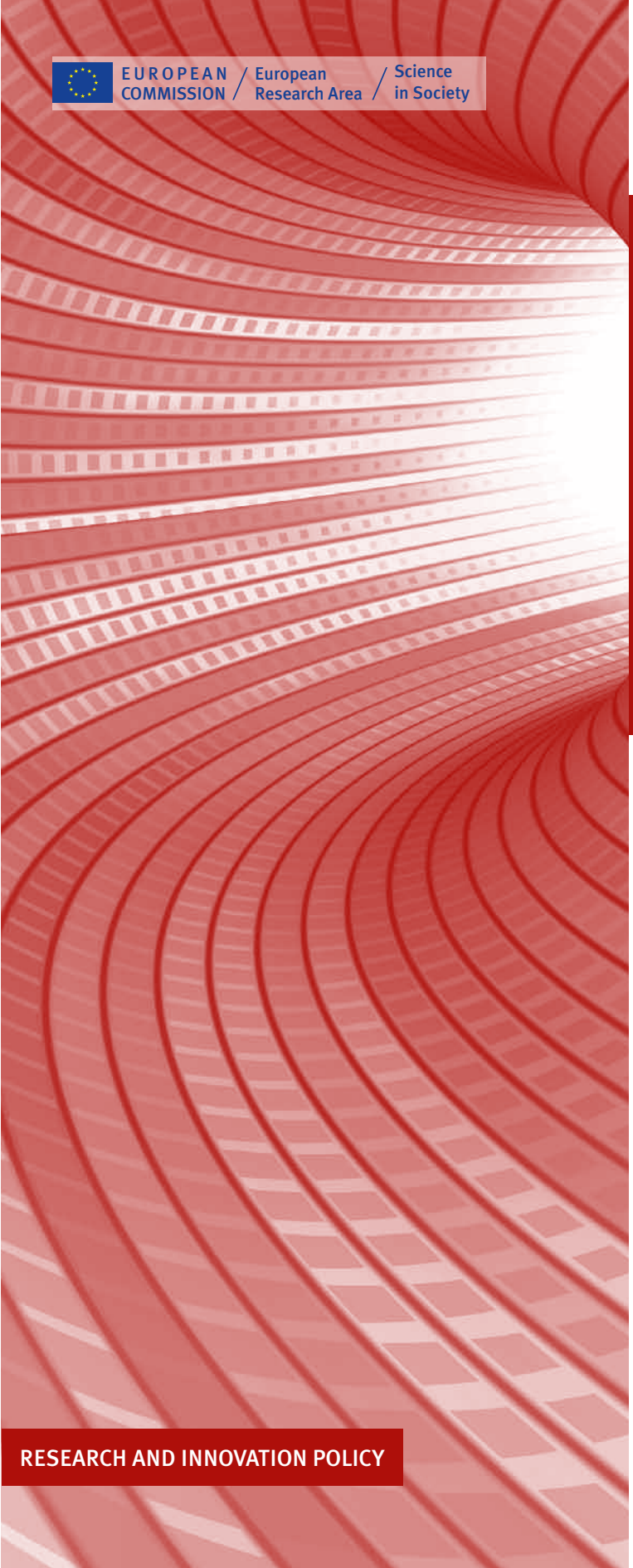
2011

Precaution and privacy impact assessments as modes towards risk management

David Wright
Raphael Gellert
Serge Gutwirth
Michael Friedewald



EUROPEAN COMMISSION / European Research Area / Science in Society

Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields

RESEARCH AND INNOVATION POLICY

EUROPE DIRECT is a service to help you find answers

to your questions about the European Union

Freephone number (*):

00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2011

ISBN 978-92-79-20404-3
doi 10.2777/58723

Printed in France

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

EUROPEAN COMMISSION

Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields

Edited by René von Schomberg[1]

A Report from the European Commission Services

1 Dr. René von Schomberg is based at DG Research and Innovation of the European Commission. This report is written for the publication series of the Ethics and Gender Unit of DG Research and Innovation. The views expressed here are those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.

2011 Directorate General for Research and Innovation

Table of contents

Acknowledgements by the editor

The contributions to this volume are based on presentations made at a workshop hosted by **the Scientific and Technological Assessment Unit of the European Parliament in November 2010**. I want to thank *Miklós Györffi*, who was instrumental in enabling the hosting of this successful event.

I also want to express my gratitude to the following Members of Parliament who addressed the workshop,

Mr Jorgo Chatzimarkakis, Member of the "Group of the Alliance of Liberals and Democrats for Europe"

Mrs Silvia-Adriana ȚICĂU, Member of the "Group of the Progressive Alliance of Socialists and Democrats"

I am gratefull the for various input to this workshop by the following colleagues of the European Comission

Francis Pēteris Svilans from the "Data protection" unit of DG Justice, *Maria-Eva Engdahl* from DG Enterprise and *Peteris Zilgalvis* from DG Information Society for responding to the various presentations

Prabhat Agarwal of DG Information Society, who addressed the workshop and who organised a workshop chaired by Director General *Robert Madelin* on *Future Technology and Society* on 19 November 2010. This workshop was also attended by most of the contributors to this volume. See:http://cordis.europa.eu/fp7/ict/fet-open/events-future-technology-and-society_en.html

Lino Paula of the Ethics and Gender Unit of DG Research and Innovation, who chaired a session of the workshop and who is project officer of the projects TECHNOLIFE and EFORTT.

Marie Cocquyt , Roya Kamran, Jolanta Klimczak-Morabito of the Ethics and Gender Unit of DG Research and Innovation for substantial technical, organisational and logistical support

Introduction: Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields

René von Schomberg[1]

1 Dr. René von Schomberg is based at DG Research and Innovation of the European Commission. This report is written for the publication series of the Ethics and Gender Unit of DG Research and Innovation. The views expressed here are those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.

Ethical frameworks for new and emerging fields of science and technology increasingly must address the issue of privacy and data protection issues. This topic emerges as a theme across various new technologies, such as information technology, security technology, biometrics, biomedical technology and the prospective applications of particular nano-technologies. At the same time, it is a relevant policy issue for various sectors, such as the health sector and justice and homeland security.

The consumer is also concerned, for *example* when confronted with Radio Frequency Identification Technologies (RFID) and surveillance technologies. New techniques, such as DNA research, smart cameras, data mining, etc., have made it easier than ever before to store and process large amounts of personal and sensitive information. The question arises whether the European citizen has sufficient knowledge of what information is stored for which purpose and for what period of time. Moreover, it is not evident that the citizen will have access to that information and, if appropriate, that he or she could modify this information.

Our privacy protection is guided in part by European legislation which predates the emergence of new technologies. Possibly, some technologies are developed in an uncertain legal environment. How can the Charter on Fundamental Rights, in which privacy and data protection is mentioned, serve as a basis for possible further legislative action in this field? The current overhaul of EU data protection law has to take this into account.

This book brings together early results of research and coordination projects funded under the European Commission funded Science in Society programme (FP7) which addresses the Research and Technology Development phase or the application phase of new technologies. These projects yield insights on how our understanding of privacy may change in the light of those technologies, and how privacy is weighed against other ethical values related to security and practical convenience. These research and coordination efforts usually do not address only single, particular technologies since the privacy issue will be shaped by the simultaneous use of various technologies and address relevant EC directives and national legislation.

Why Responsible Research and Innovation?

There is a significant time lag (this can be several decades) between the occurrence of technical inventions (or planned promising research) and the eventual marketing of products resulting from RTD and innovation processes. The societal impacts of scientific and technological advances are difficult to predict. Even major technological advances such as the use of the internet and the partial failure of the introduction of GMOs in Europe have not been anticipated by governing bodies.

At the same time, we are confronted with the Collingridge dilemma, implying that ethical issues could be easily addressed early on during technology design and development whereas in this initial stage the development of the technology is difficult to predict. Once the social and ethical consequences become clearer, the development of technology is often far advanced and its trajectory is difficult to change.

For new technologies to become accepted by society, they have to be aligned with societal needs and values. ICT generally has been very successful in delivering new processes and products that have been embraced by consumers. However, new generations of ICT technologies are more controversial, as their increased pervasiveness into people's daily life

and into the social infrastructure also raise a number of ethical, legal and social issues. Developments in areas such as biometrics (i.e. body scanners), telecare technologies and ambient intelligence raise questions regarding privacy, coercion and solidarity. These issues need to be assessed early on by policy makers, but expert assessment alone do not suffice. In order to optimally align innovation with societal needs and values, early engagement of producers with users and stakeholders is also of paramount importance. Both current innovation practises and expert assessment frameworks are in need of improved conditions for early communication and dialogue.

Defining Responsible Research and Innovation

The following working definition for Responsible Research and Innovation is proposed:

Responsible Research and Innovation is a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view on the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products(in order to allow a proper embedding of scientific and technological advances in our society)

Early societal intervention in the Research and Innovation process can help to avoid that technologies fail to embed in society and or help that their positive and negative impacts are better governed and exploited at a much earlier stage. I see two interrelated dimensions: the product dimension, capturing products and outcomes of research in terms of overarching and specific normative anchor points and a process dimension reflecting a deliberative democracy. The following normative anchor points should be reflected in the product dimension. They should be:

- *Ethically acceptable*: refers to a mandatory compliance with the fundamental values of the EU charter on fundamental rights [right for privacy etc] and the safety protection level set by the EU. This may sound obvious, but the implementing practice of ICT technologies has already demonstrated in various cases the neglectance of the fundamental right for privacy and data protection. It also refers to the "safety" of products and security of the citizens in terms of *acceptable* risks. It goes without saying that ongoing risk assessments is part of the procedure towards acceptable products when safety or security issues are concerned. Often, the risks related to new technologies, can neither be fully quantified nor a normative baseline of acceptability assumed by scientists as, if such a particular assumed baseline would represent *the* baseline of societal acceptance.
- *Sustainable*: contributing to the EU's objective of sustainable development. The EU follows the 1997 UN "definition" of sustainable development, consisting of economic, social and environmental dimension in their mutual dependency. This anchor point can become further materialised under the following overarching anchor point:
- *Socially desirable*:"socially desirable" captures the relevant, and more specific normative anchor points of the Treaty on the European Union, such as "Quality of life", "Equality among men and women" etc. It has to be noted that a systematic inclusion of these anchor points in product development and evaluation, would clearly go beyond simple market profitability, although the latter could be a precondition for the products' viability in market competitive economies. However, it would be consistent with the EU treaty to promote such product development through financing RTD actions. In other

words, at this point, Responsible Research and Innovation would not need any *new* policy guidelines, but simply would require a consistent application of the EU's fundamentals to the research and innovation process reflected in Treaty on the European Union[2]. Perhaps it has been wrongly assumed that these values could not considered in the context of research and innovation.

Product dimension:

Products be evaluated and designed with a view to their normative anchor points: high level of protection to the environment and human health, sustainability, and societal desirability

Deployment of Methods:

1. Use of Technology Assessment, Privacy Impact Assessment and Technology Foresight

In order to anticipate positive and negative impacts or, whenever possible, define desirable impacts of research and innovation both in terms of impact on consumers and communities. Setting of Research priorities with their anticipated impacts need to be subject to a societal review. This implies broadening the review of research proposals beyond scientific excellence and includes societal impacts[3]. Specific Technology Assessment methods also help to identify societal desirable product by addressing the normative anchor points throughout their development. Privacy impact Assessment address the particular normative anchor point of the fundamental right of privacy for EU citizens as specified in the EU charter for fundamental rights (*see especially the chapter 2 and 5*).The advantage is that Technology Assessment and Technology Foresight can reduce the human cost of trial and error and make advantage of a societal learning process of stakeholders and technical innovators. It creates a possibility for anticipatory governance. This should ultimately lead to products which are (more) societal robust.

2. Application of Precautionary Principle

The precautionary principle is embedded in EU law and applies especially within EU product authorization procedures (e.g. REACH, GMO directives etc). The precautionary principle works as an incentive to make safe and sustainable products and allow governmental bodies to intervene with Risk Management decisions (such as temporary licensing, case by case decision making etc) whenever necessary in order to avoid negative impacts.

---

2 Various top officials of the European Institutions refer to common European values for promoting particular public policies. It seems to me that this could also be applied the type of Research outcomes we wish to achieve with European Public Funds. Note the following quotes: «The defence of human rights and a justice system based on the full respect of human dignity is a key part of our shared European values" Jerzy Buzek, European Parliament President (10 October, 2009); "Europe is a community of Values". Van Rompuy, First European Council President, 19 November 2009;»My political guidelines for the Commission's next mandate stress the idea that Europe's actions must be based on its values".,President Barroso, European values in the new global governance, 14 October 2009

3 The Netherlands Organisation for Scientific Research (NWO) has developed a research funding programme on Responsible Innovation under which research proposals are subject to a review in terms of societal relevance. See: http://www.nwo.nl/nwohome.nsf/pages/NWOA_7E2EZG_Eng

The responsible development of new technologies must be viewed in its historical context. Some governance principles have been inherited from previous cases: this is particularly notable for the application of the precautionary principle. This principle is firmly embedded in European policy, and is enshrined in the 1992 Maastricht Treaty as one of the three principles upon which all environmental policy is based. It has been progressively applied to other fields of policy, including food safety, trade and research. It can also be of relevance for the development of ICT and security technologies (*see chapter 5)*

3. Use of demonstration projects: moving from risk to innovation governance

These projects should bring together actors from industry, civil society and research to jointly define an implementation plan for the responsible development of a particular product to be developed within a specific research/innovation field, such as information and communication technology or nanotechnology. Responsible innovation should be materialised in terms of the research and innovation process as well as in terms of (product) outcomes. The advantage is that actors can not exclusively focus on particular aspects (for instance, civil society organization addressing only the risk aspects) but have to take a position on the innovation process as such. Thus allowing a process to go beyond risk governance and move to innovation governance. The development of privacy-enhancing technology by industry in cooperation with users reflects such a shift in focus.

Process dimension

The challenge is to arrive at a more responsive, adaptive and integrated management of the innovation process. A multidisciplinary approach with the involvement of stakeholders and other interested parties should lead to an inclusive innovation process whereby technical innovators become responsive to societal needs and societal actors become co-responsible for the innovation process by a constructive input in terms of defining societal desirable products.

Deployment of Methods

1. Deployment of Codes of Conduct for Research and Innovation: organizing collective co-responsibility

Codes of Conduct in contrast with regulatory interventions allow a constructive steering of the innovation process. It enables the establishment of a proactive scientific community which identifies and reports to public authorities on risks and benefits in an early stage. Codes of Conduct are particular useful when risks are uncertain and when there is uncertain ground for legislative action. Codes of Conduct can also allocate tasks to actors in the field and thereby promoting a context of co-responsibility among developers and users of new technologies. (*See chapter 7)*

2. Ensuring market accountability: Use of Standards, Certification and accreditation schemes and labels

The adoption of standards and even "definitions" are fundamental requirements to allow for a responsible development. Lawrence Bush[4] notes that the use of standards,

4 L.Bush (2010). «Standards, Law and Governance» in Journal of Rural Social Sciences 25 (3), pp56-78

certifications and accreditations constitute a new form of governance which progressively has replaced and transmuted positive law, as a product of the state, with its market equivalent. Although this form of governance is in need of improvement, we unavoidably have to make productive use of it, as the flood of products and processes coming on to the market will not be manageable through governmental bodies and agencies alone. Yet, the perception and working practice of these standards is significant. In 2005, it was claimed that the EU had forced local authorities to remove see-saws from children's playgrounds. No such EU measures were taken. Some standards were set by the European Committee for Standardisation (CEN), a voluntary organisation made of national standards bodies. CEN sought to limit the height from which children could fall, by specifying the maximum height for seats and stands, and by setting standards for hand supports and footrests. Manufacturers could choose to follow these standards, which carried the advantage of being able to export across Europe, instead of having to apply for certification in each country[5]. (European Communities, 2006).

The area of data- and privacy protection in the context of the use of ICT and security technologies should also be impacted by forms of self-regulation and standard setting. Data controllers based at operators need to provide accountability, which can be termed as a form of verifiable responsibility (*see chapter 6*). Crucial will be the involvement of third parties which can implement, minimally, a transparent verification practice. The introduction of a European Privacy Seal would also make a difference (*see chapter 2*)

3. Ethics as a "Design" factor of Technology

Ethics should not be seen as being only a constraint of technological advances. Incorporating ethical principles in the design process of technology can lead to well accepted technological advances. For instance, in Europe, the employment of Body Imaging Technology at Airports has raised constitutional concerns in Germany. It has been questioned whether the introduction is proportional to the objectives being pursued. The introduction of a "smart meter" at the homes of people in the Netherlands to allow for detection of and optimalisation of energy use, was rejected on privacy grounds, as it might have allowed third parties to monitor whether people are actually in their homes. These concerns could have been avoided if societal actors had been involved in the design of technology early on. "Privacy by design" has become a good counter example in the field of ICT by which technology is designed with a view to taking privacy into account as a design principle of the technology itself. Yet, practicing it is still rare. The project ETICA has recommended the introduction of specific governance structures for emerging (ICT) technologies.(*See chapter 1*)

4. Deliberative mechanisms for allowing feedback with policymakers: devise models for responsible governance

Continuous feedback from information from Technology Assessment, Technology Foresight, Privacy Impact Assessments and demonstration projects to policy makers could allow for a productive innovation cycle.

---

5 This example is adopted from: European Communities (2006) Better Regulation. Simply explained, Luxembourg: Office for Official Publications of the European Communities, 2006

Models of responsible governance have to be devised which allocate roles of responsibility to all actors involved in the innovation process. Ideally, this should lead to a situation in which actors can resolve conflicts among each other without the need for governmental interference. Co-reponsibility implies here that actors have to become mutually responsive, thus companies adopting a perspective going beyond immediate market competiveness and NGOs adopting a constructive role in the development of new technologies. More research is needed to devise normative models of governance (*see chapter 3)*

5. Public debate: Moderating "Policy Pull" and "Technology Push"

On-going public debate and monitoring public opinion is needed for the legitimacy of research funding and particular scientific and technological advance. Continuous public platforms should replace one-off public engagement activities with a particular technology and, ideally, a link with the policy process should be established. The function of public debate in viable democracies includes enabling policy makers to exercise agenda and priority setting. Public debate, ideally, should have a moderating impact on the "Technology Push" and "Policy Pull" of new technologies. Technology push has occurred in the European Union in the past when operators tried to accomplish a *fait accompli* with the market introduction of genetically modified soya in the mid 1990s. Environmental groups, notably Greenpeace who did not react to GMOs as an environmental concern prior to their introduction on the market, responded with an outright rejection. Technology push as a product-acceptance strategy does not work. At the other extreme, we can notice a strong policy pull concerning the introduction of security technologies such as the use of biometrics for passports, asylum applications and whole body image technology ("body scanners") at airports. Politicians and policy makers have been eager to accept and promote the implementation of these technologies, sometimes beyond their technical feasibility. Impact Assessments should consist of a proportionality analysis. Such an analysis should identify whether particular measures or potential infringement of privacy and data protection are proportional with a view to possible legitimate objectives for implementing security technologies. However, both "technical safety" and the determination of proportionality cannot be fully left to scientists or, in case of proportionality, to legal experts. Both cases assume normative baselines for acceptable risks or acceptable infringements of privacy rights. These baselines should be subject to public debate.The case for a deliberative approach is made in *chapter 4*

Figure 1: Overview on features of responsible research and innovation

Features of responsible research and innovation	
Product dimension: addressing normative anchor points	**Process dimension: deliberative democracy**
Institutionalisation of Technology Assessment and Foresight	Use of Code of Conducts
Application of the precautionary principle; ongoing risk assessment; ongoing monitoring	Ensuring market accountability: Use of Standards, Certification schemes, Labels
Use of demonstration projects: from risk to innovation governance	Ethics as a design principle for technology
	Normative models for governance
	Ongoing Public debate: Moderating «Policy Pull and Technology Push»

Outline of the book

Bernd Carsten Stahl describes in the first chapter of this book the way in which ethical issues are currently addressed in ICT research. He argues that there is a mismatch between the ethical issues one can reasonably predict and the ways currently used to address them. The paper concludes by outlining the recommendations that the ETICA project has developed and mapping them to the concept of responsible innovation. This will show how the ETICA project and its findings can contribute to a more responsible approach to innovation

Early societal intervention in the Research and Innovation process can help to avoid that technologies fail to embed in society and or help that their positive and negative impacts are better governed and exploited at a much earlier stage. Therefore, in the case of ICT and Security Technologies with a view on privacy and data protection, *Walter Peissl*, makes the argument in Chapter 2 that it is cheaper to decide on the fundamental design earlier in the process rather than applying end-of-pipe solutions to ensure that a product or service complies with legal requirements or to gain acceptance on the market. He develops his case on the basis of his involvement in the two European projects PRISE und EuroPriSe.

Chapter 3 takes us into a more fundamental reflection on the ethical basis of possible ways of governance of ICT technologies. *Stephen Rainey and Philippe Goujon* give an outline of a normative epistemological basis for governance and argue that current technology governance suffers from too many ad-hoc approaches.

In chapter 4, *Kjetil Rommetveit* makes the case that responsible innovation in Information and Communication Technologies should be accomplished through the establishment of broad, Europe-wide platforms for deliberation and inclusion of citizens and civil society. He draws on the TECHNOLIFE project which addresses among other the case of biometric technology.

David Wright et al develop in chapter 5 a specific mode for risk governance by applying the precautionary principle and developing an outline for privacy impact assessment informed by the PRESCIENT project.

Daniel Guagnin, Leon Hempel and Carla Ilten reflect in chapter 6, inspired by early findings of the PATS project, on the importance of the accountability principle for the implementation of EU data protection law. They argue that the principle of accountability can be seen as a bridge between privacy and practice. Such a bridge is necessary as they diagnose a gap between the theory and law of data protection and the actual practice.

Codes of Conduct for Research can function as useful tools in the context of a responsible research and innovation. *Zaharya Menevidis, Samantha Swartzman and Efstratios Stylianidis* taking into account the early findings of the ETHICAL project make in chapter 7 recommendations for a code of conduct and implementation measures for FP7 researchers with this report on data collection, use and retention in medical and biometric applications

In Chapter 8, *Aharon Hauptman, Yair Sharan and Tal Soffer* take a foresight perspective and see that privacy is progressively challenged by more intrusive technologies. Informed by early results from the PRACTIS project, they identify major trends. They give special attention to the understanding of privacy perception among adolescents, informed by a Europe wide survey.

In Chapter 9, *Maggie Mort, Celia Roberts, Christine Milligan* find that the introduction of telecare technologies is infused with ethical issues and that these technology may well reorder social relations. Based on the EFORTT project, they suggest that if it is to make a positive contribution to the lives of older people and those who care for and about them, and then it must be carefully and inclusively designed and integrated into wider policy.

In ANNEX I, *Emilio Mordini* reviews whole body imaging technology with a view to inform policy based on the work accomplished in the context of the projects HIDE and RISE and should be read as a *policy brief*. Regarding the EU Charter for Fundamental Rights as a general framework for guidance for the introduction of this technology, he recommends EU policy makers that respect for the primacy of the human person and attention to his or her needs are the leading principles to be followed in the establishment of aviation security. Emilio Mordini and the partners from RISE and HIDE further recommends, among other, that the European Commission should propose a specific framework for detection, profiling, and identification technologies for aviation security whereby the operating procedure should be subject to a public, democratic scrutiny.

CHAPTER 1
IT for a Better Future. How to integrate ethics, politics and innovation

Bernd Carsten Stahl

Introduction

One can frequently hear stories about changes in the way we live caused by information and communication technologies (ICTs). One can frequently hear references to an information "revolution" which would seem to imply that such technologies fundamentally change the way we live (Floridi, 2007). The revolution metaphor is taken up and intensified by commercial interest, which emphasise the significance of changes of consumer products. Personal lives become more variable in some respects but also more constrained as more choices are offered and communication is increased.

