controllers is then a laudable goal, is there not a case to be made that citizens themselves through PETs may become personal data controllers, both in consumer and non-consumer settings. The recognition by the Commission itself that data protection in an increasingly globalised data sharing and disseminative world may be increasingly difficult may point towards a resolution based on individual privacy controls as opposed to national or structural controls.

In such a situation then the definition of PETs becomes a critical one. The Commission itself has acknowledged that a variety of definitions exists both within academic settings, supported pilot projects exploring PETs as well as industry. There is an argument to be made then perhaps that the differences in definitions may in actuality be a differentiation between the different uses for which PETs are envisaged as being put to. The question of uses and of more generally deployments is also then a critical element of assessing the ethical impacts of PETs as the contexts of PETs and their uses will determine the contexts of the ethics that we must be concerned with. While it will be beyond the scope of this initial focus group to provide concrete answers to this question it is the intention of the focus group to at least provide a possible overview of the potential uses and hence the potential contexts in which ethical impacts will arise that can be assessed.

PETs as Empowering, Guarantors and Balancing Technologies

- The first possible function of PETs that might accompany their deployment is the notion that such technologies might empower citizens and 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 then that this focus group will seek to explore. Yet we perhaps must situate such concerns with examining key questions for societies and individuals concerning the nature of privacy, the meanings of security and the interactions between rights, needs and preferences. The dialog needed to assess the impact of privacy enhancing technologies is therefore we believe a multi-faceted and multi-actor one by the nature of the topics to be explored. At its heart PETs could conceivably empower citizens in new

and innovative ways within security contexts but the nature, form and functions associated with this empowerment remain undefined and unexplored. Much of this may be attributed to the fact that PETs are a relatively nascent field in terms of their conceptualisation as a package of technologies designed to meet a specific need.

- The notion of empowerment may indeed be an important one as it is a potential solution to problems associated with trust, trust between citizens and the state, consumers and businesses and between citizens and other citizens. Trust is arguably a critical issue in security, indeed in many instances the use of biometric technologies is done so in order to identify trustworthy persons. Similarly in opposition to the use of such technologies is an oft cited concern of a lack of trust by citizens in the use of data generated by such techniques in a way which guarantees their personal liberty and rights. Opposed to this is the lack of trust between other citizens and non-citizens which leads to demands for the use of such technologies in creating and ensuring secure spaces, whether these are political, environmental or commercial. Feelings of disempowerment may in turn be important ones to consider in dealing with issues of building trust and the possible role of PETs thus may become increasingly important in terms of enhancing trust at various levels.

- 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 collected. 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 therefore along with enabling and empowering citizens a role for PETs in guaranteeing certain liberties and rights. But in tandem with these PETs can also be seen as balancing technologies between different needs and preferences of different actors in relation to the collection and processing of data generated by their activities or collected when they engage in certain activities. The balancing of interests is as such a critical agenda for security policy and one which is at the core of the HIDE project as well. Similarly in terms of enabling the balancing of interests' privacy enhancing technologies may arguably occupy a central and critical role in allowing this to occur. The growing lack of power and control able to be exercised by citizens' over a bewildering amount of places, sites, devices and transactions which record and process data concerning individuals behaviours places an emphasis on PETs as being an enabler of citizens in exercising particular rights related to their privacy.

What may be suggested given the discussion above is that the uses of PETs may determine the definitions which are then applied to them. As such seeing PETs as guarantors, of citizens' rights, as enablers, empowering citizens with control over their data or as balancers, whereby PETs may mediate between the interests of different actors may be a useful starting point in developing a robust categorisation of privacy enhancing technologies. An exploration of each of these roles is beyond the scope of this initial focus group yet we expect at the least to consider which function, or combination of functions it appears that the development of the technologies will progress towards in the near future. Similarly this question of the roles and uses of PETs or working towards definitions of them will lead us to be able to consider in a much more effective manner what the ethical impacts of such technologies and these uses will be.