The changes in technology and their consequences for social and individual lives can be of significant ethical relevance. This means that policy makers who want to take their role as representatives of the people seriously are well advised to think about what those ethical implications might be. This is particularly true on the European level where the Union is often described as a community of values. It would be desirable to embed these ethical values into technology and ensure that they are considered during all stages of the technology life cycle. At the same time, there is the well-established problem that ethical issues could be easily addressed early on during technology design and development but not enough is known about technologies then. Once the social and ethical consequences become clearer, the development of technology is often far advanced and its trajectory is difficult to change (Collingridge, 1981).

The ETICA project (Ethical Issues of Emerging ICT Applications) contributes to this complex mix of views and events. The paper briefly describes the approach and rationale of the project. It uses the findings of the project to develop a larger picture of emerging ICTs as well as the ethical issues these are likely to raise. On this basis the paper then looks at the way in which ethical issues are currently addressed in ICT research. It argues that there is a mismatch between the ethical issues one can reasonably predict and the ways currently used to address them. The paper concludes by outlining the recommendations that the ETICA project has developed and mapping them to the concept of responsible innovation. This will show how the ETICA project and its findings can contribute to a more responsible approach to innovation.

Emerging ICTs

It may be too obvious to state, but in order to avoid misunderstandings, it may nevertheless be necessary to underline that we do not know the future. The future is fundamentally characterised by being unknown and unknowable. But, of course, things do not stop there. Humans' desire to know the future is probably as old as humanity. In addition, there are reasons to believe that some aspects of the future are predictable and, in fact, much of the organisation of societies is based on this predictability of the future. Commercial and administrative activities rely on recurrence of activities and usually rightly so. And to some degree this predictability extends to technologies.

It is not the purpose of this paper to go into much depth into some of the conceptual and epistemological issues that research on emerging ICTs raises. This was done in more depth elsewhere (Stahl et al., 2011). It is nevertheless important to give a brief definition of what is meant by the term "technology" in the context of the ETICA project. A technology in the ETICA sense of the word is a high level system that affects the way humans interact with

the world. This means that one technology in most cases can comprise numerous artefacts and be applied in many different situations. It needs to be associated with a vision that embodies specific views of humans and their role in the world.

A final preparatory statement is in order to delineate the claims that can be made by ETICA in the light of the uncertainty of the future. The best way of understanding the ETICA project and to provide a framework for interpreting its findings and recommendations is to see it as a technology foresight project (Martin, 2010). The idea is to move away from the idea of one determined future to a multiplicity of possible futures. A main purpose of this type of research is to explore possible futures with a view to identifying and selecting desirable ones that can then be pursued. As a final step, decisions can be made today that influence the outcome of the future options. The aim of foresight activities is not to describe one true future but to enlarge the choice and opportunities, to set priorities and to assess impacts and chances, and work towards a shared view of a desirable future (Cuhls, 2003, p. 98).

Identification of Emerging ICTs

In order to develop an understanding of the ethics of emerging ICTs and develop policy recommendations, the ETICA project started by identifying emerging technologies. This was done via a distributed discourse analysis of publications on emerging ICTs. The sources used in this activity were either governmental / funding sources or publications emanating from research institutions. The justification of this approach is that governmental and funding bodies have a strong impact on research agendas and can shape future research. Research institutions, on the other hand, undertake the research and know what is currently happening in research laboratory. Together, these two types of entities are therefore well placed to assess which research in ICT is currently happening and to which outcomes it is expected to lead in the medium term future, in 10 to 15 years.

The discourse analysis was undertaken using a grid of analysis that was developed by the ETICA consortium through a series of theoretical considerations and pilot data analysis exercises. It is important to understand that the analytical grid is not exclusively theory-led but emerged inductively from the data. The rules of analysis were not defined a priori but emerged from the engagement with texts and were then collectively inscribed in the analytical grid and its subsequent implementation in a bespoke online database. This grid of analysis is represented in the following figure.

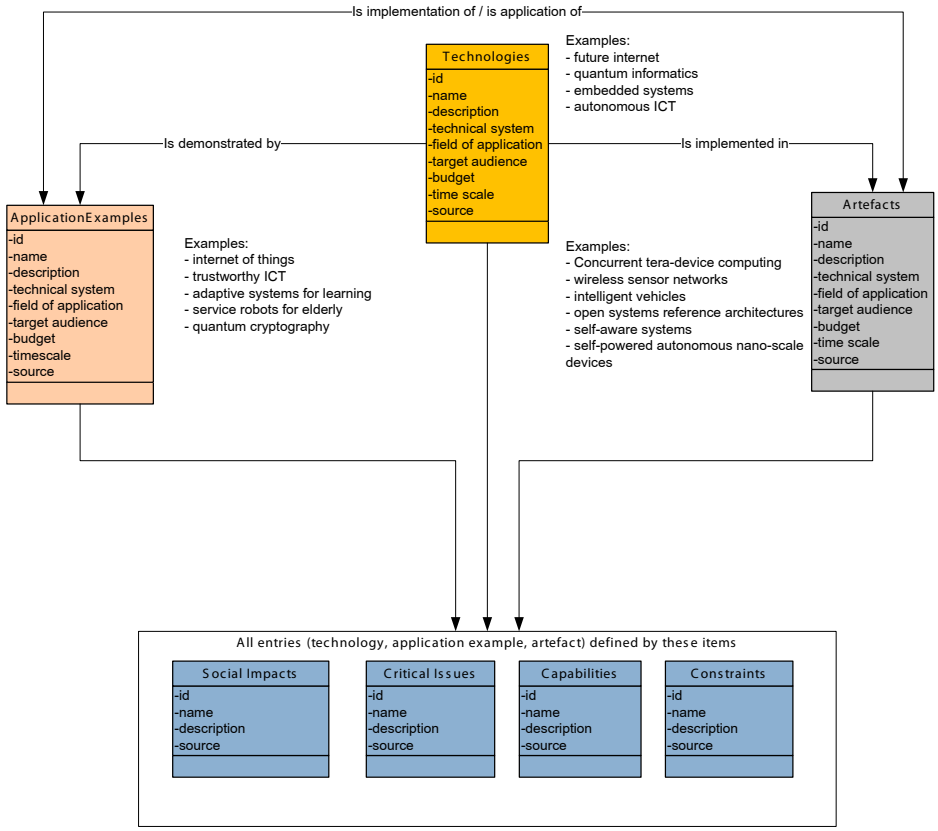


Figure 1: Analytical grid for discourse analysis

The consortium analysed 27 different documents worth analysing. The criteria for identifying and including documents were that they had to belong to one of discourses of interest to the research, they had to clearly discuss emerging ICTs, this discussion had to be sufficiently detailed to allow the collection of relevant detail about the technology and they had to be accessible to the consortium. Data collection was stopped when theoretical saturation was reached, i.e. when no more new items were identified.

The analysis of the texts led to the identification of 107 technologies and 70 applications. A more detailed look at the lists revealed that there was considerable overlap. It was therefore decided to group the technologies, applications and artefacts in a way that would correspond with the earlier definition of technology as a high-level and abstract concept that is sensitive to the way humans interact with the world. The aim was to identify those technologies that are at a high level of abstractness and that would cover the applications, artefacts and contributing technologies.

The initial list of 107 technologies was regrouped, ordered and categorised to allow the most important high level technologies to remain, whereas component technologies were subsumed into these high level technologies. This left a list of about 20 technologies.

Several rounds of discussion among project team members and consultation with external experts followed. These external experts were individuals who were knowledgeable in the individual technologies listed below. They were not members of the consortium and did not receive any remuneration for their involvement. Their main task was to critically review the descriptions of the technologies in order to ensure that these descriptions did not contain factual inaccuracies. During discussion within the consortium and with the external experts further technologies were eliminated because they were perceived to be applications rather than technologies, did not offer an insight in the underlying vision of the relationship of humans and the world or because they fell outside the ICT remit of the study. The end result of this process was the following list of technologies:

Affective Computing
Ambient Intelligence
Artificial Intelligence
Bioelectronics
Cloud Computing
Future Internet
Human-machine symbiosis
Neuroelectronics
Quantum Computing
Robotics
Virtual / Augmented Reality

Table 1: List of emerging ICTs

It is important to recapitulate what this list of emerging ICTs represents. It is the result of an analysis of two interlinked discourses on emerging technologies. The paper's claim is that these are reasonable and robustly determined candidates of ICTs that are likely to have significantly increasing social impact in the next 10 to 15 years. They are thus a good guess of what the future holds in stock and they serve the purpose of reflecting on which futures they will facilitate and which consequences this might require at present.

Shared Features of Emerging ICTs

For each of the technologies identified, the ETICA consortium developed a more detailed description that followed this structure:

- History of the technology and concepts
- Approximately 5 application examples
- Defining features of the technology
- Critical issues, i.e. ethical, legal questions; capabilities and constraints.

Space constraints preclude a recapitulation of justification and approach taken as well as a detailed description of these features. All relevant details are published on the project website www.etica-project.eu. It is important in the context of the current paper to briefly outline what the larger social implications of these technologies are likely to be. In order to develop a better understanding of these more general social implications, all features of all technologies were collected in a mind map. Each technology was represented as a node in this map. The node of affective computing, to take an example, would therefore look as follows:

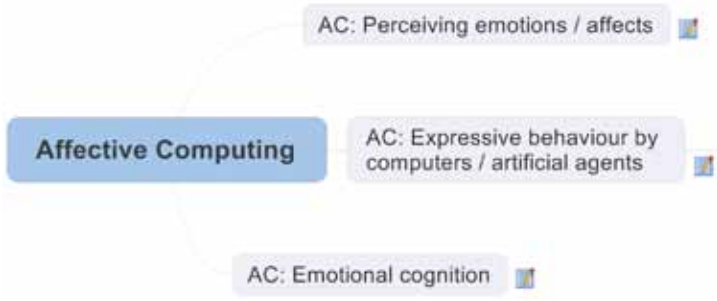


Figure 2: mind map of "affective computing"

Clicking on the notepad icon would reveal the full text description of the technology in question. For the first point, for example, this would read:

"Perceiving emotions / affects i.e. sensing of physiological correlates of affect). The principle here is that humans send signals that allow others to infer the agent's emotional state. Such emotional cues may be with the agent's control, such as tone of voice, posture or facial expression. They may also be outside the agent's control as in the case of facial colour (blushing), heart rate or breathing. Humans are normally aware of such emotional cues and react easily to them. Most current technology does not react to such emotional cues even though they are part of the illocutionary and perlocutionary function of a speech act."

This was done for all technologies, producing the following mind map:

Figure 3: Defining features of emerging ICTs

This overview was then used to regroup the defining features from individual technologies to more general social consequences or shared assumptions about humans and society they betrayed. The aim of this type of data analysis was to provide an insight into shared predictable consequences of these different technologies, which would allow for a broader description of the way a future society modelled on or involving these technologies would look like.

To pre-empt predictable but unnecessary criticism, we need to state that we are aware of the possible downsides of this approach. It uncritically accepts descriptions and features of technologies that are still under development. It abstracts from real uses and environments without considering the possible role of human agency, be it in strengthening, changing or resisting the different technologies and their consequences. Furthermore, it regroups features without deeper regard of the nature of the different technologies, which may lead to combinations of technologies that will never occur.

It is therefore important to reiterate what this categorisation is meant to represent, namely a view of current discourses on emerging technologies. These discourses are important in that they shape perceptions but also infrastructures and funding that will be used to promote the futures implied in them. Figure 4: Social and socio-technical implications of emerging ICTs should be understood as the attempt to graphically represent dominant discourses. Doing so helps us understand the content of expected technologies as well as their implications, which, in turn, is a condition of engaging in any attempt to change them.

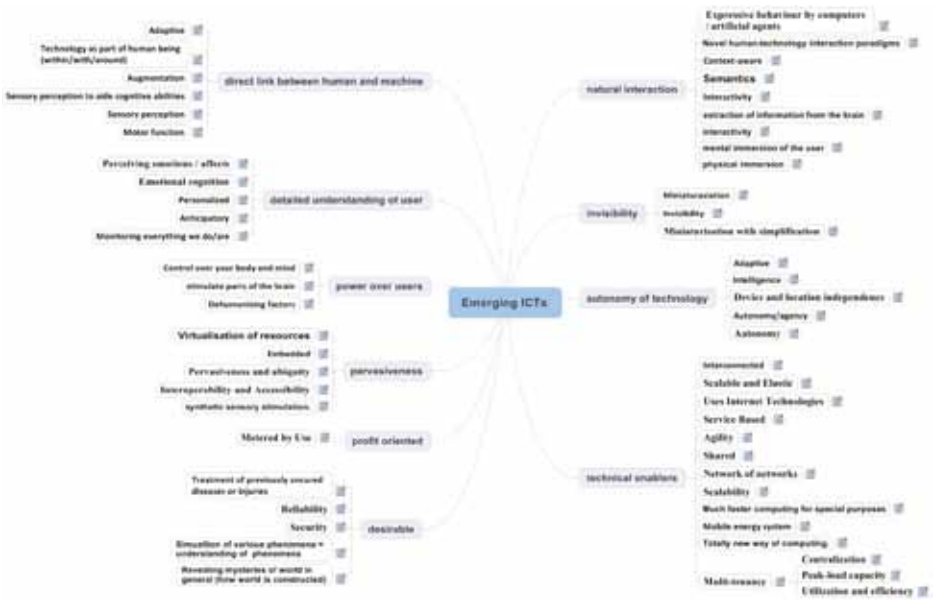


Figure 4: Social and socio-technical implications of emerging ICTs

Social Consequences of Emerging ICTs

Figure 4, above, deserves a closer look and interpretation. This section will therefore briefly explore each of the main term and spells out its relevance and meaning.

Natural interaction is core to many of the emerging ICTs. The idea behind it is to move away from specialist ways of interacting with technical devices such as mice, keyboards or screens to engaging with them in ways that users are more familiar with. The technologies use a number of ways of gathering information about the user which can be intentionally given information but also contextual information or personal information that the user may not even be aware of (as, for example, emotional states). The user will in many cases not even notice that she or he is interacting with technology which is deeply embedded in the user's environment.

One recurring aspect of this natural interaction is the invisibility of the technology. Technical artefacts recede to the background making it easy to forget their presence and interacting with users in numerous ways. A further aspect of the interaction is the direct link between humans and technology. This can either be physically implemented, as in the case of implants which can be inserted inside users' bodies and even brains. In many cases the direct link is less intrusive, for example when the technology continuously surveils the user. This direct link is not only an input device of technology but often has the purpose of supporting and strengthening the user and in particular those aspect of the user that are viewed as problematic. Technologies are described as adaptive and augmenting, giving users' greater reach of their natural faculties.

This direct link implies that the technology has a detailed understanding of the user whose needs, wants and preferences need to be modelled and interpreted correctly for the augmentation and direct link to be successful. This means that bodily, cognitive and emotional models of the users need to be embedded, which refers back to the natural and invisible interface between user and technology. In order for this to be possible the technology needs to be pervasive, i.e. embedded in a wide range of environments for the user to be able to profit.

As a consequence the technology will gain a significant degree of power over the user who will need to rely on the technology and embedded models to achieve the chores that technology is meant to help her or him with. In extreme cases, for example in neurocomputing, a direct link between the technology and the human brain can control not only people's actions but even their thoughts. But even in less intrusive cases, the technology can easily determine and circumscribe avenues of activity.

This power is linked to autonomy of the technology, which will be relied upon to make numerous decisions and act proactively in order to achieve its functions. The technology therefore needs to be context sensitive, mobile and intelligent. It correctly interprets the user's situation and acts accordingly.

It is important to note that as a general point the different technologies under investigation are described as positive and desirable in their use and consequences. They will allow a better understanding of all sorts of natural and social phenomena. Their aim is to help and support users, in particular in those cases where they find it hard to fend for themselves, e.g. in cases of disability or disease. In the above figure, several defining features of different technologies were collected under the heading of "technical enablers". These are aspects of the technologies that are deemed to be necessary to fulfil the functions of the technologies. For space reasons these are not investigated in more detail here, even though this would doubtlessly be an interesting further task. We will finish this brief attempt to outline the main socio-technical consequences of the emerging ICTs and move towards a reflection of the assumptions, beliefs and models that underlie them.

Ethical Consequences of emerging ICTs

While the general social consequences of emerging ICTs clearly point towards some ethical issues, a more detailed analysis of ethical issues was required in order to develop useful recommendations. This paper briefly describes the methodology used by ETICA, presents findings and synthesises them.

Identification of Ethical Issues[1]

Research on ethics generally raises numerous conceptual questions, which are exacerbated by the application to emerging technologies. Moor (2008), for example, suggests that we need better ethics for emerging technologies. This raises the question of the

1 For a more detailed description of approach and findings, please refer to deliverable D.2.2, Normative Issues Report, available from the ETICA website at www.etica-project.eu.

choice and justification of the ethical approach taken. Just as most technologies have a potential infinity of possible applications and thus a potential infinity of moral problems, there is now a huge number of ethical evaluations to contend with. One possible approach would be to decide on a particular ethical approach that is widely accepted, such as the mid-level ethical principles generally used in biomedical ethics (Beauchamp & Childress, 2008). This would leave open the question of the relationship to other ethical views and might lead to blind spots where the chosen ethical theory is not well developed.

The ETICA project therefore decided to take a pluralist approach that allows a number of different voices to be heard. This plurality, while running the risk of inconsistency, has the advantage of covering a broad range of issues and views and offering different interpretations. It was therefore decided to concentrate on the discourse of ICT ethics and, in the first instance, extract this field's views on the ethics of the emerging technologies. The chosen approach for ethical analysis thus mirrors the approach used in the technology identification part in that it relies on published work and thereby seeks to minimise injecting the researchers' biases into the analysis. This section first defines the field and then describes how it has been analysed to allow the identification of ethical issues.

The actual identification of the ethical issues of the emerging technologies identified earlier used several interrelated steps. It started with a bibliometric analysis of the discourse on computer and information ethics from 2003 to 2009. It used a bibliometric tool called VOSviewer (van Eck & Waltman, 2009; Van Eck & Waltman, 2006; Van Eck, Waltman, & van den Berg, 2005). This bibliometric analysis gave a heuristic starting point for possible ethical issues worth considering. It then used the descriptions of technologies as compiled in the earlier steps to explore whether any of the defining features of the technologies was likely to raise ethical issues. Similarly, the application examples were investigated with a view to their ethical relevance. For each technology an ethical analysis was created with the following structure: (1) discussion of defining features, (2) discussion of application examples, (3) bibliometrical analysis, and (4) concluding discussion.

Ethical Issues of Emerging ICTs

While the number and detail of ethical issues of the different ICTs varied depending on their level of progress and public visibility, the ethical analysis led to the identification of numerous issues. This paper lacks the space to discuss these issues individually but instead develops a general overview of these ethical issues. The methodology employed to do this mirrors the one described above for the social characteristics of emerging ICTs. A mind map was created that detailed all of the technologies and had one branch for each of the ethical issues identified. The full description of the ethical issue was available in the comment of the branch. The mind map tool allowed grouping the different ethical issues into more general categories. This allowed the development of a more abstract view of the ethical issues that the emerging ICTs as a whole are likely to raise.

Figure 5 shows a view of the categories ethical issues that emerged from this analysis.

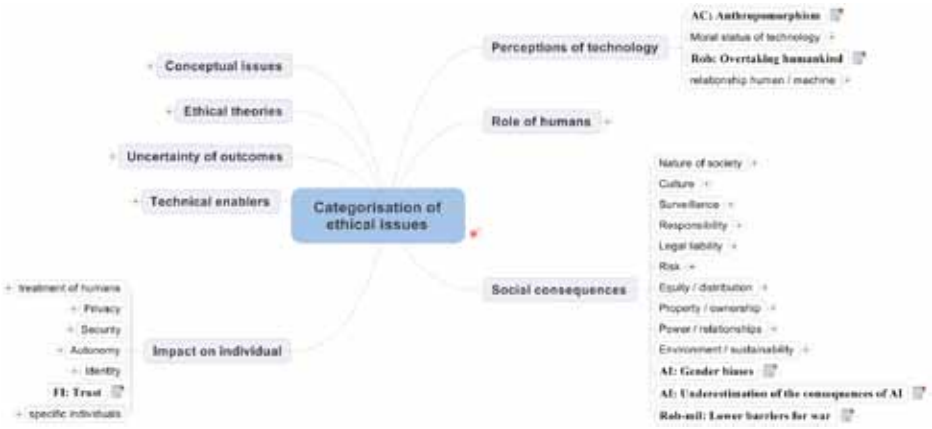


Figure 5: Categories of ethical issues of emerging ICTs

Looking these categories, one can find that some of them are not particularly surprising. Current problems are likely to persist in future ICTs. Notable examples are privacy, data protection and surveillance as well as issues of property, ownership and digital divides. While these problems will not disappear, they have been well recognised and there are institutions, norms and regulations that aim to address them.

It is important, however, to see that there are numerous ethical issues in the list above that are currently less visible and that we may not have good answers for. Many of these arise from the relationship of computers and humans and the consequences this relationship has on social interaction and society. Many of these issues also reflect the more general implications of ICT discussed earlier. One core issue has to do with the status of ICT and the way humans view themselves in relation to such technology. It is expected that ICT will continue to become more and more autonomous and less obvious in its interaction with humans. This raises the question of the agency of technology and thus of the moral status of machines. Numerous current examples of ICT research go in this direction, where ICT-enabled devices make autonomous decisions, for example in healthcare or search and rescue situations. These decisions will undoubtedly have moral qualities but it is unclear how they are to be evaluated.

As one consequence of this increasing autonomous agency of ICT, there is a possibility that our view of ourselves will change. Weizenbaum (1977) predicted this development more than three decades ago, but it may now become social reality. The impacts that emerging ICTs can have on the individual are thus far-reaching. They relate to the way we see and thus treat humans. Autonomous ICTs requires us to rethink our own autonomy and thus our identity. What this will mean in detail for society is not clear. It stands to reason, however, that the potentially fundamental changes arising from new technologies will not only create new risks, liabilities and responsibilities but may change the very fabric of society. Changes in the way we work, engage in political activities and leisure will raise questions about appropriate rules and regulations. They will create winners and losers and therefore lead to conflicts that need to be addressed.

Responsible Innovation for ICTs for a Better Future

This very quick overview of the ethical issues of emerging ICTs as identified by the ETICA project should render it clear that current technical developments have the advantage of significantly affecting the way we live. They will have positive and negative consequences and implications that should be addressed as early as possible. The main mechanism of integrating ethics into ICT research and development on the European level is that of ethics review. This mechanism relies heavily on bio-medical ethics. It has the advantage of providing clear guidance and precedence in some cases, notably those related to direct medical intervention. At the same time ethics review is structurally unable to address most of the more interesting issues outlined above. By relying on informed consent it focuses on the individual and neglects social changes. It is premised on the belief that the research itself is morally good and desirable, which may be true in many cases in medicine but is not obviously true in technical research. It is furthermore mechanistic and relies on an ethical issues list, which can give the misleading impression that ethics can be reduced to a pre-defined set of issues.

The concept of responsible innovation can therefore be interpreted as an attempt to provide a broader and more holistic framework in which ethical, social and legal issues can be addressed. It will most likely include established ethics review procedures but it needs to go beyond them. This section will contextualise ETICA findings and recommendations in a framework of responsible innovation by first outlining the concept of responsibility and then demonstrating how the ETICA recommendations will facilitate a more responsible approach to innovation.