Potential Ethical Impacts

- In examining the contexts of PETs and their possible uses and definitions the focus group is also aimed at exploring what these principal ethical impacts will be. We assume a broad definition of ethical impacts which is concerned with individual, group as well as societal impacts. For the purposes of this focus group we aim to deal with and explore the impacts on autonomy, privacy and social justice. It is worth noting some comments on each of these. The notion of autonomy is perhaps a critical one when considering PETs if we assume autonomy to mean the capacity to take informed decisions and be in control of one's action through these decisions. PETs in clear ways can not only be seen as privacy enhancing but also as autonomy enhancing where the focus for PETs is on granting individual control over their data and the uses of this data. In many ways existent national legislation as well as European data protection legislation rest on notions of autonomy for citizens in empowering them to restrict access and the use of personal data stored on them. On one level then we can see PETs arguably as strengthening and enforcing this aspect of autonomy enhancement. If we proceed down this path in examining the issue of control and empowerment then there is a potential argument that the use of PETs can further enhance autonomy above and beyond existing legislative structures. This can be so for both back end use of PETs in terms of data processing automation as well as front end devolvement of control to users through technological means. PETs both as enablers and guarantors would then seem to have a potential positive impact on citizens' lives.

- There remains an issue however in that autonomy can be said often to depend on the ability to exercise that autonomy. Lessons from informed consent are therefore perhaps relevant to this in the being technologically 'savvy' often appears to be a prerequisite for availing oneself of the

benefits of particular technologies. An example of this lies in the Internet where arguably more technologically savvy users are less prone to losses of data, more aware of threats to privacy and better self-informed in terms of the available technological tools that can guarantee privacy and safety in using the Internet. In terms of PETs this issue may have ramifications in two ways in light of the objectives of the Commission. In terms of the use of PETs by data controllers, if the focus is on backend procedures which for the most part are not visible to citizens then we can question the degree to which autonomy is enhanced. The obvious solution to this perhaps then is clear communication and engagement with citizens about how such procedures are used, deployed and managed. Secondly on encouraging the use of PETs by consumers a similar issue needs to be resolved in that there may be a body of consumers for whom engagement with and communication is much more easily relative to others whose technological knowledge and awareness of such devices may be limited. This means then a key issue for future consideration in relation to PETs will be the development and exploration of communication strategies that effectively highlight PETs, discuss the ethical implications as explain how PETs are relevant to as broad a range of users as is possible.

- Privacy is clearly the most relevant ethical implication of the use of such technologies yet an argument exists that privacy is dependent not only on autonomy but also on social justice. Seeing PETs as only relevant to privacy may ignore how privacy is changing and that in a global world in which data is collected, individuals are surveyed almost continuously then guaranteeing privacy may become an increasingly difficult challenge. Changing social attitudes may also be a concern, an example here is the increasing expansion of almost continuous monitoring of public spaces by CCTV systems. Given their growth in recent years it is perhaps interesting to note the lack of concrete visible public opposition to such devices. In many ways and in particular in the UK an argument can be made in that such devices have become transparent in terms of their acceptability. However it cannot be taken for granted that opposition remains invisible to such devices. Whether there is a shift in personal notions of privacy is an important one. New interactive websites such as MySpace, Bebop illustrate one example of this, where increasingly users are more willing to post their own information online in a form which is accessible to anyone using the Internet as well as restricting access to certain data through the use of friends lists. While concern is often expressed about the dangers of children or other vulnerable people posting too much sensitive information the point is sometimes obscured that this represents a shift in personal thinking on the meaning of privacy among both young people as well as other groups who use such sites.

- Privacy then may not be a flexible rigid construct in its interactions between people, technology and the conduct of their lives. How one defines privacy as such has an important bearing on how one might define a privacy enhancing technology? Are such technologies safeguards from others or from ourselves? Such 'nanny' devices may indeed often be used by parents in order to restrict children's activities on the net but it may also be the case that some PETs will assume a protective role to safeguard us from our own activities. If this is the case then definitions of privacy become increasingly relevant as the establishment of norms for what constitutes privacy will inform the technology development process. In some instances technology may already be ahead in allowing consumers to select their desired privacy levels, the use of firewalls for example allow for different levels of protection. Is there a case to be made then that continuing development of user choice on the level of protection afforded by PETs should be continued. But again in a circular fashion we are returned to our comments in relation to autonomy above in that the provision of information and the relative awareness levels among different groups in respect of the technologies or procedures involved will create challenges in terms of the equitable access to such technologies by European citizens.