The Concept of Responsibility

Responsibility can be defined as a social construct of ascription. Etymologically derived from the response, the answer, responsibility implies a communicative structure. This communication implies that there is something (the subject) that has the ability to answer. The subject needs to answer for something (the object) and it needs to answer to something (the authority) on the basis of a distinct set of rules or guidelines. There are numerous further conceptual aspects of responsibility ascriptions. There are different types of responsibility that affect the authority and the underlying rules. Moral responsibility (Wallace, 1998) differs from but is often related to legal responsibility (Hart, 1968), for example. Role responsibility tends to be related to both moral and legal. A further important aspect is the temporal dimension (prospective versus retrospective).

This paper does not have the space to develop a detailed theory of responsibility (for an overview see (Fischer, 1999), for an application to technology see (Lenk & Maring, 1991) and to information systems see (Stahl, 2004)). It only uses the main components of the concept of responsibility to explore how the findings of the ETICA project can be translated into practical recommendations that have relevance for the development of ICTs. In order to do this, two more remarks are important. First, we understand responsibility as an attempt to achieve socially desirable outcomes. This means that if responsibility is ascribed to a subject (e.g. a software developer, a company, a government) this implies that there will be positive or negative sanctions (i.e. rewards or punishments) that will contribute to a particular outcome, such as, for example, user involvement or less environmental impact. Second, it is important to realise that responsibility ascriptions always take place in concrete situations

and are always entangled in a complex web of different ascriptions. The individual software engineer, for example, will have responsibilities towards her company, role responsibilities as a member of a professional body, legal responsibility as a citizen, moral responsibility as a member of different communities etc. While it may be analytically desirable to disentangle these responsibilities, they always co-exist in practice.

Responsible Innovation and its Limits

Before this very brief background of the concept of responsibility, we can now ask what responsible innovation can mean. In the European context, the term needs to be interpreted taking the policy background into account. Europe needs economic growth to address many of the challenges that it is facing. However, growth needs to be conducive to other policy aims. The President of the European Commission therefore states that Europe needs smart, sustainable and inclusive growth (European Commission, 2010). Innovation in science and technology is seen as a key enabler of these policy aims. ICTs form an important aspect of this strategy, as can be seen from the Digital Agenda for Europe[2]

The term "responsible innovation" represents the aim of using innovation in science and technology (and beyond) to achieve these policy aims. In accordance with the earlier discussion of the concept of responsibility, the term here stands for the aim to achieve desirable outcomes. Innovation is not seen as an aim in itself but a contributing factor to the overall good. Sustainability and social inclusion are two of the values that need to be considered in innovation.

Achieving such responsible innovation is a complex task. It entails the definition and enforcement of a large number of interlinking responsibility ascriptions. These will cover numerous subjects which will be held responsible for different objects, using different mechanisms and leading to different sanctions. This section briefly discusses some of the problems that responsibility ascriptions face in the area of emerging ICTs. Emerging ICTs are a core area of responsible innovation given the cross-cutting nature of such technologies and the strong influence they can have on innovation in other disciplines and across society as a whole.

For the sake of simplicity of the argument we will concentrate on the subject of responsibility for emerging ICTs. We distinguish two may sets of subjects: On the one hand there are policy makers who are responsible for the framework of responsibility. Their main responsibility is a type of higher level responsibility, something that could be called a meta-responsibility or a transcendental responsibility. This is the responsibility for providing the conditions that facilitate specific responsibility ascriptions during the technology research and development process. On the other hand there are subjects involved in this process itself, such as companies, individual researchers or technicians, but also society at large and its representatives. These subjects will be responsible for individual technologies and their consequences in a range of different ways.

In the following sections the paper discusses the recommendations of the ETICA project and contextualises them in this framework of responsibility. It first outlines recommendations for policy makers and the for other subjects involved in the ICT innovation process.

2 http://ec.europa.eu/information_society/digital-agenda/index_en.htm, accessed 28.02.2011

Recommendations for policy makers

Policy makers have an important role to create the regulatory framework and the infrastructure to allow ethics to be considered in ICT. If emerging ICTs are to be developed in a responsible manner that allows identifying and addressing the social and ethical problems outlined above, then a framework and infrastructure for the development of responsibility needs to be provided. Such a framework should cover at least the following three main areas of policy activity:

- Provide regulatory framework which will support Ethical Impact Assessment for ICTs
- To raise awareness of the importance of ethics in new ICTs
- To encourage ethical reflexivity within ICT research and development
- To provide appropriate tools and methods to identify and address ethical issues
- To address the wide range of current and new ethical issues arising from ICT, modelled along the lines of environmental, privacy or equality impact assessments
- To allow ICT professionals to use their expertise in emerging ICTs to contribute to ethical solutions
- To raise awareness of ethical issues regarding animals and environmental issues
- To proactively consider legal solutions to foreseeable problems that will likely arise from the application of future and emerging technologies

Overall, this set of recommendations addresses the institutional framework that will be required for further subjects to recognise responsibilities and develop mechanisms of discharging it. The idea of an "Ethical Impact Assessment for ICTs" was chosen because it provides precedent from areas of the environment, privacy, or equality. Such a framework is required to provide incentives to engage with issues of responsibility in innovation and emerging ICTs. It will thereby encourage discourses that will lead to the development of specific responsibility ascriptions.

- Establish an ICT Ethics Observatory
- To collect and communicate the conceptual, methodological, procedural and substantive aspects of ICT ethics
- To provide a community-owned publicly accessible repository and dissemination tool of research on ICT ethics
- To give examples of approaches and governance structures that allow addressing ethical issues
- To disseminate past and current research ethics and ICT including relevant work packages and deliverables and relevant National Ethics Committee opinions
- To facilitate the Ethical Impact Assessment
- To provide an early warning mechanism for issues that may require legislation

While the first recommendation aimed at providing a procedural framework for identifying and addressing ethical issues in ICT, this set of recommendations aims to provide a set of content required for actual responsibility ascriptions. The work undertaken by the ETICA project, for example, provides important pointers towards possible ethical issues to be considered. Individuals involved in technical development are often not experts in these matters. A shared repository of ethics-related theories, practices, methodologies etc. is a necessary condition for the successful ascriptions of responsibilities and the related sharing of good practice.

- Establish a forum for stakeholder involvement
- To allow and encourage civil society and its representations, industry, NGOs and other stakeholders to exchange ideas and express their views
- To exchange experience between to develop ethical reflexivity in the discussion
- To reach consensus concerning good practice in the area of ethics and ICT
- To build a bridge between civil society and policy makers

This final recommendation for policy makers points to the necessity of institutionalising important discourses that allow civil society and other stakeholders to engage on a content level with the policy as well as the technical community. Such a forum is required to ensure that responsible innovation covers not only specific technical interests and perspectives but is allowed to reflect broader societal concerns. In terms of a theory of responsibility, the forum contributes to the definition of the object of responsibility: what is it that should be achieved and what does responsibility need to be ascribed for?

Recommendations for Industry and Researchers and CSOs

Industry, researchers and other individuals or organisations should adhere to the following recommendations in order to be proactive and allow innovation to be socially responsible. If the institutional framework, background, repository and societal discourses are there, then the conditions will be favourable for the incorporation of ethics and reflexivity into technical work and application usage.

- Incorporate ethics into ICT research and development
- To make explicit that ethical sensitivity is in the interest of ICT users and providers
- To distinguish between law and ethics and see that following legal requirements is not always sufficient to address ethical issues
- To engage in discussion of what constitutes ethical issues and be open to incorporation of gender, environmental and other issues
- The points of this recommendation aim to ensure that specific responsibility ascriptions are realised within technical work. It furthermore aims to sensitise possible subjects of responsibility some of the difficulties of discharging their responsibilities
- Facilitate ethical reflexivity in ICT projects and practice
- To realise that ethical issues are context-dependent and need specific attention of individuals with local knowledge and understanding
- To simultaneously consider the identification of ethical issues and their resolutions
- To be open about the description of the project and its ethical issues
- To encourage broader stakeholder engagement in the identification and resolution of ethical questions.

This final set of suggestions aims to ensure that the different subjects of responsibility realise that responsibility is not a pre-determined and fixed structure. Possible objects of responsibility are context-dependent and need to be interpreted in the particular situation. Interpretive flexibility of technology requires the participants in a technology development project to collectively engage in the initial definition of ethical issues to consider, but also to continuously review this initial definition and engaging with stakeholders involved in other stages of the technology development process.

Conclusion

This paper has outlined the main approach and findings of the ETICA project. It has given an abstract view of the social consequences and ethical implications of the technologies that were identified as emerging ICTs. It has then shown how these findings and the subsequent recommendations can contribute to an environment of responsible innovation.

Following these recommendations will allow for an early and pro-active engagement with ethics in future ICTs. While this cannot be a guarantee that all problems will be identified and solved, it is an important step towards ensuring that technology development is conducive to social ends.

The recommendations are also not the final step in the journey. If they are recognised as important and implemented then this will lead to numerous follow-on questions. Which form exactly should the institutional framework for Ethical Impact Assessments take? How is the ICT Ethics Observatory to be created and maintained? What form will the stakeholder forum take? How can the introduction of reflexivity into projects and organisations be realised and assessed? All of these are difficulty questions requiring further research.

For the moment, ETICA has shown that there are important ethical issues that we can expect to arise from emerging ICTs and that we currently do not have a good way of addressing them. This paper has outlined the main recommendations coming from the project and shown how they fit into the approach of responsible innovation. Implementing these recommendations will contribute to an approach to research and development of technology that is not only technically excellent but sensitive to ethical issues and thus contributes to the greater good of Europe and beyond.

Acknowledgements

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° [230318].

The author acknowledges the contribution of the members of the consortium without whom this paper could not have been written.

References

Beauchamp, T. L., & Childress, J. F. (2008). Principles of Biomedical Ethics (6th ed.). OUP USA.

Collingridge, D. (1981). The Social Control of Technology. Palgrave Macmillan.

Cuhls, K. (2003). From forecasting to foresight processes - new participative foresight activities in Germany. Journal of Forecasting, 22(2-3), 93-111. doi:10.1002/for.848

van Eck, N. J., & Waltman, L. (2009). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 1–16.

European Commission. (2010). COM(2010) 2020: Europe 2020 - A strategy for smart, sustainable and inclusive growth. Retrieved from http://ec.europa.eu/eu2020/

Fischer, J. M. (1999). Recent Work on Moral Responsibility. Ethics, 110(1), 93 - 139.

Floridi, L. (2007). A Look into the Future Impact of ICT on Our Lives. The Information Society, 23(1), 59-64.

Hart, H. L. A. (1968). Punishment and Responsibility: Essays in the Philosophy of Law. Oxford: Clarendon Press.

Lenk, H., & Maring, M. (Eds.). (1991). Technikverantwortung. Güterabwägung - Risikobewertung - Verhaltenskodizes. Frankfurt, New York: Campus Verlag GmbH.

Martin, B. R. (2010). The origins of the concept of ‚foresight' in science and technology: An insider's perspective. Technological Forecasting and Social Change, In Press, Corrected Proof. doi:10.1016/j.techfore.2010.06.009

Moor, J. H. (2008). Why we need better ethics for emerging technologies. In J. V. D. Hoven & J.

Weckert (Eds.), Information Technology and Moral Philosophy (pp. 26-39). Cambridge: Cambridge University Press.

Stahl, B. (2004). Responsible Management of Information Systems. Hershey, PA: IGI Publishing.

Stahl, B. C., Heersmink, R., Goujon, P., Flick, C., van den Hoven, J., Wakunuma, K., Ikonen, V., et al. (2011). Identifying the Ethics of Emerging Information and Communication Technologies: An Essay on Issues, Concepts and Method. International Journal of Technoethics.

Van Eck, N. J., & Waltman, L. (2006). VOS: a new method for visualizing similarities between objects. In Advances in Data Analysis: Proceedings of the 30th Annual Conference of the German Classification Society, Studies in Classification, Data Analysis, and Knowledge Organization (pp. 299–306).

Van Eck, N. J., Waltman, L., & van den Berg, J. (2005). A novel algorithm for visualizing concept associations. In Database and Expert Systems Applications, 2005. Proceedings. Sixteenth International Workshop on (pp. 405–409).

Wallace, R. J. (1998). Responsibility and the Moral Sentiments. Cambridge, Mass: Harvard University Press.

Weizenbaum, J. (1977). Computer Power and Human Reason: From Judgement to Calculation (New edition.). W.H.Freeman & Co Ltd.

CHAPTER 2
Responsible research and innovation in ICT: The case of privacy

Walter Peissl

Introduction

The broad use of information and communication technologies (ICTs) in almost every part of daily life produces a huge amount of data. Personal data of the user or of people involved constitute a major part of the data stored and processed. They reveal a lot about the users' behaviour and help creating a picture of people's personal lifestyles. Data stem from economic enterprises as well as from state surveillance systems, and together they manifest a threat to privacy. These new threats can no longer be dealt with by legal means alone; rather, interdisciplinarity is the key word. Since the erosion of privacy is a fundamental problem for liberal democracies, we need combined efforts and a common understanding of the value of privacy among engineers, political and social scientists and decision-makers in private enterprises as well as in the public domain. To take these considerations into account is to be considered part and parcel of responsible research and innovation; therefore, we have to develop new ways to secure privacy in a networked world.

This bookcontribution will present new approaches to incorporate privacy-oriented thinking and PETs[1] principles early into the design-process. The starting point is the idea that even in data protection it is cheaper to decide on the fundamental design earlier in the process rather than applying end-of-pipe solutions to ensure that a product or service complies with legal requirements or to gain acceptance on the market. These approaches will be discussed along with the results from two recent research projects ITA was involved in: PRISE[2] und EuroPriSe[3].

TA and Privacy

According to von Schomberg (in this book), technology assessment is a relevant method in the product dimension of Responsible Research and Innovation (RRI). Presenting two recent research projects of the Institute of Technology Assessment (ITA) of the Austrian Academy of Sciences, this paper shows how technology assessment can feed into RRI processes. Before going into detail I will give a short overview over the Institute and TA in general.

The Institute of Technology Assessment of the Austrian Academy of Sciences (ITA) is an interdisciplinary research institution that investigates the relationship of technology and society and especially is interested in the impacts on society of the widespread use of new technology. The institute's work is devoted to academic analysis as well as to policy advice in technology-related issues. One of the main areas of work is to analyse the impacts of new ICT applications on society. Important areas of work are privacy, e-governance and networked environments. Apart from the focus on the information society, ITA deals with technology and sustainability as well as with the governance of controversial technologies such as biotechnology, nanotechnology and new emerging technologies for human enhancement.

Technology assessment is an interdisciplinary concept, which provides policy advice for technology and research policy. The potential impacts of technology use are analysed in

1 Privacy Enhancing Technologies (PETs)

2 http://prise.oeaw.ac.at

3 https://www.european-privacy-seal.eu/

several dimensions and, if possible, alternatives are described. Technology assessment is always pro-active and constructive in contributing solutions to societal problems. Technology assessment was first established in the USA as an independent and impartial instrument of policy advice for the Senate in the early 70s of the 20th century. Today in Europe, 18 TA institutions work for their respective regional or national parliaments. These parliamentary technology assessment institutions are organised within EPTA[4]. On the European level, the STOA Panel[5] serves the European Parliament. The STOA secretariat is supported by members of the European Technology Assessment Group (ETAG)[6].

In TA we distinguish between different basic approaches: a) technology induced studies analyse potential impacts of the broad implementation of certain technologies and their potential alternatives; b) problem induced approaches focus on societal problems and search for technological or organisational solutions for the problems found; c) project oriented approaches focus on impacts of concrete projects like energy-plants.

With regard to privacy we use a problem-oriented approach based on empirical evidence for the erosion of the fundamental right to privacy due to the widespread use of ICT facilitates (vgl. Tichy/Peissl 2001; Klüver 2006; Peissl 2007; Sterbik-Lamina et al. 2009). Studies in this domain try to find technological, organisational or legal measures to halt the ongoing erosion of privacy. In addition, we investigate how technological and societal developments as described later may change our attitudes towards privacy.

Technological and societal developments

Over the last decades, three lines of development characterised the technological progress in the domain of ICT. Rendering everything digital resulted in a qualitative change, making many applications possible and revolutionising others. The digitisation of analogue communication systems enabled and accelerated the convergence of information- and communication systems. At the same time, privacy became an important issue. The technological development necessitated the implementation of further measures in order to keep up with legal requirements. For instance in old analogue telephone systems, the connection data disappeared with the end of the communication process. In digital systems, you have to save the addresses of all communication partners as a technical requirement. To comply with data protection rules, you have to design the system to include additional automatic erasure routines.

The second important line of development was *minimisation*. The computing power of 1970s' big machines is nowadays contained in tiny PDAs and smartphones. This is, of course, not the end of minimisation. Thinking of RFID tags[7] and the concept of the Internet of things (Commission of the European Communities 2009; ITU 2005) we see an ongoing development towards smaller or even irrecognisable devices. Minimisation, at the same

4 http://www.eptanetwork.org/EPTA/

5 http://www.europarl.europa.eu/stoa/default_en.htm

6 http://www.itas.fzk.de/etag

7 RFID: Radio Frequency IDentification

time, paved the way for decentralised computational power. Some of the early data protection laws in Europe (e. g. in Austria) are more or less based on the idea of securing data in a centrally locked computer centre. This is why modern data protection laws have to focus much more on the so-called informational self-determination. A centralistic concept of "data protection" no longer matches the conditions of modern decentralised data processing.

This development is accelerated by the third big technological line of development: *networking*. Establishing the universal Internet protocol (IP) actually enabled every user to be connected and to exchange data all over the world within seconds. This raised new challenges to data protection in a globalised world.

Summing up we may say that digitisation, minimisation and networking built a totally new framework for privacy policy.

However, not only technological developments contribute to the erosion of privacy. There are at least two other ambivalent developments in society. On the one hand we can see a higher sensibility for data protection issues, which basically popped up in public debate after huge data losses occurred in several European countries. On the other hand, we face a new trend in communication. In web 2.0 applications or so-called social media platforms millions of users share information rather unscrupulously even on a very private level. Social scientists increasingly become interested in the long-term impacts of such a behaviour (see Sterbik-Lamina et al. 2009; Klüver 2006).

Developments after the terrorist attacks in New York, London and Madrid were even more important. Globally, we recognised a hype of surveillance demands to prevent future terrorist attacks – surveillance mostly served as a synonym for security. As an over-reaction, this entailed new regulation that endangered privacy (see Peissl 2005). Recent studies demonstrated that security and privacy are not necessarily a zero sum game (Raguse et al. 2008).

This short overview on technological and societal developments shows how endangered the fundamental right of privacy is. Are there any ways to cope? Since in the future, technology design will play a more important role, the "Privacy by Design" approach by Cavoukian (2009) as well as the results of the PRISE project[8] can be considered important steps. In addition, it will be necessary to promote research and development and, in particular, to implement so-called Privacy Enhanhcing Technologies (PETs) (Klüver 2006).

The technological and societal developments, of course, need to be mirrored in a modern data protection directive, which is under discussion right now.

Hypotheses and solutions

In order to structure the discussion of possible ways to overcome the challenges to privacy, we present three hypotheses as starting points:

8 http://prise.oeaw.ac.at

Hypothesis 1: Privacy is a fundamental right. Today, it is jeopardised in various ways and can no longer be enforced by legal means alone. Reasons are the very low level of users' awareness of ICT and the lacking resources of data protection authorities (Cas/Peissl 2000; Cas et al. 2002; Klüver 2006; Sterbik-Lamina et al. 2009).

Hypothesis 2: Privacy increasingly is on the political agenda. Indicators may be found, on the one hand, in the media coverage of data-loss scandals around Europe, the low level of acceptance of the data-retention directive and the protests against its implementation in several European countries. On the other hand, the European Commission continues to issue calls for data protection research and to finance pilot projects like the EuroPriSe project. On a global level, there are developments to establish a kind of data-protection standard (Bennett/Raab 2003).

Hypothesis 3: Privacy often is seen as a cost factor only. The main line of argument is that data protection systems cost money and cannot be afforded in a globally competitive market.

It may be true that the adaptations needed to make an IT system comply with data protection regulation or to gain acceptance on the market are rather costly. However, in contrast to this end-of-pipe approach, we argue that the "privacy by design" approach is more cost-efficient. Early implementing privacy-oriented thinking in the design process does not cost much and "built-in-privacy" is an added quality feature of the respective IT product. As success in global markets is no longer solely dependent on competitive pricing, "privacy" as a new quality feature is a comparative advantage for those who include it at an early stage. The success of the data protection seals in Schleswig-Holstein[9] and the European Privacy Seal may serve as an indication how successful this kind of thinking already is[10].

Summing up, privacy should be seen as a quality feature of IT products and services; and privacy can no longer be guaranteed by legal means alone. Therefore, pro-active and constructive approaches are necessary. Two such approaches will be presented in the following chapters: first, the "engineer-oriented" approach takes up standards and guidelines from IT security and enhances them by catering for the privacy dimension. The aim is to incorporate privacy know-how as early as possible into the design process. Secondly, the "market-oriented" approach stands for self-regulation, audit schemes and quality seals.

The PRISE Approach

The PRISE project aimed at defining criteria for privacy-friendly security technology research funded by the EC in the framework of PASR[11]. The PRISE approach shows how privacy can be designed into security technologies, and how privacy considerations can be operationalised within the research and development process and the deployment phase of a security product.

9 https://www.datenschutzzentrum.de

10 https://www.european-privacy-seal.eu

11 Preparatory Action on Security Research

By applying this evaluation procedure produced for Framework Programme 7, certain generalizations can be made. The method selected was a combination of classic expert Technology Assessments featuring the analysis of literature and documents, together with participative approaches.

The participative approaches had two components: on the one hand, two stakeholder workshops were held with representatives of industry, science, and users of security technologies to discuss the research design and provisional results. The other component comprised so-called "Interview meetings"[12] carried out in six European countries[13]. The main purpose was to stimulate an "informed debate" on the subject with approximately 160 participants and to discover their basic views, in particular lines of argument, and to determine how these might be changed. During the preparation the participants were introduced to several scenarios on the subject. After an introductory talk, the participants were asked to fill in a comprehensive questionnaire. Using a list of questions, the subject was subsequently discussed in small groups.

The results showed a high level of consensus among the non-specialist groups in all countries. Among the key statements made, for example, was that a threat from terrorism does not justify an infringement of privacy, that technologies invading the very private (intimate) sphere are unacceptable, and that the abuse of security technologies ought to be prevented. Of special relevance – as a distinguishing feature between countries – was the degree of trust people had in various institutions. The independent judiciary, in particular, enjoys a high degree of public confidence, which was also reflected in the list of values participants considered to improve acceptance of security technologies. Top of the list was the principle of proportionality, which would only appear to be assured if certain supervisory measures were legally permitted subject to strict checks. The fear of possible abuse was indicated by the demand for strict controls, and by the emphasis people placed on security technologies infringing privacy being implemented as a last resort only. More generally, an informative and open debate on the subject was called for, which should involve as many concerned groups as possible, as well as an obligatory analysis of the implementation effects of such technologies (see Jacobi/Holst 2008).

The key result of PRISE is the so-called PRISE matrix. It is an evaluation instrument for measuring the expected effects of a new security technology in three stages. The three stages investigated are the so-called *baseline of personal life*, which comprises very personal – intimate – data and which, as a matter of principle, should be free from any surveillance. The second area is about *data protection compliance*, i.e. how already existing principles are applied, and the third area deals with *context-sensitive trade-offs*. The latter area examines whether a security technology apparently infringing privacy justifiably promises a sufficient security gain.

There are several evaluation stages in the course of designing a system or evaluating a project. If the initial evaluation of the project idea renders the conclusion that the first or second area is not catered for satisfactorily, there is a package of measures contributing to alleviating a recognised privacy problem, as summarised in the so-called PRISE

12 A short description of interview meetings can be found on the website of the Danish Board of Technology: http://www.tekno.dk/subpage.php3?article=1234&toppic=kategori12&language=uk

13 Denmark, Norway, Germany, Spain, Hungary and Austria

Handbook. Three types of instruments are available – legal, technical and organisational –, which are also described in the report (Raguse et al. 2008).

Using the matrix together with two checklists, which enable a quick evaluation to be made, an attempt was made to develop guidelines and support for product proposing enterprises, for evaluators, and for research and development teams in general. The PRISE matrix and the PRISE Handbook can, however, also provide users of security technologies with valuable information on an ICT use that complies with basic law and enhances privacy.

Taken together, it was possible to show that security and privacy do not necessarily exclude each other and that it is possible to endorse both at the same time, provided design principles are appropriately complied with..

The PRISE results were presented at an international conference, where representatives of the security technology industry, users, NGOs and representatives from the scientific community discussed them. The conference concluded with the presentation of a Statement Paper[14], summarising the project team's and its international advisory committee's main results in terms of recommendations for action and policy options.

The Statement Paper contains the following conclusions and recommendations: i) An inviolable *baseline of privacy* needs to be established. ii) There is no linear, interchangeable relationship between privacy and security, and the relationship between them is *not a zero-sum game*. iii) Minimising the processing of personal data is an important principle of data protection. iv) *The consolidation of databases* in order to analyse the behaviour of the entire population breaches the principle of the presumption of innocence and the principle of proportionality. v) The protection of privacy is the shared responsibility of all involved, and observance of *privacy should be a key non-functional requirement* of security technologies. vi) In addition, the *criteria* for evaluating security technologies must be *continuously developed* and regulations should be introduced for a limited time and continuously reassessed (see as 2008).

The European Privacy Seal

After the description of the "engineer-oriented" approach we now present a brief description of the "market-oriented" approach, based on the example of the EuroPriSe project[15], which focuses on conditions for introducing a European Privacy Seal. Such a privacy quality seal is intended to certify "that an IT product or IT based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection, taking into account the legislation in the pilot countries." (Bock 2009)

The project had several aims. Firstly, it was concerned with a market analysis, which was intended to assess the extent to which a European privacy seal might be viable on its own without subsidies from certification fees, and whether it would be able to succeed in the market. The second aim was to promote awareness of data protection issues

14 http://prise.oeaw.ac.at/docs/PRISE_Statement_Paper.pdf

15 https://www.european-privacy-seal.eu

among manufacturers. The most challenging theoretical task was to develop criteria for evaluating data protection friendliness at a European level. EU Directive 95/46 already provides a standard framework for data protection legislation, but member states vary widely in interpreting it. The project succeeded in establishing a common set of criteria based on the European framework (Bock et al. 2009). It also undertook to collect existing experience regarding the European certification of products and services and European admission criteria for the relevant experts.

The specific aims of the seal are to promote data protection per se, to improve consumer trust in IT products and services, to contribute to greater transparency in data processing and to demonstrate theoretically and empirically a possible competitive advantage for products complying with data protection, carried out using the ROSI model – Return on Security Investment (Borking 2009). In addition, EuroPriSe aimed to simplify the certification procedure for businesses interested in data protection, since a certification recognised throughout Europe would abolish multiple certification requirements, rendering immediate effects.

The certification procedure is largely based on the privacy seal the Independent Centre for Privacy Protection Schleswig-Holstein (ICPP/ULD) established in 2002. The procedure comprises two stages, which are voluntary in principle but regulated by law. In each case the manufacturer or vendor of a product and/or service to be certified selects a legal and a technical expert from a register of accredited experts. Together they agree the "Target of Evaluation" (ToE). At this stage, initial contact is made with the certification body to clarify the ToE. Subsequently, the two experts begin their independent evaluation of the product or service. Once the evaluation has been concluded the manufacturer submits the report to the certifying body, which carries out its own examination of the report. If the result of the examination is positive, the seal is awarded and a short report is published on the Seal Homepage. It is important that the entire procedure remains confidential, that no business secrets are contained in the published short report, and that any negative examination results are not made public.

The only costs incurred by the business enterprise are the fees for the two experts and the fee charged by the certifying body.

A key factor in this process is the criteria used in certification. The fundamental question is: can the product or service be designed so that its use will comply with data protection? This refers in particular to settings, configurations and also to the pertaining documentation. The European Privacy Seal particularly emphasises the combination of law and technology. The certification criteria have been worked out in great detail and are also published in a comprehensive catalogue (Bock et al. 2009). They basically follow the standard principles of data protection such as the legitimacy of data processing, purpose limitation, data subjects' rights, transparency and auditability, data minimisation and avoidance, as well as data security.

Ever since it was launched the project proved surprisingly popular with experts as well as with manufacturers. No fewer than 110 experts from ten countries attended the training seminars to be trained, examined and accredited. Austria currently has twelve experts. A total of 19 pilot certification processes had been initiated, which in the meantime have resulted in the award of 15 seals.

Conclusion

The starting point for this article was the question of how to manage responsible research and innovation with regard to ICT development and privacy. Based on the evidence that privacy protection can no longer be assured by legal means, attempts have been made to find alternative solutions. These have shown that (new) instruments for ensuring privacy protection do already exist. On the one hand, design-oriented assistance supports early compliance with data protection aspects in the design phase, involving only minimal additional costs. Fitting an IT system with PETs can qualify as a quality feature providing the product a competitive advantage, which is reflected in a positive Return-on-Investment (ROI). On the other hand, market-oriented mechanisms of self-regulation such as the Quality Seal can contribute to greater transparency on the market.

Particular responsibility falls to the policy-makers and those areas of public procurement that purchase large IT systems or are responsible for providing widely used IT applications. There is a particular potential in so-called "sensitive" areas such as, for example, security applications in the fight against crime, in e-government and, above all, in e-health.

Finally, the arguments and results discussed above are summarised in four messages:

1) Security and privacy do not not necessarily exclude each other; security technologies can often be designed in such a way that they fulfil their function and enhance security without, at the same time, infringing the fundamental right of privacy.
2) The debate about data protection and privacy thus far has been concerned with legalities almost exclusively. It now needs to be widened to include technical and social scientific aspects. This broader perspective has become necessary because of both, technological developments and changes in society. It would therefore appear helpful if, in future, we were to speak about privacy protection rather than "just" data protection.
3) The well trained and powerful statutory regulations in Europe are needed as a "support", but it would be insufficient to rely on them exclusively. We need to remember that statutory regulation only makes sense if it can be enforced. This means that data protection authorities need to be equipped with the technology and the legal resources required being able to adequately meet new challenges.
4) Additional instruments and incentives need to be used. These include the promotion of the "privacy by design" approach and the use of the PRISE matrix tools, of Privacy Impact Assessments (PIA) etc. This represents a key task for public procurement and funding agencies. Also, from today's perspective it is clear that there is a great potential for the implementation of self-regulation instruments such as, for example, data protection audits and quality seals. An additional and still too little funded public task is raising relevant awareness – including a debate of privacy issues and of the inalienable right to privacy at an early stage in schools –, which will play an important part in future privacy protection activities.

With a package of measures, an interdisciplinary approach and the appropriate political will at European as well as nation state level, it should be possible, in the future, to preserve the fundamental right of privacy so important for our democracies.

References

Bennett, C. J. und Raab, C. D., 2003, *The Governance of Privacy*, Aldershot, Hampshire GB: Ashgate.

Bock, K., 2009, *European privacy Seal – Final report*, im Auftrag von: European Commission – eTEN, Kiel: Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein (ULD, Independent Centre of Privacy Protection) <https://www.european-privacy-seal.eu/results/deliverables/Final%20Report>.

Bock, K., Meissner, S. und Storf, K., 2009, *Description of EuroPriSe Criteria and Procedures (updated Version 1.1)*, im Auftrag von: European Commission – eTEN, Kiel: Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein (ULD, Independent Centre of Privacy Protection) <https://www.european-privacy-seal.eu/results/deliverables/procedures>.

Borking, J. J., 2009, *The Business Case for PET and the EuroPrise Seal*: unveröff. Manuskript.

Čas, J., 2008, Privatsphäre und Sicherheit Ergebnisse aus dem europäischen TA-Projekt PRISE, *TECHNIKFOLGENABSCHÄTZUNG – Theorie und Praxis 17(3)*, 79-82 <http://www.itas.fzk.de/tatup/083/jcas08a.pdf>.

Čas, J. und Peissl, W. (Institut für Technikfolgen-Abschätzung und Österreichische Akademie der Wissenschaften), 2000, *Beeinträchtigung der Privatsphäre in Österreich – Datensammlungen über ÖsterreicherInnnen*, im Auftrag von: Bundeskammer für Arbeiter und Angestellte, Oktober 2000, Wien: Institut für Technikfolgen-Abschätzung, <http://www.oeaw.ac.at/ita/ebene5/d2-2a24a.pdf>.

Čas, J., Peissl, W. und Strohmaier, T., 2002, *Datenvermeidung in der Praxis – Individuelle und gesellschaftliche Verantwortung*, im Auftrag von: Bundeskammer für Arbeiter und Angestellte, Wien: Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften <http://www.oeaw.ac.at/ita/ebene5/d2-2a29.pdf>.

Cavoukian, A., 2009, *Privacy by Design ....take the challenge*, Toronto: Information and Privacy Commisioner of Ontario, Canada <http://www.privacybydesign.ca/pbdbook/PrivacybyDesignBook.pdf>.

Commission of the European Communities, 2009, *COM(2009) 278 final. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Internet of Things — An action plan for Europe*; Letzte Aktualisierung: Brussels, 18.6.2009 [Aufgerufen am: 2009-09-07 2009] Commission of the Euroepan Communities, <http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf>.

ITU, 2005, *IITU Internet Reports 2005: The Internet of Things - Executive Summary*; [Aufgerufen am: 2009-09-07 2009] International Telecommunications Union (ITU) <www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf>.

Jacobi, A. und Holst, M., 2008, *PRISE D5.8 Synthesis Report - Interview Meetings on Security Technology and Privacy*, im Auftrag von: European Commission PASR, Vienna: Institute of Technology Assessment Austrian Academy of Sciences, <http://prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf>.

Klüver, L., Peissl, W., Tennøe, T., Bütschi, D., Cas, J., Deboelpaep, R., Hafskjold, Ch., Leisner, I., Nath, Ch., J., Steyaert, St., Vouilloz, N.„ 2006, *ICT and Privacy in Europe – A report on different aspects of privacy based on studies made by EPTA members in 7 European countries*, 16 October 2006: EPTA <http://epub.oeaw.ac.at/ita/ita-projektberichte/e2-2a44.pdf>.

Peissl, W., 2005, Überwachung und Sicherheit – eine fragwürdige Beziehung, in: Nentwich, M. und Peissl, W. (Hg.): *Technikfolgenabschätzung in der österreichischen Praxis Festschrift für Gunther Tichy*, Wien: Verlag der Österreichischen Akademie der Wissenschaften, 73-90.

Peissl, W., 2007, Die Bedrohung von Privacy – ein grenzüberschreitendes Phänomen und seine Behandlung im Kontext internationaler Technikfolgenabschätzung, in: Bora, A., Bröchler, S. und Decker, M. (Hg.): *Technology Assessment in der Weltgesellschaft*, Berlin: Edition Sigma, 277-288.

Raguse, M., Meints, M., Langfeldt, O. und Walter Peissl, 2008, *D6.2 – Criteria for privacy enhancing security technologies, Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies* im Auftrag von: European Commission PASR, Vienna: Institute of Technology Assessment Austrian Academy of Sciences, <http://prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf>.

Sterbik-Lamina, J., Peissl, W. und Čas, J., 2009, *Privatsphäre 2.0 (Beeinträchtigung der Privatsphäre in Österreich; Neue Herausforderungen für den Datenschutz),*, im Auftrag von: Bundesarbeitskammer, Wien: Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften <http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a53.pdf>.

Tichy, G. und Peissl, W., 2001, Beeinträchtigung der Privatsphäre in der Informationsgesellschaft, in: Österreichische Juristenkommisssion (ÖJK) (Hg.): *Grundrechte in der Informationsgesellschaft – 24.-26. Mai Weißenbach am Attersee*, Wien: Neuer wissenschaftlicher Verlag, 22-48 <http://www.oeaw.ac.at/ita/ebene5/GTWPweissenbach.pdf>.

CHAPTER 3
Toward a Normative Ethical Governance of Technology. Contextual Pragmatism and Ethical Governance

Stephen Rainey and Philippe Goujon

Introduction

In highly functionally differentiated societies such as those we live in today, there is a tendency to presume that each sphere within society, be it economic, scientific, industrial etc. has an internal structure sufficient for its own development.[1] This includes a normative dimension. The terminology here is derived from 'systems theory'[2] which itself seeks to discover modules within social systems that effectively reproduce society over time. Though that theory takes many guises[3] and is not strictly adhered to here, nonetheless the concept of *functionally differentiated systems* can do some work.

To be clear, the notion of a functionally differentiated society is that the 'lifeworld' is the system wherein social actors act in the broadest sense (it is the world as it is known by them, within their horizons of action).[4] The lifeworld is itself reliant upon the functioning of various sub-systems. For instance, life in a consumer-capitalist society, the life wherein one can work, visit restaurants, parks, meet friends in public spaces etc. is regulated by economic transactions, legal provisions, business decisions and so on. These different systems' operations permit the patterns of possible life decisions (the going to work, restaurants, parks etc.). Moreover, as each performs a different function in determining or facilitating that pattern, they can be differentiated on that basis. The law certainly regulates the manner in which businesses can operate, for instance, but law and business are appreciably different. Moreover, each of these functionally different spheres of action has its own way of proceeding – in law we might see this in terms of politics, statute and precedent, whereas in business we might see this in terms of supply and demand. There is therefore a particular logic attaching to the outworkings of functionally differentiated spheres within societies.

The result of this latter thought is the presumption of an ethics internal to the different sectors of highly functionally differentiated societies – each would appear to contain *its own sources of normativity*. Hence we see legal ethics, business ethics, medical ethics, ethics of science and so on. Moreover, we tend to see these sectors as independent of one another. We see them in this way owing to the manner in which social actors comprehend the multiplicity of values as they appear in modern, highly differentiated societies. So we see in legal

1 See for instance, Habermas. J., 'The Uncoupling of System and Lifeworld' in Outhwaite, W, (ed.) *The Habermas Reader*, p.281

2 The core element of Luhmann's systems theory is communication. Social systems are systems of communication, and society is the most encompassing social system. A system is defined by a boundary between itself and its environment, dividing it from an infinitely complex exterior. The interior of the system is an area of less complexity. Social systems and psychical or personal systems operate by processing meaning. Different systems have distinctive identities that are reproduced in communication.

3 See Habermas *Op Cit*.

4 "In whatever way we may be conscious of the world as universal horizon, as coherent universe of existing objects, we, each 'I-the-man' and all of us together, belong to the world as living with one another in the world; and the world is our world, valid for our consciousness as existing precisely through this 'living together.' We, as living in wakeful world-consciousness, are constantly active on the basis of our passive having of the world... Obviously this is true not only for me, the individual ego; rather we, in living together, have the world pre-given in this together, belong, the world as world for all, pre-given with this ontic meaning... The we-subjectivity... [is] constantly functioning" Husserl, E, *Crisis of European Sciences*, 1936, p.108-109 Other definitions appear, but broadly connote the same things.

circles the acceptability of a lawyer arguing to win a case in which they know their client is guilty. Such a disregard for truth would be shunned in science, wherein a case for a theory would be expected to yield to emerging facts. More personally, we expect values held by individuals to be respected and tolerated even though they clash. Perhaps a religious position forbids abortion whereas a political position permits it, in the name of freedom (i.e. the religious person can refrain due to their beliefs if the freedom is there, but the pro-choice person cannot exercise their choice in a context of the practice's being banned).

For example, we could imagine a social setting wherein people greatly value their general privacy. So valuable is privacy to them that they seek its official protection. One can imagine at least two potential futures, for illustration's sake: one could see a programme enacted to erect cameras on every street corner (to catch snoopers) whereas in the other potential future, all cameras are banned (to prevent intrusion). We see here the norm of privacy, the motivation for action at all, being contextualised in directly opposing ways between the two futures. Each is a response to the dearly felt need to protect privacy. But 'privacy' in each is clearly differently construed.

The proliferation of cameras could be felt to be an invasion of privacy. The banning of cameras could be felt to be an impoverishment of freedom with respect to options available in private life.[5] Merely having a principle gives us nothing to go on when a concrete decision must be made. Clashes of this sort, between normative principle and value in the face of a decision can be seen as frequently occurring – abortion debates often see pro-life parties softening their line in particular cases (cases of rape or incest, for instance); animal rights activists may deplore in one sense certain practices such as bullfighting, yet recognise them as culturally relevant to a given people and so find them in another sense tolerable. What we see clearly is the split between contextualised norms (mediated in values) and the uncontextualised ethical norm. Moreover it is the latter which provides the impetus for acting on the former.

We must examine this notion further in order to establish a basis on which to understand practical ethics. We must get this as in its absence we have merely functional, *ad hoc* accounts of relativistic nature – 'you do your thing and I'll do mine'. In establishing a basis for practical ethics we can establish a basis for ethical governance.

Normative approach

The importance of a normative perspective is that it entails an *approach*, rather than a *mechanism*, so it seeks to deal with ethical issues as or before they arise in a principled manner rather than waiting until a problem surfaces and dealing with it in an *ad hoc* way. This is in order to incorporate a constitutive idea of what ethics is.

Ethics must condition emerging empirical conditions in order to ensure those conditions are ethical. Otherwise, should emerging empirical conditions be thought of as conditioning an ethical response, ethics is absent as possibilities for responses are circumscribed by non-ethical contingencies. A reactive ethics is inauthentic, it must

5 The example is an extreme oversimplification designed more to illustrate than define the problematic in any exhaustive sense, it should be noted

be pro-active. 'Hume's guillotine'[6] states that an 'ought' cannot be derived from an 'is', meaning matters of norms cannot be derived from matters of fact. Thus we would have an illegitimate process from an ethical point of view were we simply to amass empirical information and (statistically, maybe) prescribe or proscribe actions on that basis.

Such descriptive data require interpretation as the very nature of norms, values and contexts must be the material from which is spun an ethical approach to dealing with technology development. This is so owing to the fact that it is through engagements between contextualised actors that technological artefacts gain meanings, implications and possibilities. In short, it is via these means that their *relevance* is determined. It is also the case that once an issue is relevant, it may not remain so, and *vice versa*. The reason that taking relevance into account is important in terms of ethics is that relevance is keyed to how people conceive of their possibilities. An account of a person's possibilities, moreover, is keyed to their freedom. And freedom is a necessary component for the ethical, i.e. if someone is not free, they cannot be held responsible for what they do, and ethics doesn't enter the picture.

The steering function of a governance approach essentially involves utilising the perspectives of the people governed by it. In an instance of change, what is to change and what that change will mean are issues central to those set to undergo the change. Careful consideration is thus required of the *status quo* as experienced by the people, the level of disruption or disorientation likely brought about by the change (again from the people's perspective) and the likely ramifications from adopting the change. The perspective of the public is essential as it is they who are to be steered, and so it is things *as they are seen by the public* that are the object of enquiry. This is the case in instances of governance, but in ethical governance the inclusive imperative is (arguably) even more important as ethical challenges can represent challenges to modes of being for members of the public. The course of ethical governance is a sensitive one that must bear in mind issues that are of deep importance, including the Bourdieuian 'naturalised arbitrariness' and 'reframings' of Laws and Rein.[7]

Taking Perspectives Seriously

There are good reasons for taking seriously the testimony of social actors with regard to their positions, concerns and values in the face of change.[8] Epistemologically, if we listen to others we expand our sources of evidence. From even this merely aggregative perspective we improve our evidential base and so can gain more evidence, critical appraisal or new

6 Max Black refers the the Humean roots of the severance of value from fact as "Hume's Guillotine", based on David Hume's passage from *A Treatise on Human Nature*: "In every system of morality, which I have hitherto met with, I have always remark'd, that the author proceeds for some time in the ordinary ways of reasoning, and establishes the being of a God, or makes observations concerning human affairs; when all of a sudden I am surpriz'd to find, that instead of the usual copulations of propositions, *is*, and *is not*, I meet with no proposition that is not connected with an *ought*, or an *ought not*. This change is imperceptible; but is however, of the last consequence. For as this *ought*, or *ought not*, expresses some new relation or affirmation, 'tis necessary that it shou'd be observ'd and explain'd; and at the same time that a reason should be given; for what seems altogether inconceivable, how this new relation can be a deduction from others, which are entirely different from it." See Black, Max, "The Gap Between 'Is' and 'Should'", *The Philosophical Review*, Vol. 73, No. 2. (Apr., 1964), pp. 165-181.

7 Bourdieau, P, Bourdieu, P. *Outline of a Theory of Practice*, 1977, p.164. Laws and Rein, " Reframing Practice" in Hajer and Wagenaar, *Deliberative Policy Analysis* p.172

8 See Misak, C, *Truth, Politics and Morality*, pp124-5

perspectives upon the beliefs we have. If we harbour any desire to have good (reliable, true) knowledge, then the case for taking into account the views of others is fairly airtight on an epistemological front.

From a moral perspective there is a plain enough injunction to take seriously others' testimony about their perspective owing to basic respect. Others' experience of the world, though it is different in fact from one's own, is not different in principle. The deeply held values of another are as deeply held as one's own, even if in terms of content they are utterly opposed. If I take seriously my own deeply held view, as I likely do, then it would seem a contradiction in action to ride roughshod over those views as equally deeply held by the other.

Politically, it makes sense to take perspectives seriously from the simple fact that governance bodies that issue injunctions without a care for the perspectives of those to whom the injunction is to be addressed will likely see said injunction rejected or opposed. The will be a dearth of legitimacy should injunctions appear for the public as if from nowhere. Moreover, from a point of view of integrity, should a governance body fail to respect the views of those whom it purports to govern via steering, then it backslides to command/control policy-making. Failing to take perspectives seriously, then, is *beneath* governance.

The Foreseeable

It is in the light of possible changes to ways of life, established customs, self-conceptions etc. that ethical issues can arise from technological research and advance. This means that not only the changes in technology that can be predicted well by experts are of importance. The consequences of accepting the technological change into a way of life, its possibilities, ramifications, and so on, are where genuine ethical concern can arise for people. The technology expert alone is not likely to be well equipped to discern the relationship between a technological change and its every ramification in terms of a way of life. It is here that the perspectives of social actors are required as it is these perspectives that inform what a change in technology *means*. This capacity (or the will to develop it) cannot be presumed in any given researcher.

It's the reality of a technological change in a context of a public that these issues arise. And they arise precisely in terms of a question like: *what does this mean for our way of life?* The issues determined from the local perspective by those on the receiving end of a potential change of way of life resulting from a technological advance will be those that entail meaningful upheaval, or re-evaluations of established frames of reference. This is the picture as it is, because technological change is ongoing, with ethics done in a manner that is effectively *post hoc*, i.e. on the assumption of the reality of the change. In fact, ethics needs to precede development as contextual constraints relevant to ethical concerns are due to transversal ethical imperatives (the meaningfulness of an ethical concern is to do with the available context, but the impetus is a broader reference).[9] This means foresight is required. Without knowledge of future contexts, however, we need a grasp of how norms work *per se* so we dissolve the context-specificity problem. The current approach, rather, attempts to take present issues and subtract content, formalising them.

9 Part of human interest in general is the ethical. To allow *de facto* realities of context to bind ethics undercuts the ethical interest as it is the potential for future realities that need to be bound by ethics. In no other way can ethics be said to have been implemented in fact.