- These points lead then to a consideration of social justice in terms of the deployment use and take up of PETs. We believe this is so as a result of the observation that such technologies may be exclusionary as well as inclusionary on a different number of levels as well as in a different number of ways. In one way the provision of and general holding of information amongst particular groups of users can be seen as a knowledge based exclusion. Yet this exclusion is not necessarily combated by information alone, while being illiterate for example (other than medical conditions) is a relatively easy knowledge to impart given time and proper support some illiterate persons rarely seek such support and attempt to manage social situations where their inability to read may or may not be detected. Technological illiteracy may share some similar features in that people lacking comprehension that may have been communicated with in terms of utilising features may or may not actually understand what can be quite complex procedures and technologies. Similarly while academic or legal protections about particular constructions of privacy are importance in a world where individuals are increasingly conceptualising their own versions of privacy means privacy enhancing technologies may diverge in terms of their commercial usage and regulatory usage. Indeed inasmuch as there is a need to communicate in terms of imparting knowledge concerning technological innovations to consumers or users there may also be a need for governments and vendors to respond to customer conceptions of what their privacy spaces might be or might need to be in a variety of settings

and contexts. Privacy and technology both then may need to be responsive, dynamic and demand reflexivity amongst all actors in terms of their interactions and uses.

Examining these three issues, of autonomy, privacy and social justice are we believe core reference points for the focus group and also central themes within the issues surrounding the development and deployment of PETs. This focus group then is convened with the express intention of discussing these issues. While an agenda is set in terms of speakers and the intention is to allow a free discussion the focus group is also orientated towards three objectives which we believe e both our speakers and participants are well positioned to deal with. These objectives are also in line with the nature of the report that forms the final outcome of all three focus groups and thus are important elements to be teased out during the progress of these activities within the general framework of the HIDE project. It is important as such that it is recognised that each of these objectives is an ongoing objective to be resolved within the plan of activities dealing with the exploration of privacy enhancing technologies.

Main Issues at Stake

1. How can we define Privacy Enhancing technologies?

We believe that an essential precursor to exploring potential ethical aspects while obvious on one level is not so clear in the detail is the manner in which we define Privacy Enhancing Technologies. Mentioned in these discussion notes has been made of the potential uses of PETs in terms of their roles as guarantors, enablers and balancers. These definitions do not of course preclude other potential definitions of PETs such as a focus on those which are invisible or visible to end users. Or indeed even definitions dividing PETs into software or hardware based. As such a critical aim for this initial focus group is to consider potential definitions of PETs where these are possible. Such definitions will we believe be an invaluable guide towards contextualising the ethical impacts of PETs in different contexts where they will be used.

2. How do such technologies interact with legal frameworks existent within member states and which are existent within the European Union?

Our second point of discussion will be to examine how such technologies can be reconciled with existing legal frameworks. Do such technologies complement existing legal frameworks on privacy within the European Union as well as within member states? While a full discussion of such issues may be beyond the scope of this initial focus group we intend at the least to explore how our definitions of

PETs above fit into European legal frameworks as well as other statutory definitions of privacy that exist. Similarly the discussion here should explore how definitions of privacy across Europe and within European documents may dictate the nature of PETs and their development and deployment.

3. What are the ethical ramifications?

A final discussion point for the focus group is based on the definition and exploration of possible uses of PETs and in tandem with discussing how these complement or interact with existing legal frameworks. This final discussion point will be an exploration of what the key ethical issues will be in relation to the use, development and deployment of technologies. Again given the scope of this initial focus group it is not our intention to have an exhaustive list of the potential ethical implications but rather to explore in relation to autonomy, privacy and social justice what the major areas will be where positive and negative impacts might be expected to derive in the development and deployment of PETs.