These mistakes are symptomatic of a domination of the sphere of ethical thought by a logic more suited to scientific reasoning, instrumental reason or argumentative discourse. We generally see in the reduction of context in the current approaches, a positivistic stance whereby ethical issue determination is thought to be deducible from putative 'facts of the matter'. These facts, moreover, are treated as if they determine ethical issues in an absolute manner – universally. This was the mentalist and schematising presupposition also present within the approaches. We also saw the default position of recourse to law and compliance in the ethical approaches. These facets lead to a reduction of ethics itself to law, sociology, expert advice and so on. In one notable case, ethics is reduced to adherence to scientific principles: "Research is only entirely ethical when it is dictated by rigorous scientific commitment."[10]

Consequently, there is an underlying issue with the notion of meaning embedded within the discourse regarding ethics in prevailing ethical governance approaches. What these findings mean from the perspective of the parties interested in the problems of governance and ethical governance in particular will now be examined as it will be from this basis that we can discover the effective problems *in situ* and thus establish a basis for alternative proposals.

The Problem of the Norm

As has been stated above, the multiplicity of sources of normativity in modern societies is a problem for governance. Rather than substantial rationality, pushing a dominant model, given plurality and the complexity of current social groups, the drive is to recognise networks running within a social group. Such a recognition permits the utilisation of the full resources of society in constructing a view of important social issues. It is also intended to cut across functional lines in modern societies. This ought to mean that a more fully representative and meaningful picture of society and its view on matters can be achieved: "... procedural, learning-based approaches are expected to resolve the dilemmas of governance because they are less likely than others to stiffen into models and more likely than others to prompt competing models to re-examine themselves so that they might learn from the others."[11]

Governance in general, having moved from a command/control structure, has an open question as to which source of normativity it can appeal.[12] In fact, owing to the separation between the sciences and the humanities, scientific rationality is often the *de facto* source of normativity in science and technology research.[13] The enlightenment attitude of emancipation through the use of reason is thus deformed into a rational sub-routine

10 Alperovitch, Annick Chairman of the CCNE's Technical Section, French National Consultative Ethics Committee for Health and Life Sciences. http://www.ccne-ethique.fr/upload/CCNE-brochure-GB_2008.pdf

11 De Schutter et al. 2001:25 referenced in Overdevest, «*The Open Method of Coordination, New Governance, and Learning : Towards a Research Agenda*.", http://wage.wisc.edu/uploads/Working%20Papers/overdev_open.pdf p.9

12 See for instance, Bohman, J, *Public Deliberation*, ch. 2

13 For a discussion of the issues here see Bijker, Bal, Hendriks, *The Paradox of Scientific Authority*, MIT Press, 2009

of instrumental intervention along the lines of decision-theoretic matrices. In a context of industrialised living, to which this sub-routine is particularly suited, the deformed rational procedure can prove highly effective. Thus there is a real difficulty in controlling or tempering the process, owing to its apparent effectiveness in a specific and dominant context of production and consumption. It is all too easy to equate this effectiveness within set boundaries as 'goodness', *simpliciter*.

What's required is an approach that can offer first criteria of evaluation and second a more interesting way to address the conditions not only for an ethical reflexivity, but also for determining the conditions of construction of ethical issues, of ethical norms, and the conditions for their adoption and implementation.

The Problem of Procedure

From the full resources of formal reason anything is possible; the issues deduced from the uncritically, tacitly employed presuppositions will be deduced *validly*.[14] But when the search for relevance is uncritically conditioned from the outset by a particular framing, it seems natural or logical to the individual that whatever set of valid issues they fix upon in their search is *the set* of valid issues. Moreover, given the uncritical nature of the framing, its unreflexive nature, access to means of construction of these issues (from the resources available to the individual) will remain closed off. Owing to the unrepresentative nature of the researcher or expert engaged in an investigation such as this, the idea that the public will understand, respect and adopt the normative injunctions required by the project. But it will be a validly argued-for, logically respectable opinion, from an expert – what could the problem be?

The idea that a discursive and rational procedure, mobilized in order to define the norm considered to be relevant in some given context, is capable by itself of taking account of all the possibilities of the social context to be regulated is at work here. Further, it is then presumed that this formal process will be gifted with the ability to choose, from the diversity of possibility, the right option for all. Finally, it is assumed that owing to its impeccable rational credentials, only the irrational could fail to see the value of the injunctions made.

But this is highly problematic. It ignores the fact that the concrete choice of a norm, even when judged relevant following a discursive process of reason, necessarily results from an operation of the selection of possibilities which is prior to it. This choice therefore depends on something other than the simple discursive operation of reason. The determination of possibilities, on the basis of which the discursive process will be able to check relevance, must be the object of a specific arrangement organising the reflexivity of the actors concerned. It cannot in effect be supposed that the capacities of these actors are such that they can by themselves, either spontaneously or through the effect of procedural constraints[15] reconstruct their context in order to identify the possibilities and subsequently submit them to the filter of relevance.

14 This point could be made in terms of logic alone – an inference might be valid, but not sound. Validity pertains to formally correct inference, soundness to formally correct *and actually true* inference.

15 As a Habermasian position might suggest

The reasons that we have to filter according to relevance, that is, those reasons we have to accept or refuse a proposition in any given discussion are not necessarily equal to the reasons why we accept or refuse those reasons (e.g. I could accept that astrology is predictive of my prospects, citing supposed past successes, but refuse to let failures of prediction dent my conviction, even though the rational structure is symmetrical. My reasons for refusing the reasons to reject astrology are based in something separate from my reasons to accept successes as verifications.) Understanding these reactions requires empathy more than formal logic – at play is the practical logic of the individual.[16]

Framing

Somewhere, reason runs out and the framing that constitutes a way of seeing the world steps in – the deep sense of self including all that one's convictions connote. One's being, in a thick sense that includes upbringing, cultural/religious convictions, feelings of indebtedness to a past, honouring legacies etc. While this is clearly important in comprehending who/what a person is, it is only comprehensible if we step back from the primarily argumentative mode of discourse (with its scientistic overtones) and regard framing not as an aggregative report of experiences had between various times, but rather as the authentic self-portrayal of a human being in terms of a life lived – i.e. we need to use a recognition principle in order to cognise the information encoded by the manner of framing.

Since the notion of framing at work here will only be relevant in terms of a life lived, via specific interpretations of life-events by an agent, an ethical dimension is required in order to comprehend it. The place of framing can be seen as illustrated by the following problem: In discourse ethics, when matters of justice arise and competing, contradictory arguments are aired, it is required that the parties involved will submit themselves to nothing but the force of the better argument. But the acceptance of arguments will itself be conditional on values embedded within an agent's way of seeing things. Thus, frames don't fit *within* argumentation, but rather argumentation *decentres* the expressive authenticity of the perspective from a frame. 'Decentring' means the way in which actors must move away from their own contexts of action when considering questions of what is true or right: "An absolute claim to validity has to be justifiable in ever wider forum, before an ever more competent and larger audience, against ever new objections. This intrinsic dynamic of argumentation, the progressive decentring of one's interpretative perspective, in particular drives practical discourse ...."[17]

16 More recently, Jean-Marc Ferry distinguishes four distinct types of rationality relevant to the human condition. His position is summarised as follows: "Historical and discursive progress from narration toward reconstruction is associated with increasing reflexivity about identity and the grounds upon which it is established. Narration, in Ferry's view, consists of ossified traditional myths which define identities in a more or less prescriptive, taken-for-granted way. Interpretation, on the other hand, involves the assimilation of identity to universal categories like law and justice and is exemplified in early Christian and ancient Greek thought. Argumentation opens up claims of identity to rational dialogue as embodied, for example, in the Enlightenment. Reconstruction, the final step toward reflexivity, involves hermeneutic attempts to understand the historical grounds behind the «good reasons» offered by others in argumentation. This is in part a logical and ethical consequence of the shift from it to you (acknowledging subjectivity) which emerges with argumentation itself." Smith, Philip, 'Les puissances de l'expérience' in, *Contemporary Sociology*, American Sociological Assoc., May 1994, vol. 23, number 3

17 Habermas, J. (2005) Truth and Justification, trans Fultner, B., Cambridge, MA: MIT Press p.109

This problematic of constructing norms in contexts (in order that we might determine and address ethical issues of emerging technology) requires that we look deep into the theory of normativity and action. Among the problems with current ethical governance efforts has been the consistent way in which the relations of norms to contexts are construed and the predominance of an argumentative conception of reason. Here, in the preponderance with one variety of rationality among others that engenders contextual reduction, we have a serious part of the theoretical problem. Thus we cannot avoid pursuing this line of analysis given we require a theoretically sound and efficient manner in which to address our central problem.

Theoretical treatments of problems

We have seen problematic instances so far wherein reason has been supposed to be sufficient both to justifying and applying rules. Contrary to this view is that wherein asymmetry is cited as the key feature between formal justifications and practical enactings. Asymmetry means that the social meaning of a norm is embedded as part of a system of significance not itself expressly predicated upon a formal conception of reason (hence the limits of all expert ethical assessment that presumes an Archimedean point of view.) Asymmetry suggests that reconstructions of the processes mobilized by the production of a norm mobilise two operations, which don't respond to the same conditions – the formal and the social. While the former may produce rigour, it is the latter that produces *meaning*. Meaning is ineliminable, naturally, as without it the purported addressees of a normative entreaty are denied access to the potential for understanding.

At this point, in attempting to describe the components of a solution to problems in governance, it will be essential to discuss the work of the 'Louvain school'.[18] Jacques Lenoble and Marc Maesschalck's *Toward a theory of Governance: the Action of Norms*[19] provides much of the basis for appreciating the problems of current governance approaches that we have developed here. Lenoble and Maesschalck attempt to address the deficiencies of governance approaches by paying close attention to the nature of norms in terms of their being enacted. Their concern is to formulate with rigour how reason is in fact enacted, in a manner which pays close attention to the perspectives of the addressees of norms. They address this via developing an account of how norms are apprehended by social actors. This provides promising material given the inadequacies of the paradigmatic approaches as we have outlined them here and in terms of the reasons sketched as to why perspectives are important.

18 We turn to the Louvain School as it is a prominent treatment of these problems that is well known at the European level. Moreover, much of the trajectory of the issues we have been pursuing are anticipated and deftly articulated in the work of Louvain. Their treatment is an analysis of the conditions for the possibility of norms in action. In order that we can address our problematic, which concerns the construction of an ethical norm in context, this deep theoretical material is essential. Were we to attempt to make practical suggestions regarding the construction of a norm in context without reference to the deep arguments concerning normativity in action, we would simply be suggesting *ad hoc* measures relevant to a narrow class of examples. This is what we are required to improve upon, in fact, and so it is impossible not to engage with these deep, detailed and influential theoretical treatments.

19 Lenoble, J & Maesschalck, M, *Toward a Theory of Governance: The Action of Norms*, Kluwer Law International. This deliverable doesn't pretend to be either a full exposition of every detail of the Louvain School's approach, nor does it claim to offer a complete critical appraisal of it. Rather, we raise and address issues of relevance to our argument using relevant resources from the Louvain approach.

For the Louvain approach, this means that judgments (including norms) can only be applied and produce a meaning, and therefore can only affect reality at the end of a complex operation which is an exchange between the effects expected by the abstract norm on the one hand, and on the other the effects rendered possible by the coherences specific to the existing way of life. This is a clear effort to account for an internal perspective on norm construction and so provide a potential basis to transcend the limited paradigms described above.

Central to the problematic above was the idea of the relation of norm to context and argumentative reason. It is therefore very important to get an impression of what role these plays. Lenoble and Maesschalck describe three facets of 'context' to which the entire notion cannot be reduced:[20]

- Not a set of factual constraints
- Not a false representation or a framework offering resistance
- Not a particular culture which cultural anthropologists could identify and which could be deposited in the individual minds of individual actors as continually adaptable conventions that would serve as capacitating structure for them.

These three components exist but don't exhaust the function of context. They are each of them formalistic reductions of the notion of context. By reducing the context to those components one misses the question of the potentiation or the capacitation of context to produce these meanings effects, that is, the reflexivity of the judgment by which the context, on the basis of which a norm is given sense, is perceived.

"The epistemological insufficiency of every theory that supposes the context as given or identifiable is important because such presuppositions, even in the form of conventions that are adaptable or revisable by an individual, don't take into account the reversible or reflexive character by which *one gives oneself* this preference, this convention or whatever it is that makes this ability to adapt or revise possible."[21]

One's perceptions of elements of context are members of a set entailed by particular theoretical presuppositions; they are symptoms of a framing, linked via informal inferential connections to beliefs. Hence, there are no cognitively significant representations of one's predicament untouched by background theory. [22] In any and every use of reason whatsoever there is contained within it implicit reference to background. Neutrality in the sense seemingly required by the prevailing approach is thus impossible. Moreover, an approach more rooted in an appreciation of contexts is motivated.

The concept of context must be itself reflexively constructed – it must be thought of as that which, through norm-centred judgement, enables possibilities for human existence. It might well be rendered as "potentiating way of life",[23] to highlight that this reflexivity of

20 Lenoble & Maesschalck, *Towards a Theory of Governance: The Action of Norms*, p.87

21 L&M *ibid* pp.90-91

22 This position is elaborated in the work of various theorists such as Quine, Putnam etc. Hume could be seen as a counterpoint

23 Lenoble & Maesschalck, *Loc. Cit*

the concept of context cannot be reduced to any convention supposed as given. In established approaches, contextual background is generally itself formally reintegrated into a decisionist matrix by an anticipation of the consequences. The context is reduced to the merely something that offers resistance; to a set of foreseeable and objectifiable constraints that rational approaches or choice theories should take into account. The criticism here formulated by emphasising the necessity for reading the reference to the background as a transcendental logical function of the operation of reason helps us to understand the consequence of our approach to the reflexivity of judgement on the level of the construction of governance arrangements. The intention is to develop an internal perspective and thus to appreciate the position of social participants in a thick sense.

With these concepts in mind, advocates of the Maesschalck/Lenoble position suggest that each current democratic governance approach is faced with two fundamental problems or 'conceptual blockages' relating to the necessary conditions for the meaningful uptake and enacting of norms adopted. Such an uptake and adoption requires a self-redefinition in terms of the normative injunction understood as such.

The first of these conceptual shortcomings can be called a reductionist failing. This failing sees the normative injunction's adoption and enacting as something which can be exhaustively described in terms of the existing authorities' interventions. However, when we consider the adoption of a norm, including a self-redefinition in the light of the norm adopted, and that this process will be a deliberative one, existing authority structures show themselves to be inadequate to the task. For the Louvain School, this is not least due to the presence in the situation of a learning operation: "When the success of a collective action is understood as depending not just on market-style decentralized coordination but also on deliberative and cooperative practices, the process of development of what we call a reflexive approach to governance is under way. In contrast to governance based on the command and control model or the market mechanism alone, the success of any collective action comes to be subordinated to the success of a learning operation."[24]

The presence of a learning operation in the kind of scenario described above is to account for how a normative injunction can have meaning for the people to whom it is addressed. It is to account for how actors can mobilise their resources to adjust their ways of life to new scenarios, or to adjust their entire *modus vivendi*, should it be required. Such an operation cannot be assumed to be somehow 'natural' given what is known from experimental psychology regarding the consistent use of logically incorrect 'heuristics and biases' in decision-making under uncertainty even among the well-trained.[25] Philosophically too there is a problem is simply assuming that human beings are apt to make decisions that gradually form sets with growing verisimilitude.[26]

Learning is the capacity to change in light of judging circumstances to require novel treatment. This is why it is prior to the success of the governance operation itself. It is the

24 Lenoble, J, *A reflexive approach to governance* http://refgov.cpdr.ucl.ac.be/pdf/presentations/FP6REFGOV-Conference-Intro-JL-May2010.pdf, p.2

25 cf Tversky and Khaneman, "Judgment Under Uncertainty: Heuristics and Biases" in *Science*, New Series, Vol. 185, No. 4157. (Sep. 27, 1974), pp. 1124-1131. http://psiexp.ss.uci.edu/research/teaching/Tversky_Kahneman_1974.pdf

26 cf Popper's account of scientific knowledge and its critics.

learning operation that gives meaning, content, to the normative injunction. Without this, governance is at best ambiguous, probably meaningless, misdirected, ill-addressed and generally inadequate.

The second conceptual blockage consists in predicating the effectiveness of the practical acceptance of a shared norm among a given public entirely on the proliferation of mechanisms that are taken to create cooperation and participation among social actors. By simple recourse to participation (public dialogue, say) it is assumed a norm will be binding for the public in general. In other words, the blockage relates to how the capacity of the public to accept a new norm is thought to be given just because a legitimate or justified approach is used in developing that norm – justification and legitimation are equated with application.

This is a problem as the application of a norm is a real, practical action requiring the transformation of perspectives and ways of being among a public. It is far from certain that such an outcome will simply issue from a dialogue, even if such a dialogue is rational. One cannot assume, therefore, that simple inclusion will result in cooperation and participation, nor even that cooperation and participation will result in practical acceptance of a norm. Dialogue is part of a problem, not a solution in itself.

In a sense, the learning operation can be seen as central to the Louvain approach, even regarding the second conceptual blockage noted. The concerns about participation revolve around the inadequate account of learning employed in dialogical processes. There is a constellation of concepts implicated in these matters, however, which will arise in subsequent discussion here. For instance, learning and participatory processes imply dialogism, which subsequently implies communicative rationality, including argumentation (and other forms of rationality). The differences between legitimation, justification and applicability employed in mentioning problems with practical acceptance imply ideas of formalism and proceduralism.

The task here is to get these concepts somehow to cohere in a manner that permits the construction of a norm in context such that an ethical governance mechanism can be the result and we can make policy recommendations on this sure foundation. We will pursue this agenda with reference to 'learning' because learning is credited as being at the heart of governance measures, prior to their success, by the influential Louvain School.

Learning

According to Argyris and Schön's 'organisational learning' approach[27] an often ignored factor in learning are the "obstacles" that could prevent success of a learning operation through assumption of the sufficiency of the actors "spontaneous capabilities" for the success of the "joint experiment". They develop an experimentalist approach that questions the conditions for actors' "capacitation", through looking at "defensive strategies" that actors could perhaps unwittingly use and thus ultimately restrict the amount of fulfilment of their normative expectations, such as negotiation techniques taught in public policy education.

27 Argyris, C and Schön, D. A., *Organisational Learning*, Vol.1 *A Theory of Action Perspective*, Reading, MA, Addison, Wesley, 1978

After a joint inquiry, a "reframing" operation takes place, and each actor will deploy a frame that, according to the organisational learning approach, constitutes the actor's rule of identity. This is a personal frame sensitive to the social group, and has a dual function, with two guaranteed outcomes:

1. It allows the actor to assign a personal "meaning" to the context & adopt a role within that. This is a generative act and produces a rule (call it rule #1) for the interpretation and integration of facts.
2. It guarantees that, despite the novelty of each problem to be solved, actors will transpose the new onto the familiar. This is a scheme (a rule #2) that can be applied to the construction of a context-sensitive and identity-sensitive (i.e. #1) representation (i.e. "I remember something like this happening before.")

"When a practitioner makes sense of a situation he perceives to be unique, he sees it as something already present in his repertoire. To see this site as that one is not to subsume the first under a familiar category or rule. It is, rather, to see the unfamiliar, unique situation as both similar to and different from the familiar one, without at first being able to say similar or different with respect to what. The familiar situation functions as a precedent, or a metaphor, or... an exemplar for the unfamiliar one."[28]

According to Schön, it is in a sense "sufficient" to pay attention to the problem of reframing for rule #1 to take place, and if #2 happens, #1 is assumed to have happened because of the attention paid to it – in other words, it is through the reflection on and negotiation of personal identities (and their associated framings) that controversies are surmounted in matters such as policy-making. It is this assumption, along with the incitement approach that is associated with it that the Louvainians consider insufficient for a complete system of governance, and which they wish to approach as an extension of these theories.

Louvain Approach

The Louvain approach seeks to allow for a schematic approach to the conditions for identity representation and its variety according to the application of context.[29] It sees the formulation of the learning operation in the pragmatic approaches as incomplete and seeks to complete it with the development of this meta-approach.

It removes the assumption of the way that actors adopt identities (and fulfil #1 above). The way that actors adopt an identity (have a capacity to "self-represent") is through "terceisation", i.e. "a third element whose externality makes possible the actor's construction of [their] image".[30] If you look in the mirror you will recognise yourself, and it is necessary

28 Schön, D., *The Reflective Practitioner. How professionals think in action*, London: Temple Smith, 1983, p.138

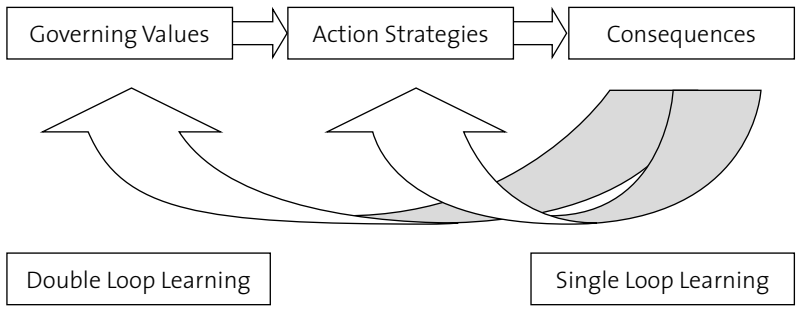
29 See Lenoble, Maesschalck, *Beyond Neo-Institutionalist and Pragmatist approaches to Governance*, http://iap6.cpdr.ucl.ac.be/docs/TNU/WP-PAI.VI.06-TNU-1.EN.pdf See also their *Toward a Theory of Governance*, p.172ff

30 Lenoble, Maesschalck, *Synthesis Report Two: Reflexive Governance: Some Clarifications and an Extension and Deepening of the Fourth (Genetic) Approach*, REFGOV: Reflexive governance in the Public Interest, Services of General Interest/Theory of the Norm Unit, p.14ff. Observations in this report and the previous one inform the discussion generally at this stage of the argument.

to recognise yourself. So it is necessary to allow for the other to, firstly, exist, and then to differentiate between you and your image (the other), so the fact of the mirror itself must also be acknowledged (invoked).

> "It is the product of an operation of 'terceisation', that is, an operation that requires the invocation of a third element – be it a person or an organizational device – whose externality makes possible the actor's construction of her image, i.e. of what will enable her to identify herself, and her own interests, in a given context for action. To carry out this operation of 'terceisation', collective actors must submit to a twofold inferential operation:
>
> 1°) a retrospective relationship with experience: reconstructing the form its identity takes on through its past actions, and in so doing installing a capacity to be an actor (reflectability)
> 2°) an anticipatory relationship with the current situation: identifying the transformations that will be necessary to ensure the realisation of this form in a new context for its application (destinability).
>
> Reflexivity is no longer a schematic rule-based approach but a permanent reflective attention to the operation of 'self-capacitation'."[31]

In this perspective, learning is more than metaphorically a 'double loop' operation; it is not just learning how to choose solutions, but learning how to choose how to choose solutions. As can be seen in the following diagram, rather than merely allowing consequences to condition future action strategies, they are also allowed to influence the very guiding values that condition possible actions.[32]



Put differently, in order for an actor to be able to express something of the form, "I think that *x*", where '*x*' is some state of affairs, it must be credited to them that they can distinguish the description and a possibly falsifying, transcendent reality owing to the fact that in order for a state of affairs to seem a certain way, it must be a certain way. Moreover, the fallible knowledge of criteria for fulfilling *x* implies the possibility of the criteria for *not x* (states of affairs *a*, *b*, *c*, say). Thus in the interpretation of a fact and the assigning of a personal meaning to it, upon which decisions and other actions will be based, we see the activation

31 *Democratic Governance and Theory of Collective Action*, Annual Scientific Activity Report 2008, p.39-40, http://iap6.cpdr.ucl.ac.be/docs/IAP-VI-06-AnnualReport-2-final-2.04.09.pdf

32 Diagram sourced from Hajer and Wagenaar, *Deliberative Policy Analysis*, p.45

of a host of knowledge in a proactive and dynamic form. In this sense, as an activity, there is an element of expression involved in perception and interpretation rather than merely simple reaction to given data from without (as a decision-theoretic account might have it). This is a manner of thinking which takes an internal perspective, yet maintains the epistemic resources for immanent critique of claims and their procedural genesis.

The idea is clearly to account for diversity, while retaining a universal element, i.e. the universal moment of framing *per se* that serves to unite diverse framings in a procedural sense. This, it can be presumed, is to account for a sense of human nature that is not tied to any particular conception of the world. So, this conception hopes to provide a genuinely representative account of persons in society *howsoever they see the world they inhabit*.

The importance of this is that if we model better the manner in which personal identity factors in decision-making among actors; how socially perpetuated identity and self-conception figures in the perception of public facts, we can better conceptualise the actual ways in which institutional mechanisms are developed. A detailed and well informed conception of this genesis and these mechanisms will allow for a greater and more effective understanding of the intentionality of collective actions. A genuine, authentic and complete theory of governance will depend upon a proper grasp of these ideas.

To carry out the above terceisation, each collective actor must take part in the twofold action described previously. This operation of self-capacitation is "attention paid to two questions reflecting the dimensions of reflectability (collective identity making) and destinability (ability-to) that together constitute the reflexive operation by which an actor constructs its capacity to build a representation – of itself and of the context."[33]

Reframing is not a simple substitution operation (such as that which Schön suggests), but what the Louvainians call a "combination" of the old and new frames. Schön's reframing is a reductionist one, which can lead to a simplification of the real process, it is argued.[34]

The implications of this are that it's not the diachronic relationship between the actor and herself but between the actor and other actors and with the "institutional mechanisms" that form the framework within which they interact. This is key to the Louvain theory of governance. Their major critique of the pragmatist approach is that it fails to move beyond some of the assumptions of those theories it seeks to better. The assumptions they make are that the mechanisms for reflexivity they introduce operate from the outside and excite some internal transformational capacity within actors. This stumulus:reponse kind of approach (possibly with some further assumption of increasing representational verisimilitude) is inadequate.

The idea is of mobilising the powers of intentional and self-conscious, socially informed, immanent critique of procedural mechanisms in the context of sought-after outcomes, outcomes that are themselves open to scrutiny by the same powers. This means that it is possible to determine the very conditions for the learning mechanism itself and so achieve some manner of universal insight.

33 Lenoble and Maesschalck *Beyond Neo-Institutionalist and Pragmatist Approaches to Governance*, p.159. The critical outlining of the Louvain school's position here draws upon this document

34 See for instance, Lenoble, Maesschalck, *Les insuffisances réflexives de l'apprentissage dialogique*, http://iap6.cpdr.ucl.ac.be/docs/TNU/WP-PAI.VI.06-TNU-2.pdf

A learning mechanism such as this permits reflection on processes and upon the reflexive capacity itself in a manner that permits the enumeration of possibilities from a real perspective as well as speculation upon alternative possible perspectives and their possibilities. This means that for each participant in deliberation both concrete, actual horizons as well as speculative horizons of possibility are opened up. In this way, deliberative participants can call into question, or problematise, processes of governance, the contents of governance issues (including their ethical content), and the status of each in terms of their own view and that of a wider public of which they are a part. This problematisation, moreover is extendable via speculation into future states of self and public such that a real forum for testing and evaluating the processes and contents of governance problems is available. Its basis in intentional, self conscious, immanent critique allows for authoritative judgements to be made as the reflexive moment is founded in the normative expectations of the public. Thus, arguments or decisions have a connection with those they will affect.

Limits of the Current Solution

The experimentalist approach was felt to presume too much regarding the assumption of identities. The experimentalist-pragmatist approach to learning is supposed by Lenoble and Maesschalck to be incomplete and therefore inadequate owing to the manner in which it fails to posit a 'third thing' that underlies the supposed process of learning *qua* rule #1 and #2. Without the third thing, an enabling process, presumably the fear is that unreason could mar the learning mechanism. One could adopt a perspective on 'the unfolding scene' such that the transition between #1 and #2 was derived improperly, perhaps. Or again, perhaps one's perspective, while phenomenologically prompting certain interpretations, could not be said to be modelled upon entailment – if there is any real requirement for a relation at all – there is too much room for caprice, perhaps, in the learning mechanism and so too much scope for arbitrariness.

The Louvain solution is then to 'complete' the learning process by introducing the universalising element via conceptualising the conditions for it. But this suggests that in principle everything relevant can be known about a particular scenario (including the parameters of the test of relevance). It forgets the lessons of bounded rationality *viz.* the rationality of individuals is conditioned by the information they actually have (according to their real filters of relevance, like their values). In forgetting this, the approach falls into the very trap concerning reason that it describes so well, namely that of positing an impersonal reason whose determinations motivate through mere articulation.

Terceisiation effectively decentres the social actor in the process supposedly required by their self-recognition – the self awareness prompted on the model of looking in a mirror would be akin to enumerating one's qualities as propositions true of oneself. This is precisely *not* what it is like to be a social actor. One's qualities, history, values and so on are not just sentences one would assent to. That is the point that makes the endeavour to account for them so difficult. Thinking about thinking is still thinking. However, thinking about thinking a particular thought is no longer thinking that thought. If I think about who I am in terms of propositional knowledge, I am no longer reflecting on who I am, but am describing myself as an object of experience. The problem is how to account for myself as a bearer of experiences.

The 'complete' learning[35] procedure in terceisation involves what is essentially a decentring operation, thus throwing the whole approach into the argumentative mode. Since governance is subservient to the learning operation and that operation turns out in Louvain to be argumentatively construed, the whole governance edifice built upon this foundation is rocked. As a side-effect, moreover, the problematic parallelism between reason and morality is re-affirmed as argumentative reason takes over – valid argument is thought to be inherently motivating, thus the approach ultimately conflates the conditions for justification with conditions for application. This undoes *all* of the succinct and astute critical work of Lenoble and Maesschalck (critical work we in fact rely upon).

To repeat, the reasons that we accept or refuse a proposition in any given discussion are not necessarily the same as the reasons why we accept or refuse those reasons. For example, a frequenter of mediums accepts that astrology is predictive of his prospects, citing past successes, but refuses to let failures of prediction dent his conviction, even though the rational structure is symmetrical. Somewhere, reason runs out and narration steps in – the deep sense of self and all that one's convictions connote, etc. The frequenter of mediums has a deep-seated need to feel the universe isn't a blind, meaningless system, for instance, so favours confirmatory evidence over falsificatory. So, they employ deductive reason in matters of confirmatory 'facts', but narration trumps that same process in falsificatory eventualities.

While this is clearly important in comprehending who/what a person is, it is only comprehensible itself in argumentation if we step back from the primarily argumentative mode of discourse (with its positivist overtones) and regard narration not as an aggregative report of experiences had between t_1 and t_2, which predisposes certain outcomes by dint of history, but rather as the authentic self-portrayal of a vulnerable human being – i.e. we need to use a *recognition* principle in order to cognise the information encoded in this. This calls for a re-synthesis of private and public reason, contrary to the privatising march of modernity in general.

Synthesis

Argumentation, *qua* Habermasian discourse, is not the only form of discourse admissible as public reason, with understanding of a real life context seen as being more fine-grained than merely argumentatively construed. Argumentative discourse is the foreground of ideal public space. Narration, interpretation, reconstruction are also admissible on this account. Since narration will only be relevant in terms of a life lived, via specific interpretations of life-events by an agent, an ethical dimension is required in order to comprehend it.

The place of narration can be seen as illustrated by the following problem: In discourse ethics, when matters of justice arise and competing, contradictory arguments are aired, it is required that the parties involved will submit themselves to nothing but the force of the better argument. But the acceptance of arguments will itself be conditional on values. Thus, narration doesn't fit *within* argumentation, but rather argumentation *decentres* narrative authenticity.

35 Just exactly what a complete learning procedure means is a problem in itself. Learning by its nature, one would imagine, is at least open in one direction – receptive of input – and therefore would require an incompleteness. Terceisation could be read as implying some manner of rational flight into omniscience-through-procedure

For a sense of reason not simply centred upon a solipsistic reverie, and in the context of a mind limited (wherein assumption must feature) different forms of discourse are essential: narrative, interpretive (generalisations from experience mediated by narration), argumentation (proceeding by universalisation of individual maxims of action – integrative power through voicing action-plans) Reconstruction, wherein the view of what is good for another from their point of view is articulable and comprehensible.

Transcending the Limits of Louvain

The Louvain school misses the diversity of reason in trying to augment the account of learning present in the experimentalist-pragmatist view by underwriting with a meta-principle of argumentative, universal reason. It is a complex way to exclude value, hence to box off subjectivity from activity in the public sphere. Recognition is not possible in this account as the overriding effect of the Louvain learning mechanism is that of decentring. Narrative authenticity is ruled out, so interpretive generalisation is impossible as is reconstruction. The 'incomplete' experimentalist-pragmatist view might be more true to reality precisely because it is tied to particularities and has no universalising moment.

If we recall Giambattista Vico's view, as interpreted by Isaiah Berlin, we get this view of how to understand people from another time: "...to understand history is to understand what men made of the world in which they found themselves, what they demanded of it, what their felt need, aims, ideal were. [Vico] seeks to recover their vision of it, he asks what wants, what questions, what aspirations determined a society's view of reality."[36] Berlin goes on to emphasise that this knowledge is not that gained by purporting to apprehend certain facts, or logical truths, but is rather that insight gained via imaginatively empathising with a given people. This is possible, in Vico's opinion, as civil society is a man-made structure wherever or whenever it springs up, therefore it is possible to comprehend as a human reaction to given information – we can *reconstruct* their view by analysing what they considered good for them.

In terms of a learning operation this runs parallel. When confronted with a 'shock' (the term used in Lenoble and Maesschalck for emergent conditions), the reactions of socially engaged individuals will not be based in a presumed deduction from circumstances, by way of data on new facts, to conclusions reached *via* logic.[37] In order to understand a reaction to a change it will serve better to empathise with the situation in which the actors find themselves. This is 'better' precisely because it doesn't abstract value from norm in their actions, so we get a genuine picture of how the affected parties see the world and conceive of the possibilities entailed by the change *for them*.

How is this not simple relativism? The sort of truth aimed at in the mode of apprehension here aimed at is pragmatically construed.[38] Pragmatism aims not at ultimate metaphysical

36 Berlin, I, 'The Divorce Between the Sciences and the Humanities', in *The Proper Study of Mankind*, Hardy & Hausheer (eds.) p352

37 This is an objection elegantly made by Lenoble and Maesschalck themselves, cf. *Toward a Theory of Governance*, p.184 Nonetheless terceisation recreates the problem they see in others' work.

38 Recall from earlier that we dismissed a 'view from nowhere' in establishing that 'neutrality is a fiction'. This is a logical development from that.

truths, truths we should rightly suppose don't exist in such clearly historicised domains as politics and practical ethics, but instead aims for the most effective truths possible - our best effort. What's true is that which current best practice can't improve on (and it is open to and subjected to testing).[39] The claims made by the pragmatist are inferentially articulated, that is, firmly based on *reasons* as opposed to being based in Reason (capitalised). They are claims embedded within systems stocked with evidence, hypothesis and conclusion. It uses the faculty of reason upon the deliverances of sense and produces judgements of more or less sturdy epistemological stuff.

The Louvain school seeks equality of applications of learning via formalising argumentative processes, thereby trying to liberate the power of reason itself rather than relying on reasons as understood by a people in question. The learning process's deliverances, then, will be the very definition of rational. Despite carefully formulating their account of asymmetry, moreover, latent within this movement in the Louvain approach is the assumption that 'rational' equates with morally good, since it is presumed within the account of learning that the better supported in argument, the more irresistible a precept becomes. In other words, despite all their careful statements of context and the pragmatic requirements of an approach to reason in governance, in this the Louvain school fall back on the principle that *reason is sufficient to determine its own application*.

Two assumptions can be discerned that are latent within this part of the Louvain approach:

1.) that the removal of content, or formalisation, offers a route to fairness via neutralising differences
2.) that rationality, in this case well-argued cases, are morally compelling

1.) The pragmatist can better the position offered by the formalist by opposing these wrong assumptions while still being able to lay claim to utilising rationality. Content, rather than being eliminated in order to ensure fairness, must be included and articulated in such a way as to render it as explicit as possible.[40] This is fairness as this is the material stuff individuals, groups, societies have to work with. Anything other than as full an explication of the contents adhered to and deployed by individuals and groups is a misrepresentation of the players in any debate and thus warps the dialectic from the start. There is a kind of category mistake in pursuing anything based on such a skewing.

2.) Rationality is not morality. In the spirit of content-inclusion, rationality ought to be conceived of in terms of the operations made upon the inferential articulations of contentful claims endorsed, denied etc. Thus, morality gains a mechanism as moral debate carried out in this way will be able to draw upon the power of reason in concrete terms, terms that are meaningful to those using them. Reason doesn't contain within itself the terms of its own application, but given content, logic can provide the means to determine whether a claim justifies a conclusion, presupposes another etc.

39 Misak, C, *Truth, Politics, Morality*, p.1

40 This view has a strong philosophical pedigree from JL Austin, Paul Grice, Peter Strawson, through to Wilfrid Sellars, Robert Brandom and (in certain writings) J Habermas. See Rainey, S, "Austin, Grice and Strawson: Their Shadow from Pittsburgh to Frankfurt" in *Essays in Philosophy*, Vol. 8: Iss. 1, Article 17 (http://commons.pacificu.edu/eip/vol8/iss1/17)

'Material inference' – case in point

Material inference is contrasted with formal inference. For formal inferences, structures (e.g. the form of a syllogism) are taken to be valid or invalid independent of the actual substantive content of the variables. So we can say that an argument of the form "If *p* then *q*, and *p*, therefore *q*" is valid for any *p* and *q*. Material inference, however, is that manner of inference that is valid or not in relation to the conceptual contents (the meanings of the terms) deployed within it. It is defined clearly by Robert Brandom as follows:

> "The kind of inference whose correctnesses essentially involve the conceptual contents of its premises and conclusions may be called, following Sellars, '*material* inference'."[41]

The point is that these types of inferences utilise the meanings of the contents of argumentation in a way that formalist approaches expressly reject. This central difference between material and formal reason is emblematic of the skewed account of reason that itself leads to the equating of argument and moral compulsion that arguably underlies the majority of current ethical governance attempts.

The abstract, pinned down in fact, gives us the basis upon which to pursue normative enquiry including the investigation of ethical aims. The meanings of language and hence the significance of the world from the perspectives of social actors, once engaged with, permits normative discussion as in so engaging we have to use the reasons for assuming a premise (narrative reasons, perhaps), inferring from this premise (maybe an interpretive or argumentative reason) and concluding something from all of this, again for potentially diverse reasons. In recognising the diversity of reasons we recognise the role of value in self-perception and social deliberation and so we can properly represent in public reasoning the public themselves. So, we adopt an attitude necessary for ethical thinking in that we reconstruct the object of ethical enquiry – the social actor. This permits the policy-maker (in the case of governance) to provide reasons for a social actor to adopt a norm, as opposed to merely dealing in commands. Since this engagement runs on reasons embedded within the purview of the social actor, this also gives a means whereby that actor can transcend their own values and adopt a norm independent of their predilections.

Synthesis

Having gone through this theoretical work, we have established *why* the deployment of uninterpreted terms is a problem for governance – without the construction of context, and without care to utilise significant terms governance injunctions:

1.) Meaningless for those it is supposed to serve (the public)
2.) Impossible to use in governance by policy-makers (it can't be accepted by a public)[42]

41 Brandom, R, Making It Explicit, Harvard 1994, p.97

42 Decontextualised governance injunctions would require enforcement through law or other means, and so would be against the spirit of governance as dialogical, etc.

Moreover, having established these things in the manner we have, via a theoretical approach to understanding normativity and governance itself, we have placed ourselves in a position not beholden to any particular theory (i.e. we haven't ended up with a false dichotomy of option A or B as an *ad hoc* solution of how to interpret terms from a meta study or anything similar to that. So, in having done this theoretical work we have equipped ourselves with the conceptual apparatus required to approach the real problematic in a principled, authentic manner.

We have been able to link the idea of meaning with context and with ethical governance. In order to get to the heart of how to relate this complex to action we need to discuss a point from a theory of action relating to desire and rationality in action. It should become clear from this discussion that there is a direct parallel between the role of action and reasons in individual actions and the role of value and normative injunction in public action. Essentially, this parallel will describe the task of ethical governance of pluralist social groups, and will show the basis for how to achieve the efficiency of ethical norms in governance.

Belief and Reasons

Elements of personality, conceptions of the good and so on are contingent, but the very realisation that I act on reasons binds me to looking for *good* reasons.[43] This suggests that within the scope of action for a human being, including their practical conception of themselves, reasons play a role – they have to or the 'self' in question is no self at all, being merely determined. In fact, this is a view held by influential philosophers of action such as John Searle for whom the creation of 'desire-independent reasons' for action are the markers of human rationality.[44]

Were we, ape-like, to see a desire as necessary and sufficient cause for action we would not be rational beings, contrary to rational choice theory. Rather, to be rational we must understand how it is that we become reason-sensitive and more importantly sensitive to those reasons that do not feature in our set of desires (i.e. how we come to act in ways we don't want to but see motivation for nonetheless). Interestingly, Searle stresses the importance of the first-person perspective in understanding how this phenomenon operates. He discusses promising:

> "...how can I create a reason for myself , a reason that will be binding on me in the future , even though I may not at that time have any desire to do the thing I created a reason for doing . I think the question becomes impossible to answer if you look at the phenomena from the third -person point of view... The only way to answer this question is to see, from the first -person point of view , what I think is going on, what I am trying to do, what my intention is when I make these sounds through my mouth... I see myself as freely creating a special type of desire-independent reason, an

43 Korsgaard, C, *The Sources of Normativity*, Cambridge University Press, 1996. We refer to the highly influential Korsgaard here as she represents an updated view of autonomy that retains something of Kantianism, i.e. she emphasises and accounts for the role of normativity in action. This is key to our problematic as we seek a normative approach to ethical issues.

44 Searle, J, *Rationality in Action*, MIT 2001, *passim*

> obligation... It is the intentional creation of certain sort of obligation - and such obligations are by definition independent of the subsequent desires of the agent."[45]

The point of a promise is the making of a reason to act that is independent of any desire the promiser might have when the time comes to deliver. What's more, 'promising' is itself an institution – it is recognised among promisers and promissees as a real phenomenon. It is through this institution that promises can be freely made, accepted and relied upon (and broken ones lamented). When actual real promises are made, accepted and so on, they bind the will of the promiser and excite expectation in the promise owing to the first-person perspectives they each take on this. The promise to the promiser is binding as it is a manifestation of freedom at the point of promise-making.

Promising is a simple case wherein one can act against one's desires. The parallel with governance is that part of the governance problem was to move beyond command/control structures. Governance must 'steer' and so must provide the means whereby social actors can bind their wills to actions possibly *despite* their values. Extrapolating from promising, we can see how social actors too make decisions based upon reasons in the light of institutions.

In order for a social actor to bind their will to an injunction not necessarily in accord with their values, it is sufficient that an institutional arrangement exists such that that actor's reflection can lead to a value-independent reason to act. For such a phenomenon, as in individual action, the value-transcendent reason must be a manifestation of the social actor's freedom. The social actor, their will freely bound to a value-transcendent reason, may go on to transform their values in line with the injunctions, but this is not necessary.

Taking the parallel here between the case of promising and more generally that of binding one's will to a value not necessarily held in social action, we see a task laid out for the institutions of governance: *they must facilitate the governed in a process of deliberation such that the governed can freely bind their will* via *value-transcendent reasons.* This lofty-sounding task is nothing more than the engagement with social actors along the full spectrum of rationality, however. The recognition of rationality beyond the simply argumentative sort is the means to open up the first-person perspective required for a reason to be adopted that can trump a value. It is by means of a genuine engagement that social actors' positions are understood and can be communicated with meaningfully rather than technocratically manipulated via command.

This is of direct relevance to our problem of ethical governance as we have been developing a normative account, one facet of which required dealing with how a social actor could bind their will to an injunction not necessarily part of their own motivation set. This was a problem as in governance values must be respected as well as abstract reason (narration etc. must be considered). These values are exhibited in, among other things, the meanings different terms and concepts have for social actors. What a term such as 'privacy' means once interpreted has been a part of the problem we have been addressing all along. Here we see why this matters and obtain a means to understand it in material inference. In parallel we begin to see the connection between these points and governance as the reality of institutions comes into play with Searle's thought. Thus, in developing these points we see a basis in theory as to how a social actor can act on reasons regardless of desire – they give to themselves an obligation based on the apprehension of a norm as a norm.

45 Searle, J, *Op. Cit.*, pp.208-209

Conclusions

Beliefs aim at truth, pragmatically construed, and connect on the back of inference. They are thus interconnected by reasons. By basing governance endeavours not on a formalised conception of a given people, but rather on the thickly conceived interpreted and reconstructed views they hold, communication is made possible with that people. In communication we can influence belief and action *reasonably*. Such a conception as this, that doesn't favour argumentative reason but instead 'meaning' in a full-blooded sense, provides the means of compromise, however uneasy it may be, between competing positions including those internal to any given social actor (as between value and governance injunction, for instance).

For instance, what if the *status quo* should change for some given group? What if we find out we're wrong about something, or that our current mores no longer fit our aspirations? We can deliberate and change. But we deliberate from our actual points of view, rather than bifurcating into experts and non-experts, the former deploying abstract reasoning to 'tutor' the unpersuaded latter group. Just as democracy is best thought of not as a moment that ordains epochs of legitimacy via voting practices, reason in this contextualised way that is concerned with meaning and reasons for contentful belief must be thought of as a *modus vivendi* or a least a *modus operandi* based in the authentic portrayal of views, tempered with frank critical appraisal. Governance can't sleep in the periods between belief, acceptance and reevaluation, but must be a dynamic, deliberative mechanism that facilitates the exchange of views in the light of facts and values.

This must be so in order to respect all that we have shown so far, and that we have taken as insights from other sources, to do with:

1.) The interpretation of meanings of words like 'privacy'
2.) Context which itself cannot be reduced to a mere 'background'
3.) Human rationality as inclusive of narrative and more besides argumentation

The fact that 1.) both informs and is informed by 2.) in a so-called 'hermeneutic circle'[46] demonstrates the interrelation of belief, acceptance and reevaluation and so its dynamism. A dynamic process like this one requires a vigilant governance treatment rather than a mechanistic one in order to facilitate its many nuances and changes (the central role of dialogism in this also requires a sensitivity to nuance not present in command/control government, for instance). 3.) demonstrates that the addressees of norms, social actors to whom governance ought to be answerable, do not spontaneously divide value and norm in their experience of the world around them. Thus, any governance measure that hopes to be proportional to the governed must deal with norms and values as a complex.

When we rely upon inferentially articulated hypothetical imperatives we rely upon operant, structurally sound material inferences that are generated from a basis of lived experience. 'Lived experience', moreover, is the rationalised aggregate of the choices, values and possibilities of the subjects to whom future norms are to be addressed.