Objectives

The FG will focus on the three objectives of the EC Communication on PET, namely

1) **To support the development of PETs**

2) **To support the use of available PETs by data controllers**

3) **To encourage consumers to use PETs**

We shall ask participants to enlighten the main policy and ethical issues raised by these objectives, having in mind that the final goal of the FG is to produce recommendations to the EC for policy implementation and future policy setting.

Format:

As noted above this focus group is the 1st of three as well as comprising one part of a wider research agenda exploring PETs with the aim of producing and ethical brief of PETs for the Commission and other actors.

As such in tandem with the three focus groups other activities are planned to bridge the gap between the focus groups and to provide additional contributions to the writing and preparation of the report.

There are four other activities planned in conjunction with the focus groups are

1. Documentary reviews and literature/debate analysis

This activity will comprise of Cesagen monitoring debates on PETs as they emerge in Europe as well reviewing/analyzing literature that emerges on PETs within various settings. It is the intention that such synopsis and analysis will be made available to focus group participants in order to keep information about PETs up to date for all participants.

2. Linked to the activity mentioned above, a mailing list will be created where such information can be disseminated.

The mailing list will also be interactive with participants and invited experts able to contribute to ongoing discussion related to the drafting of the report. The mailing list will be used to assist in the drafting of the final report with review versions being sent to participants using this means.

3. It is hoped that further expert meetings will be held outside of the three focus group structure.

These expert meetings will be used to explore specific areas of PETs that become visible during the course of the HIDE project. Such meetings are dependent on co-funding opportunities being found to support such additional activities. A wider remit for seeking co-funding opportunities is also expected to be incorporated into the research

4. The final activity will be a series of consultation activities.

These will aim to leverage the platform of experts established by the HIDE project as well as target specific actor groups, such as NGOs, consumer organizations for their views in order for them to be incorporated / noted in the final report.

The format of the focus group is to have two split sessions within an informal setting to promote free and frank discussions among the participants. As the concept as well as development of privacy enhancing technologies is a relatively nascent idea the framework is to have a morning session where focus group participants will give presentations serving as a basis on which to generate discussions in both sessions. The aim of these presentations is thus to give a synthesis of technologies, an overview of potential and negative impacts of their deployments and finally a synthesis of how PETs are incorporated or rolled out in example deployments either forthcoming or already in use. These presentations are followed by a discussion session which will be directed towards identifying key issues and themes to be explored in more detail in the second session.

The second session is a focus group round panel discussion. The panel will be chaired by Prof. Ruth Chadwick and include speakers for the first session. In light of the focus group structure and framework the aim as such of the round panel discussants is to act as prompts for an interactive discussion amongst all participants in the focus group. In tandem with exploring the themes identified in the first session the aim of the focus group is to make contributions to three topics which will later be incorporated into drafts of the ethical brief. Namely the focus of the discussions will be generating definitions as to what constitutes a PET, i.e. what are the categories of technologies that might be included and what are the potential negative and positive impacts and their ethical ramifications.

Agenda

10.45-11.00 Coffee

11.00--11.10 Presentation / Overview on PET focus groups by Dr. Paul McCarthy

Privacy Enhancing Technologies: Cesagen's Workplan

11.15-12.30 Presentations

This presentation section will focus on the objectives of the Commission in relation to PETs and how these might be supported in light of the different perspectives represented by the speakers.

11.15-11.35: Michael van der Veen (*Philips, General Manager priv-ID Biometrics*)

11.35-11.55: Juliet Lodge (*Professor of European Politics*)

11.55-12.15: Jonathan Bamford (*Assistant Commissioner and Director of Data Protection Development, Office of the Information Commissioner*)

12.15-12.25: Niovi Ringou (*European Commission, Deputy Head, Media and Data Protection*)

12.45 Lunch at the Nowgen Centre

This will be a working lunch where the aim will be to continue informal discussions generated by the speaker's presentations.

Round Panel focus group Discussion chaired by Prof. Ruth Chadwick

1.15-3pm

The panel will consist of speakers plus participants. aim of the discussion will be to have an informal idea-generating discussion based on the principal themes identified and highlighted during the first session.

3pm Finish and Close of Focus Group