46 The idea is that reflection upon the parts of something is informed by reflection upon the whole and vice versa. Originally a term of Benedict de Spinoza's, with reference to understanding scripture cf. *Tractatus theologico-politicus* (1670)

Thus, when we rely upon this as a basis for policy-making, we get right the addressees of future normative injunctions. When we deploy these hypothetical imperatives in the context of material-inferential articulation and criticisability, moreover, we have the basis for compromise between tradition and change. We have this basis as we work with the material from which desire independent reasons can be made, according to the 'filter of relevance' of the social actors we wish to address. In short, we have a learning mechanism, that which was absent from previous models.

The notion of a complete, universal learning process leads to a decentring use of reason that itself presumes rational argument to be the motivation *par excellence* for the social actor. Practically, this underlying thought pattern entails a conflation of standards of justification with standards of application, which results in decontextualised injunctions being formulated. The upshot is that little or no incentive is provided for any given social actor to bind their will to the injunction issued from such a base. The concern with theoretical rationality, rationality geared toward beliefs rather than action, within this theoretical background is thus linked to practice as it is through engaging with the beliefs and the view of possibilities borne by norm addressees that the capacity for action is first realised. Theoretical rationality provides a means to inform practical rationality.

With a value/norm connection re-established by way of an underlying understanding of context we have a manner in which to comprehend desire independent reasons, and thereby a learning mechanism, hence a normative basis for ethical governance. Only by accounting for values and norms during the processes of technical development can we, incentivise the adoption of governance injunctions by their addressees within projects and in broader public. We need this to ensure ethics conditions development and is thereby proactive in research and development. This requires reflexive accounting for values and norms and incentivisation *via* policy instruments, as well as an opening of discussion on ethical matters across hitherto divided levels (expert, research stakeholder and public).

From this basis, constituting as it does the grounds for an approach, existing ethical governance tools such as those deployed within FP7 can be re-cast in an effective way that permits proactive ethics, rather than reactive, *ad hoc* measures. Practically speaking, this grounds the shift from command/control government that is presumed in governance in general. This means that governance *per se* is given a firm epistemological foundation that, in engaging with perspectives authentically, also grounds the legitimacy of the process. Moreover, since this entire approach is centred upon respecting the views of possibilities as perceived by the parties for whom change will bring about effects, it is essentially engaged with the practice of ethics as it deals with evaluative information regarding the difference between what *can* and what *ought to be* pursued. Thus, this normative theoretical backing provides the basis for an authentic, efficient and legitimate ethical governance approach.

CHAPTER 4
ICTs and responsible innovation: imaginaries of information and community

Kjetil Rommetveit

Introduction

In the introduction to this book, Rene von Schomberg defines responsible innovation in the following way:

> "Responsible Research and Innovation is a transparent, interactive process by which societal actors and innovators become mutual responsive to each other with a view on the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society)".

The definition is based in an understanding of innovation as deeply embedded in social processes. It aims to use such understanding, achieved throughout a number of disciplines, in order to achieve better and more integrated governance of innovation in science and technology. Thereby one may also hope to see more socially robust and sustainable ways of living with and using science and technology.

Over the latter years significant developments have been made in science and society fields such as ELSA (ethical legal and social aspects), technology assessment, foresight, ethics and participatory governance. In many cases, the most significant innovations have been made in close relation to (first) biotechnology, and then (in a somewhat later stage), the governance of nanotechnologies (Kjølberg 2010, Macnaghten et. al 2010). At the moment, however, there are few institutions devoted to ICT ethics and governance, and there are few or none Europe-wide platforms for deliberating and including civil society in discussions about the social and ethical implications of ICTs or related technologies. One could expect that the way forward for ICTs (and related security technologies) would be to take the learning from such experiments, and seek to extend and develop them further in the field of ICTs (as happened, for instance, in the transition from bioethics to nano-ethics). Although that certainly is a desirable goal, in this article I shall argue that one also ought to consider broader dimensions, aiming to take the deeply social and communicative characteristics of ICTs, and the many roles they already play in society, into account. To state the point briefly: whereas one may communicate and deliberate about genetic engineering, synthetic organisms or nanoparticles, ICTs themselves are powerful tools for deliberating and communicating. They already strongly transform the phenomena in question (subjectivity, society, humanity, communication, etc.), and they are already deeply transforming the character of sciences and technologies, such as bio- or nanotech. Ethics and governance evolve along with technologies and the social and cultural worlds with which they interact. In this text I shall argue that ICTs are deeply inscribed in an increasing number of controversies over resource distribution and sharing, access to political institutions and, indeed, the over-all state of our societies. ICT innovation and governance aiming at responsibility must take these aspects into account.

Following authors such as Bruno Latour (1993) and Sheila Jasanoff (2004), I shall argue that responsibility and ICTs are co-produced: the social and technological emerge in simultaneous and interconnected processes. Attempts to isolate either "responsibility" or "technology", and then work out the relations between them are not likely to get the picture right. Along with new technologies there also emerge distinct forms of sociality, ethics and justice, and hence also distinct notions of responsibility. Following Jasanoff and Kim I shall refer to such emerging landscapes through the concept of socio-technical imaginaries (Jasanoff and Kim 2009). I shall use the concept to describe what I see as mounting social

dividing lines in a number of fields using or developing ICTs. My examples are partly taken from a deliberative exercise on three emerging technologies (GIS, biometrics and human enhancements), carried out in the FP7 Technolife project (www.technolife.no). However, I shall also make reference to other technology- related events and developments, such as the recent Climategate controversy and Wikileaks. In a second section I describe and discuss the EU vision of biometrics, and I confront it with some of the issues that emerged in the previous section. I finish off with three broad-scoped recommendations for policy.

At the centre of many political controversies today stand differing imaginaries of information. By imaginaries of information I mean collective representations of what information is, what it should be, and how it relates to society and community. It seems simple to state what computers do in their most basic operations. Before the Internet they were complex calculators, useful for many things but fundamentally unconnected and isolated units. With increasing networking this role changed: computers now allow for collection, analysis, interconnection and sharing of information (i.e. enhanced end-to-end communication). As the Internet merged with an increasing number of social processes seeming simplicity fast changed into immense complexity. And, as the power of the medium dawned, states and corporations came to take a strong interest. As described by Lawrence Lessig, cyberspace is fast changing as a consequence of this:

> "...the invisible hand of cyberspace is building an architecture that is quite the opposite of its architecture at its birth. This invisible hand, pushed by government and by commerce, is constructing an architecture that will perfect control and make highly effective regulation possible" Lawrence Lessig, CODE 2.0

The Internet has become a zone of strong contestations, not simply over technology but over many of the life-forms with which it interacts. In the literature two models of the Internet are frequently invoked. Lessig himself speaks about "West coast code" and "East coast code", whereas Jonathan Zittrain and John Palfry (2008) refer to "the two Internets". According to Lessig west coast code is flexible, de-centralised, open and evades regulation; "east coast code", on the other hand, is strongly top-down and seeks to impose regulation on the ungovernable Wild West. One is centralised and imposes standardisation and control, and is associated with governmental hierarchies and large corporations. The other is bottom-up, highlights complexity and unpredictability, and so is easier associated with open and horizontal societies. Zittrain and Palfrey´s notion of the two Internets directly relate information to types of government: one grants and accepts "unfettered access to whatever" exists online (ibid., 1); the other introduces blockages and restrictions of access, frequently also increased surveillance.

The notion of the two Internets is a simplification: technologies unfold differently within different cultural and national contexts. It nevertheless seems to capture some general traits in a number of contexts, and so I shall stay with it for the purposes of this article. Not only that, I shall immediately extend the argument: I shall argue that we increasingly find these two imaginaries of information and social control within other, information-intensive contexts. Hence, I also make reference to biotechnology, controversies over climate change, the news media and controversies over interoperable biometric systems. My claim is that the two models of the Internet, through the ubiquity of information, increasingly seep into other areas where they blend with social and ethical concerns not initially connected with the Internet. In the course of diffusion they take on broad collective dimensions, and so the concept of (global) imaginaries is pertinent. Central to such debates and controversies are

questions such as: Who´s definitions of information do we presuppose; Who gets to define what counts as society, responsibility or justice? How do we imagine the complex relationships between "society" and ICTs? Through which medium is responsibility and innovation supposed to emerge: will it be through the courts, political debate, through the market, or perhaps through the technologies themselves?

The hacker imaginary

The controversy made up by Wikileaks was one powerful instance where centralised regimes of information control were confronted by bottom-up initiatives powered by the use of ICTs and media. Wikileaks is founded upon a certain view of what information can do for society, democracy and community:

> "Publishing improves transparency, and this transparency creates a better society for all people. Better scrutiny leads to reduced corruption and stronger democracies in all society's institutions, including government, corporations and other organisations... Scrutiny requires information. Historically, information has been costly in terms of human life, human rights and economics. As a result of technical advances particularly the internet and cryptography - the risks of conveying important information can be lowered" (http://213.251.145.96/About.html)

Underpinning this view is a certain diagnose of existing institutions and media: they fail to provide democracy, they thrive on secrecy and conspiracy and they are centralised to degrees approaching monopoly (or, more accurately, oligarchies). It also corresponds with a positive view of ICTs and the general public: if monopolies and secrecy can be broken, and if the public is given unfettered access to the truth, people will know what to do. Social and political empowerment will follow, and community will prosper. The popular and media responses triggered by Wikileaks were revealing: some remained sceptical and some sided with governments claims that the site should be shut down or banned. But many across the globe were sympathetic towards the goals of the organisation, and few were outright condemning. Whatever one thinks about their actions, it seems fair to say that Wikileaks gave a new voice to sentiments of growing disenchantment and alienation from existing institutions, long since observed in the sociological literature (Giddens 1990, Beck, Giddens, Lash 1996), and in policy documents (White Paper on Governance 2001).

Another case in point was Climategate, where unidentified persons hacked into the emails of leading climate change researchers at the East Anglia University and published them on the Internet. Although blamed on so-called climate sceptics, it is by no means certain that such groups were responsible. The revelations of dubitable scientific and moral practices and attitudes on the side of the researchers also gave some credit to a number of critics who were not opposing climate change as such, but who were sceptical of the power and influence of a few individuals and institutions in a highly complex and contested political field. In this case, the struggle over information is no side-product of the wider climate change debate itself: the conception of the climate system and its changing condition is generated through the interconnection of information about local climate systems worldwide, and this system is now organised around the IPCC reports and the models, methods and systems deployed by the climate research community (Miller 2004). The withholding of essential scientific information and of the codes used for modelling triggered action on the side of people who were concerned but not included in the community. One of the strongest instances of this was seen in the controversy over the data and software

underpinning the so-called hockey stick graph, i.e. the model of global warming made famous by Al Gore in his movie An inconvenient Truth.

We found similar imaginaries to be prominent in a deliberative exercise recently carried out as part of the FP7 Technolife project [1]. By the use of films and social media we mounted discussions over three emerging technologies: biometrics, geographical imaging systems and human enhancements. Discussions were kept open, a specific goal of the project being to avoid narrow framings of the debate and let participants voice their own opinions and concerns. In what follows I quote three of the responses we received in our online discussions. The first is from the biometrics forum, and addresses directly the ways in which governments and leading institutions relate (or not) to citizens in fundamental questions over social and technological development:

Participant A: "Why is there so little genuine debate on real causes of current crisis, biometrics, genetic engineering, consumption, fundamental economy? I cannot find any other cause but inertia. Inertia of outdated elitist doctrine of treating people like little kids who are unwilling/unable to accept complexity"

The topic of complexity was repeated by a number of participants, in many cases directly related to industrial/standardising modes of research and technological production, and the governance regimes that come along with them. A biotech researcher made the following entry:

Participant B: "There is another problem with "general product" scheme; as researchers this has two effects on us 1) It throws us into the lap of big establishments like militaries or big corporations and as a results the research efforts focus on satisfying their needs 2) Generalisation is in a way means simplification of the processes involved; so it reduces the amount of innovation put into the new advances (it also keeps their capacities low as a more complex system has a less chance of come through the excessive regulatory cycles). So in this sense tighter regulations will push us more to big companies as they will be the only ones with the necessary means to pass the regulations"

Finally, many would repeat the transformatory character of information, and its power to bring us into a new stage of development. Not unlikely the Wikileaks quote, the following participant highlights the sense that we find ourselves in the midst of a radical transformation, in which old institutions, concepts and ways of seeing the world are becoming fast obsolete

Participant C: "In this era of rapid and sweeping advancement, we see the old world struggling to guide and restrain the process of advancement into the new (next?) world....When we think about "biotechnology", the image that comes to mind most readily is that of white-coated scientists performing exhaustive experiments in sterile environments to make tiny incremental advances in their specific fields. More and more, however, computer technology and software are augmenting this process...we might see fully-automated virtual tools that let the layperson design unique organisms via their home computer, and distribute the fruits of their labors to all interested parties across the globe with one tiny command. When that day comes, Big Pharma will compete against the ubiquity of information and the will of the people, and it will lose"

1 A more complete account of the Technolife project can be found in Rommetveit, Gunnarsdottir et al. (forthcoming), and on www.technolife.no

In many postings on the Technolife forums, the imaginaries of the two Internets were repeated and re-interpreted in discussions over biometrics, biotechnology and human enhancements, many participants voicing similar opinions and concerns as quoted above. Although hardly a unitary group of people, many nevertheless seemed to share in a view of the character and role of information that closely resembles the hacker ethic (http://en.wikipedia.org/wiki/Hacker_ethic). The hacker ethic has been intrinsic to the development of the Internet, and to initiatives such as Open Source and the Free Software Movement. Common themes are sharing, openness, transparency and interconnectivity. Implicit is also a certain view of community as a direct relation to others, a connection that is strongly embedded in the just mentioned values. Consider this quote from one of the founders of the Free Software Movement, Richard Stallmann:

> "When I started working at the MIT Artificial Intelligence Lab in 1971, I became part of a software-sharing community that had existed for many years. Sharing of software was not limited to our particular community; it is as old as computers, just as sharing of recipies is as old as cooking" (quote from http://www.gnu.org/gnu/thegnuproject.html).

Stallmann then goes on to describe how this community was broken by the introduction of proprietary software. Strong proprietary east coast regimes of information, according to this view, are anti-community and detrimental to society. He quit his job at MIT and eventually started the Free Software Foundation and GNU (ibid.), hoping to re-invent and re-create his lost community.

The quoted participants seem to hold both government and big corporations in low esteem. On many occasions they also seem to conflate the two. So, it seems, did Lawrence Lessig in the passage quoted in the introduction of this text: east coast regimes of information express the interests of government and corporate America. But this imaginary may also imply certain simplifications: governments and corporations are not always in accordance (Lessig, a constitutional lawyer, is of course fully aware of the problem). For instance, proponents of neo-liberal regimes tend to be highly critical of public interest initiatives and government interventions, and to see them as major obstacles to innovation and entrepeneurship. Government officials, on the other hand, may see themselves as the last bulwark against total domination by corporations, as when the European Commission challenged the monopoly of Microsoft in 2005. However, the deeper problem is this: if binary positions come to occupy policy agendas, what room is left for democratic and long-term politics? I now turn to one case in which the corporate world and governments do indeed seem to work closely together, biometrics for travel and migration control.

Interoperable biometric systems in the European Union: seeing like a state?

In their most basic form, biometrics identifies people based on some "unique" characteristic, for instance the face, iris, fingerprints or behavioural characteristics (gait, typing on a keyboard etc.). Although deployable across a broad range of applications and by a number of different user groups, state security and state executive functions make up main areas of application (Lyon 2009). Hence, David Lyon uses the term (from James Scott) of seeing like a state to describe the ways in which biometrics render citizens and travellers eligible to state agencies. Following 9/11 the US Department of Homeland Security introduced strict requirements for members of the visa waiver programme to introduce biometrics in travel documents. The biometrics vision was pushed through at the highest of political levels:

through institutions such as the G8 and the ICAO (International Civic Aviation Organisation) interoperable biometric systems were introduced to governments world-wide. Within the European Union, especially the G8 member states (UK, Germany, France and Italy) played strong pro-active roles. This vision is now a central component of the EU Integrated Border Management Strategy (European Commission 2008). From the outset embedded in the east coast imaginary, it contained strong presumptions about the role and potential of interoperable information systems when placed at the service of governments. It was also inscribed with a strong political vision of the world, one (US) version of which goes as follows:

> "Allow me to share with you where I would like to see us move - toward a world that is banded together by security envelopes, meaning secure environments through which people and cargo can move rapidly, efficiently, and safely without sacrificing security or privacy. A world where, with the proper security vetting, the proper technology, the proper travel documents, and the proper tracking of cargo, it would be possible to move relatively freely from point to point all across the globe. For those within the security envelope, we will have a high degree of confidence and trust, so that trusted travellers and shippers don't have to be stopped at every point along the way to be re-vetted and rechecked. And that would enable us to focus more of our resources for those outside the security envelope - for the kind of in-depth analysis and the kind of in-depth vetting that is necessary to make sure those who seek to harm us do not slip through the cracks" (US Secretary of Homeland Security Michael Chertoff, quoted from European Commission 2005).

In a communication document from 2005, the Commission lamented the poor state of affairs for EU information systems, such as EURODAC, VIS, SIS and the planned SIS II[2], with regard to reaching such goals (European Commission 2005a). Among critical issues discussed were the lack of integration between national information systems across Europe, poor uses of EU-wide information systems, lack of use of biometric identifiers, no benefits to bona fide travellers and a lack of data on entries/exits into the Union. It was also recommended that different agencies be further integrated in their operations, that immigration and asylum authorities be granted access to EU systems, and also improved access for internal security and police to immigration, asylum and visa data. Finally, it was envisaged, increased interoperability of systems, through which many of the above problems were to be addressed, was to be managed by one EU agency, initially to be overseen by the Commission.

It seems unnecessary to dispute the necessity of collaborations between executive government branches following EU integration and removal of internal borders: clearly there is a need for police and internal security to foster closer collaboration following globalisation of crime and terrorism, but also normal migration and travel. Furthermore, biometrics can probably provide improved identification in a number of contexts and so help with a number of necessary state functions. But interoperable biometric systems in the above vision are also problematic for a number of reasons. The biometrics vision is a prime example of an "east coast" imaginary of the role and character of information. It is highly concerned with restricted access, in this case both to physical territories (the Schengen area) and to information, and it relies heavily upon information to separate friend from

2 Explanation of abbreviations: EURODAC: European Dactyloscopi, is an automated fingerprinting system for identifying asylum seekers and "irregular border crossers"; VIS: Visa Information System; SIS (II): Schengen Information System (II).

foe. Access to the systems is granted to government agencies only, but important roles are also given to industries implementing the systems. Strong presuppositions as to the social goods to follow from increased government access to information on individuals were embedded in the document:

> "Technically, "synergy" means a mutually advantageous conjunction of several elements. Economically, it means an increase in the value of assets or an economy of scale. Organisationally, "synergy" means combining previously distinct resources or streamlining the existing organisation so as to increase efficiency" (ibid., 3).

The biometrics vision and its related policies have been strongly criticised on a number of grounds, the most prominent being privacy and data protection. For instance, the Article 29 Working Party, consisting of all the data protection supervisory officers from the member states, were highly concerned about 1) the intention to create centralised databases on all passport holders in the Union; 2) the lack of clear purpose definition for biometric systems, resulting in an unclear legal situation; 3) the use of RFID chips as storage medium, and 4) a lack of clarity about who gets access to biometric information systems (Article 29 Working Party 2005). However, a number of other doubts and criticisms are also worth noticing, more related to the kind of social organisation that is being co-produced along with interoperable biometric systems. These concern both the process of introducing the technology and the kinds of organisational arrangements and implications that are likely to follow.

Firstly, there were a number of issues relating to the decision making process: The ordinary procedures of the European Council were not followed at crucial stages of decision making (Aus 2006); the European Parliament complained about not being sufficiently consulted, and civil society groups were not given access to information. In the words of a 2007 House of Lords Report on the Schengen Information System II:

> "It proved difficult for parliaments and civil society to obtain any access to texts under discussion, or to follow the progress of negotiations between the Council and the European Parliament... The lack of transparency in Council proceedings, and in co-decision negotiations between the Council and the European Parliament, is an issue relevant to all areas of EU policy-making, and has been particularly noticeable in the negotiations on the SIS II legislation" (House of Lords 2007, 15).

Secondly, there are clear indications that the decision to introduce biometric systems on the scale now undertaken was based more in needs to display political vigour than in technical capacity. The following statement is taken from a group of engineers that advised the Dutch government on the introduction of biometric passports:

> "The effectiveness of biometry is highly overrated, especially by politicians and policy makers. Despite rapid growth in applications, the large-scale use of biometry is untested. The difficulty is that it is not only unproven in a huge single application (such as e-passports), but also not with many different applications in parallel... The interference caused by the diversity of applications—each with its own security policy, if any—may lead to unforeseen forms of fraud" (Hoepman et al. 2006).

There was arguably a lack of consultation with democratic institutions, but many also claimed that there was a clear lack of consultation with technical expertise. This view was put forward by the Coelho report for the European Parliament LIBE committee: "It should

be emphasised that the European Council made a political decision to introduce biometric identifiers in EU passports without any input from practitioners and without knowing the magnitude of the problem..." (European Parliament 2004).

The seemingly simple solution offered by biometrics may turn out to generate complexities on a number of levels, both technical, political and organisational, and may jeopardise the synergies expected from interoperable systems. Signs of this can already be gleamed. For instance, the SIS II has been delayed by more than 5 years, and it still remains uncertain when, or indeed if, it will come into operation (European Council 2009). Although reasons for the delay are multiple, sheer complexity seems to make up a central problem. An EP LIBE background report described the SIS II as "complex and opaque project – hard to understand, even for experts and absolutely incomprehensible to citizens" (European Parliament 2005). Even Commission representatives admitted that "...the complexity of the project itself also had a negative impact on the planning" (House of Lords 2007, 13). Finally, complexities also emerge as industry tries to implement biometric systems within different EU legislative and operational cultures. Secrecy is a problem, as many member states do not want to share the information critically needed to establish interoperability in the first place. In one industry report it was warned that the

> "...lack of information concerning EU Member States large-scale projects does not bode well for biometrics deployment in the future as keeping this data secret could suggest that the systems are not secure, may hide poor error rates, be behind schedule or conceal unsatisfactory roll-out results" (Goldstein et al 2008, xi).

Although too early to pass judgment on large-scale biometric systems in the EU, the last sections indicate a number of problems of technical, political, ethical and economic nature. These problems can, in different ways, be connected to a specific imaginary of information, it´s socio-technical role and character, as well as the goals for which it may be deployed. According to this view, complex information can be gathered, controlled and distributed by government agencies in ways that turn out to the best for society. However, the search for a simple technical solution to a number of problems (terrorism, immigration and asylum, economic growth, visa processes, citizenship, etc.), may turn out to generate both technical, legal and organisational complexities on unprecedented scales. Secondly, the notion of information is connected to a certain view of social processes and the role of governance in which power, trust and information are uni-directional: citizens (and travellers and migrants) are obliged to trust government institutions (EU and state), but corresponding mechanisms through which government´s executive powers can be held in check are not implemented. It is, therefore, difficult to see how the biometrics innovation process could be described as a transparent, interactive process by which societal actors and innovators become mutual responsive to each other.

Concluding remarks and policy recommendations

ICTs and responsible innovation must be seen in the broadest possible terms, taking into account issues of social justice, distribution and sharing of resources, access to information and political decision-making. I brought up this argument in the introduction, and I claimed that notions of responsibility, community and justice, already intrinsic to the development of the Internet, are seeping into a number of other technology- and information intensive processes. I described two different information imaginaries, based in the hacker ethic and

in long-standing practices of state control. The extent to which these two competing and (by and large) incompatible world-views are valid descriptions of emerging socio-technical realities must remain an open and empirical question. There is little use doubting the presence of the state control imaginary: it has a long tradition in western societies. The hacker imaginary, on the other hand, is a more fleeting phenomenon: it surfaced in cases such as Wikileaks and Climategate, but parallels may also be drawn to as widely differing phenomenon as the recent uprisings in the Arab world and the Tea Party Movement in the US. All of these are strong expressions of discontent with growing social differences in which citizens no longer are able to identify with, nor access nor understand, the operations of the ruling elites. Hence, parallels may also be drawn to the rights movements in the 1960s and 70s. Growing distrust and discrepancies between elites and populations have been recognised also in the EU policy literature, as when the White Paper on Governance stated that "On one hand, Europeans want [politicians] to find solutions to the major problems confronting our societies. On the other hand, people increasingly distrust institutions and politics or are simply not interested in them" (European Commission 2001, 3). ICTs have the potential to help alleviate such problems, but this requires more complex, distributed and dialogical institutions, policies and technologies.

Privacy and data protection are not sufficient tools for governance of ICTs. This point is directly related to the previous: in many cases the possibilities for citizens or civil society to respond to and engage with ICT driven innovations are framed in terms of privacy and data protection. Far from wishing to deny the importance of these it must nevertheless be asked to what degrees they correspond with underlying concerns of individuals, communities and populations. For instance, one could ask why emerging values of connectivity and sharing are so widely embraced, for instance by Facebook users. Richard Stallmann started the Free Software movement in order to (re-) establish a sense of community. Irrespective of whether social media are the proper means for doing so or not: the wish to connect and share could turn out just as important (to people and governance alike) as privacy, originally defined as the right to be left alone (Warren and Brandeis 1890).

Expanding further on this point: the result of placing the hacker imaginary alongside the state control imaginary was the realisation that the two imagine and value most aspects of information differently. In the EU biometrics context, the main policy metaphor has become that of "balancing privacy and security" (Liberatore 2007, Balzacq and Carrera 2006). However, the validity of that metaphor presupposes taking the state imaginary of information for granted, i.e. it presupposes that information can fundamentally be contained and controlled. According to the hacker imaginary, it is based in an outdated view of information´s role and potential. Insofar as people hold different views of information, as seen in the hacker imaginary, the metaphor is not valid. This view is also supported by empirical findings into the public understanding of security technologies. The view that privacy and security can somehow be balanced in a trade-off model is a simplification of the ways in which people think and deliberate about security-related technologies (Pavone and Deglio 2010). This points to the need for both increased efforts to understand public perception in ICT related fields, and for implementing institutions that can mediate public perception and concern.

Responsible innovation in ICTs should be accomplished through the establishment of broad, Europe-wide platforms for deliberation and inclusion of citizens and civil society. In spite of Europe-wide initiatives such as the ICT 2020 agenda, at present there are few or no mediating institutions in which ICT-related issues can be discussed on a European level. This should be seen as one main arena in which the European Union can add real value,

as implied by the subsidiary principle. There are a number of good reasons for increasing deliberation, many of which have been touched upon in this article. First, issues of social justice and cohesion are prominent: a number of events have already made clear that, where large segments of society are left out, those with the resources and knowledge will nevertheless use ICTs to make themselves heard and to influence development from outside existing institutions. In this context, practices, experience and knowledge gained through a number of science in society related disciplines, practices and institutions (especially foresight, ethics and public participation), have important roles to play. Realising this potential entails recognising the highly social character of ICTs and to adjust experience and knowledge gained in other fields to these specific challenges.

References

Article 29 Working Party, Opinion on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. Brussels, September 2005.

Aus, J. P. 'Decision Making under Pressure: The Negotiation of the Biometric Passport in the Council', in, *Centre for European Studies Working Paper*. Oslo: University of Oslo 2006.

Balzacq, T. and Carrera, S. (eds) *Security versus Freedom? A Challenge for Europe's Future*. Aldershot: Ashgate 2006.

Beck, U., Lash, S., Giddens, A. Reflexive Modernisierung. Eine Kontroverse. Frankfurt am Main: Suhrkamp Verlag 1996.

European Commission. White Paper on Governance. Brussels 2001.

European Commission. Press release on US – EU collaborations, Brussels 2005.

European Commission. *Commission Communication of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs* COM (2005) 597 final. Brussels 2005b.

European Council. Council conclusions on the further direction of SIS II 2946th JUSTICE and HOME AFFAIRS Council meeting Luxembourg, 4 June 2009.

European Commission. New tools for an integrated European Border Management Strategy. Brussels 2008.

European Parliament. Committee on Civil Liberties, Justice and Home Affairs. Rapporteur: Carlos Coelho, A6-0028/2004. Report on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports. Brussels 2004.

European Parliament, Committee on Civil Liberties, Justice and Home Affairs. Background paper: 'Schengen Information System' of 10 April 2005. Retrieved from www.europarl.eu.int/comparl/libe/elsj/zoom_in/25_en.htm

Giddens, A. The Consequences of Modernity. Stanford, California: Stanford University Press 1990.

Goldstein et al. "Large-scale Biometrics Deployment in Europe: Identifying Challenges and Threats". European Commission, Joint Research Centre Institute for Prospective Technological Studies. Seville 2008.

J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R. W. Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. In Advances in Information and Computer Security, LNCS. New York: Springer-Verlag 2006.

House of Lords 'Schengen Information System II (SIS II). Report with Evidence'. London: House of Lords, European Union Committee 2007.

Jasanoff, S. States of Knowledge: The Co-Production of Science and Social Order. London: Routledge 2004.

Jasanoff, S., Kim, S-Y., *Containing the Atom: Sociotechnical Imaginaries and Nuclear Power in the United States and South Korea*, Minerva, Online 26 June 2009.

Kjølberg, K. "The notion of 'responsible development' in new approaches to governance of nanosciences and nanotechnologies". PhD Thesis. Bergen: University of Bergen 2010.

Latour, Bruno. 1993. We Have Never Been Modern. New York: Harvester Wheatsheaf.

Liberatore, A. 'Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union', *Eur J Crim Policy Res* 13 2007.

Lessig L. *CODE VERSION 2.0*. New York: Basic Books; 2006.

Lyon D. *Identifying Citizens. ID Cards as Surveillance*. Oxford: Polity Press; 2009.

Macnaghten, P., Davies, S., Kearnes, M. *Narrative and Public Engagement: Some Findings from the DEEPEN Project*. In: von Schomberg and Davies, S. "Understanding Public Debate on Nanotechnologies. Options for Framing Public Debate", European Commission, Brussels 2010.

Miller, C. "Climate science and the making of a global political order." In States of knowledge: the co-production of science and social order, ed. S. Jasanoff. Milton Park, Abingdon: Routledge 2004.

Pavone, V., Esposito, S. D. "Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security". *Public Understanding of Science* published online 26 August 2010.

Rommetveit, Gunnarsdóttir et al: "The Technolife Project: An experimental approach to new ethical frameworks for emerging science and technology", forthcoming The International Journal of Sustainable Development.

Warren S, Brandeis L. The Right to Privacy. *Harvard Law Review* 1890: IV(5). Retrieved from http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

Zittrain, J. and Palfry, J. Introduction. In Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, (Cambridge: MIT Press) 2008.

CHAPTER 5
Precaution and privacy impact assessment as modes towards risk governance

David Wright, Raphaël Gellert,
Serge Gutwirth & Michael Friedewald

Introduction

A key objective of the PRESCIENT project is to develop a privacy impact assessment.[1] This paper describes some of the PRESCIENT consortium's considerations towards that end.

A privacy impact assessment can be seen as a tool for responsible research and innovation (RRI). RRI can be defined as a "transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view on the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products in order to allow a proper embedding of scientific and technological advances in our society".[2] Such a definition is close to how one could define privacy impact assessment (PIA), i.e., PIA is a process of engaging stakeholders in order to consider how privacy might be impacted by the development of a new technology, product, service, project or policy and what measures could be taken to avoid or mitigate unwanted effects.

This paper contends that PIAs are an instrument of risk governance that should, therefore, be understood and implemented within the framework of the precautionary principle. Precaution is the best theoretical framework of action in the face of uncertain risks. After considering the precautionary principle from a conceptual point of view, this paper goes on to discuss privacy impact assessment in practice and concludes with the possibility of the integration of PIA within the context of risk governance. The paper also offers comments on the notion of balancing privacy and other values.

The precautionary principle

The precautionary principle was born from a turn in the societal discourse over the effects of technological and scientific development. Indeed, as illustrated by the Chernobyl catastrophe, it became clear that technical progress could also equate to danger for human health and the environment.[3] It is in this respect that sociologist Ulrich Beck coined the term "risk society" to designate modern societies, since the latter are characterised by a public debate largely focused on the management of technology-derived risks.[4]

As evidenced by Dominique Bourg, the nature of technical progress as such has changed over the second half of the 20th century. Technical innovation has dramatically increased,

1 The PRESCIENT (Privacy and Emerging Sciences and Technologies) project is funded under the EU's Seventh Framework Programme for research and technological development (SIS-CT-2009-244779). For an overview of the PRESCIENT project, see Friedewald, Michael, David Wright, Serge Gutwirth and Emilio Mordini, "Privacy, data protection and emerging sciences and technologies: towards a common framework", *Innovation - The European Journal of Social Science Research*, Vol. 23, No. 1, March 2010.

2 See René von Schomberg's introduction to this volume. The notion of RRI was coined in the context of the Frontiers Technology Assessment Network of Excellence. See, for instance, Robinson, Douglas K.R., "Co-evolutionary scenarios: An application to prospecting futures of the responsible development of nanotechnology", *Technological Forecasting and Social Change*, Vol. 76, No. 9, November 2009, pp. 1222-1239.

3 Hilty, Lorenz M., Siegfried Behrendt, Mathias Binswanger et al., "The Precautionary Principle in the Information Society: Effects of Pervasive Computing on Health and Environment", TA 46e/2005, TA-Swiss, Centre for Technology Assessment, Bern, 2005. http://www.ta-swiss.ch/www-remain/reports_archive/publications/2005/050311_STOA125_PvC_72dpi_e.pdf. .

4 Beck, Ulrich, *Risk society – towards a new modernity*, Sage, London, 1992; Godard, Olivier, "Le principe de précaution, une nouvelle logique de l'action entre science et démocratie", *Philosophie Politique*, No. 11, May 2000, p. 21.

due to the correlative restless multiplication of new fields of knowledge and expertise. This, in turn, has created a situation where there is no complete mastery of the effects and/or consequences of such innovation. This situation, which differs from the one where all the causes and consequences concerning a particular technique are (thought to be) known, has paved the way to a phenomenal world that is characterised by the inadequate awareness of the effects and consequences of a particular technique; in other words, that is characterised by unpredictability and *uncertainty*.[5]

Such a shift from a situation wherein well-defined risks that could trigger a carefully planned course of actions (in line with the "principle of prevention", i.e., known risks can be prevented)[6] to a situation wherein risks become potential and uncertain, draws the limit of danger aversion strategies apparent, and spurs the need for a new framework of action: the precautionary principle.

Definition

The precautionary principle has been enshrined in various international legal texts, such as the Rio Declaration,[7] the Treaty on the Functioning of the European Union (TFEU),[8] in the WTO Sanitary and Phytosanitary (SPS) Agreements[9] as well as in national legislation, such as the French Barnier Act of 1995,[10] or the French Constitution.[11]

A satisfying definition of the principle has been provided in the academic discourse, and it has been suggested European policy makers should use it. According to this definition, the precautionary principle is the principle whereby, "following an assessment of available scientific information, there are reasonable grounds for concern for the possibility of adverse effects but scientific uncertainty persists, provisional risk management measures based on a broad cost/benefit analysis whereby priority will be given to human health and the environment, necessary to ensure the chosen high level of protection in the Community and proportionate to this level of protection, may be adopted, pending further scientific information for a more comprehensive risk assessment, without having to wait until the reality and seriousness of those adverse effects become fully apparent".[12]

5 Bourg, Dominique, "Le principe de précaution: un moment particulier de la philosophie de la technique", Seminar 'Le principe de précaution. Comment le définir, comment le faire appliquer?', Université Libre de Bruxelles, 1999, *in* Godard, op. cit., p. 7.

6 Cf. de Sadeleer, Nicolas, *Les principes du pollueur-payeur, de prévention et de précaution. Essai sur la genèse et la portée de quelques principes du droit de l'environnement*, Bruylant, Brussels,1999.

7 Principle 15 of the UN Conference on Environment and Development (UNCED) in Rio de Janeiro 1992 (Rio Declaration).

8 Art. 191, 11, 114.3, and 168.1 of the TFEU.

9 WTO Agreement on the Application of Sanitary and Phytosanitary Measures (SPS), art. 5.7.

10 Barnier Act of 1995 on the reinforcement of the protection of the environment (95-101).

11 Environment Charter, art. 5.

12 Von Schomberg, René, "The Precautionary Principle and its normative challenges", *in* Fisher, E., Jones, J., and von Schomberg, R., (eds), *Implementing the Precautionary Principle: Perspectives and Prospects*, Cheltenham, UK and Northampton, MA, US: Edward Elgar, 2006, p. 47.

In other words, the precautionary principle should guide governments' actions in situations characterised by risks that are not constitutive of acute dangers. Its purpose is to minimise risks that are not presently acute but that may become evident only in the longer term, and hence to maintain a margin for future developments.[13]

Kourilsky distinguishes between potential risks (i.e., uncertainties) and proven risks (i.e., acute dangers). The former will trigger a government response based upon the precautionary principle, whereas the latter will lead to a decision taken in the framework of the danger aversion principle (i.e., prevention).[14] As Godard puts it, the precautionary principle aims not only at dangers and risks whose causes are undetermined, but whose very existence is problematic and not yet ascertained.[15]

Its scope of action has been historically associated to environmental and human health matters. However, this is not an exhaustive list, and the principle has now been extended to consumer protection policy, but also to broader societal issues, including that of changes in moral principles. In this respect, the use of the precautionary principle in matters of pervasive computing and its implications in matters of privacy and data protection appears as logical.[16]

Precaution as a principle for immediate action

In its judgment on the validity of the Commission's decision banning the exportation of beef from the United Kingdom due to fears of BSE transmission, the ECJ has ruled that, "where there is uncertainty as to the existence or extent of risks to human health, the institutions may take protective measures without having to wait until the reality and seriousness of those risks become fully apparent."[17]

The precautionary principle thus commands that, in the face of a potential or anticipated risk, action must be taken at the earliest possible stage.

As Latour points out, the precautionary principle breaks the traditional link between scientific knowledge and action. Whereas danger aversion (i.e., prudence or prevention) entails that no action be taken before a complete knowledge of a situation is reached, the precautionary principle requires immediate action, though based upon criteria other than the sole knowledge of the causes and consequences of the concerned phenomenon. In other words, by disjoining (or disentangling) political action and scientific expertise, the precautionary principle is a new mode of governmentality based upon the necessity

13 Hilty et al. 2005, p. 27

14 de Sadeleer, op. cit., *passim*; Kourilsky, Philippe, *Du bon usage du principe de précaution*, Odile Jacob, Paris, 2002, p. 51.

15 Godard, op. cit., p. 6.

16 Hilty et al., op. cit., p. 29.

17 Judgment on the validity of the Commission's decision banning the exportation of beef from the United Kingdom to reduce the risk of BSE transmission (Judgments of 5 May 1998, cases C-157/96 and C-180/96), ground 63.

to take swift actions and decisions in situations of uncertainty.[18] In this respect, the precautionary principle is a *principle of action*.[19]

Understanding precaution as a principle of action requires determining the kind of actions that can be taken. Some procedural principles can be of help in this respect, such as comparing the merits and costs of different approaches or the need to take provisional measures (i.e., measures that can be revisable according to the evolution of scientific knowledge).[20]

As the European Commission points out, "recourse to the precautionary principle does not necessarily mean adopting final instruments designed to produce legal effects".[21] On the contrary, the appropriate response in a given situation is the result of an eminently political decision that weighs the acceptable level of risk that can be imposed on society, considering the particular risk at hand. Hence, in the face of a potential risk, the decision not to take any action may also be a valid response. Equally, the funding of a research programme or the decision to inform the public of the possible dangers of a phenomenon are also part of this wide range of actions that can be taken under the precautionary principle.[22]

Precaution and participation

A last issue of particular interest (especially in the light of PIAs) concerns the participation of stakeholders, including the public, in the decision-making process.[23]

One can ask why citizens should contribute to decision-making in the framework of the precautionary principle. The key for understanding this lies partly in the need to compensate for the deficiencies of political representation. Indeed, political representation in so-called modern democracies is characterised by an asymmetrical exposure to risk: political decisions will first and foremost affect citizens. Therefore, citizens might eventually criticise political officials, not simply for the fact that decision-making in situations of uncertainty inherently carries an irreducible element of risk, but more particularly for the behaviour of such officials who, because of personal interest, turpitude or negligence, happen to engage in paternalistic attitudes that resort to lenient justification or even to the concealment of risk-creating decisions that might affect large parts of the population without the latter

18 Latour, Bruno, "Prenons garde au principe de precaution", *Le Monde*, 1 Jan 2000. http://www.bruno-latour.fr/presse/presse_art/008.html

19 Godard, op. cit., pp. 10-11.

20 Ibid., pp. 57-66. It is unsurprising that Callon et al. have resorted to the expression "measured action", to design decision-making in this framework. See Callon, Lascoumes and Barthe, op. cit., chapter 6.

21 European Commission, Communication from the Commission on the precautionary principle, COM(2000) 1 final, 2 February 2000, p. 15. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0001:FIN:EN:PDF

22 Kourilsky, op. cit., pp. 57-66.

23 Ibid., pp. 75-76.

benefiting from them whatsoever.[24] In other words, citizens have the right to be associated with decisions that carry risk for them (which the current state of political representation doesn't always fully permit).

The question remains as to what level of participation citizens should be entitled. Should it be a "simple" right of information or a fully-fledged participatory right?

In order to answer this question, it is necessary to turn to another procedure governing the precautionary principle. This procedural principle is based upon the evidence that situations of uncertainty (i.e., potential risk) are not based upon a complete ignorance of the situation, but the incompleteness of knowledge re theses situations.[25] Therefore, it is crucial to take into consideration all points of view, even the views of a minority, in order to have as complete a picture of the situation as possible. It is in this respect that the European Commission has recommended that, "even if a scientific opinion is supported by a minority fraction of the scientific community, due account should be taken of their views."[26]

The link between such an all-encompassing approach towards risk knowledge and citizens' participation goes as follows. The so-called risk society results partly from an ever-increasing complexity of technical and scientific knowledge that has gone beyond our control. Hence, as Godard argues, our management of risk cannot solely be based upon scientific knowledge. Setting aside scientific rationality, however, doesn't mean cutting all links with reason to be replaced by a heuristics of fear, for example.[27] Rather, it consists in anchoring decision-making into a new rationality, based upon collective deliberation, which is better equipped than pure scientific expertise to deal with situations of uncertainty.[28]

We now turn our attention to privacy impact assessment, which can be seen, in some sense, as an exercise in precaution, but especially as a form of risk governance.

Privacy impact assessment

Several privacy impact assessment methodologies already exist – Australia, Canada, New Zealand, the UK and the US have developed PIA policies and guidelines. The ISO has produced a standard for PIAs in financial services.[29] Interest in PIAs in Europe is growing. The European Commission's Recommendation on RFID included an article which called upon Member States and industry "in collaboration with relevant civil society stakeholders" to develop a PIA framework for RFID to be submitted for endorsement to the Article 29 Data

24 Godard, op. cit., pp. 15-16.

25 Ibid., p. 15.

26 European Commission, 2000, p. 16.

27 As put forward by Jonas. See, Jonas, Hans, *Le principe de responsabilité. Une éthique pour la civilisation technologique*. Éditions du Cerf, Paris,1990.

28 Godard, op. cit., pp. 16-19, especially p. 19.

29 ISO 22307:2008: Financial services -- Privacy impact assessment, 16 Apr 2008. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40897

Protection Working Party within 12 months (i.e., by May 2010).[30] Industry duly drafted a PIA for RFID. Although the Art. 29 WP rejected the first draft[31], it eventually agreed a subsequent draft in February 2011.[32]

There are other indications of a growing interest in PIA. European Commission Vice-President Viviane Reding said in July 2010 that "Businesses and public authorities... will need to better assume their responsibilities by putting in place certain mechanisms such as the appointment of Data Protection Officers, the carrying out of Privacy Impact Assessments and applying a 'Privacy by Design' approach.[33]

The European Parliament, in its 5 May 2010 resolution on Passenger Name Records, said that "any new legislative instrument must be preceded by a Privacy Impact Assessment and a proportionality test".[34]

Finally, the European Commission has said it will examine the possibility of including in its new data protection framework "an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance".[35]

The interest in PIAs is growing, in part because of the perceived benefits, among which the following have been commonly cited:

- Building public trust:
  - Identifying and managing risks – Undertaking a PIA will help industry and government to foresee what the media and the public will accept in regard to impacts on privacy. With the growth in data-intensity and increasing use of

30 European Commission, Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C (2009) 3200 final, Brussels, 12 May 2009. http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

31 Article 29 Data Protection Working Party, Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Adopted on 13 July 2010. http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm

32 Art. 29 Data Protection Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Brussels, Adopted on 11 February 2011.

33 Reding, Viviane, Vice-President of the European Commission responsible for Justice, Fundamental Rights and Citizenship, "Towards a true Single Market of data protection", SPEECH/10/386, Meeting of the Article 29 Working Party «Review of the Data protection legal framework» Brussels, 14 July 2010. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/386

34 European Parliament, Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0144+0+DOC+XML+V0//EN

35 European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, Brussels, 4.11.2010. http://ec.europa.eu/justice/news/intro/news_intro_en.htm#20101104

privacy-intrusive technologies, the risks of a project or scheme being rejected by the public are increasing.
  - Avoiding loss of trust and reputation – A PIA will help an organization's reputation and avoid deploying a system with privacy flaws which attract negative attention from the media, competitors, public interest advocacy groups, regulators and customers. Retrospective imposition of regulatory conditions may put the entire project at risk. A PIA provides an opportunity to obtain commitment from stakeholders early on and to avoid the emergence of opposition at a later, more costly stage.
  - Providing a credible source of information to assuage alarmist fears and alerting the complacent to potential pitfalls.
  - Achieving a better balance among conflicting interests.
  - Improving public awareness and making available more information about an envisaged system, service or project.

- Complying with national and international regulations:
  - Avoiding unnecessary costs – By performing a PIA early, an organization avoids problems being discovered at a later stage, when the costs of making significant changes or cancelling a flawed project outright are much greater.
  - Imposing the burden of proof for the harmlessness of a new technology, process, service or product on its promoters.

- Avoiding risky investments:
  - Avoiding inadequate solutions – Solutions devised at a later stage are often not as effective at managing privacy risks as solutions designed into the project from the start. "Bolt-on solutions devised only after a project is up and running can often be a sticking plaster on an open wound."[36]
  - Understanding the perspectives of stakeholders – Inputs from stakeholders may lead to a better-designed project, the difference between a privacy-invasive and a privacy-enhancing project, and pre-empt possible misinformation campaigns by opponents.
  - Improving security of personal data and making life more difficult for cyber criminals.[37]

The PRESCIENT consortium is examining these different initiatives, particularly those of the above-mentioned countries, to identify the best features of existing PIAs and, based on those, to produce a framework that integrates those "best" features. As PIAs are used in several different countries, it's not surprising that there are some differences in the process – when they are triggered, who conducts the process, the reporting requirements, the scope, the involvement of stakeholders, accountability and transparency.

PIAs can be distinguished from compliance checks, privacy audits and "prior checking". A compliance check is to ensure a project complies with relevant legislation or regulation. A privacy audit is a detailed analysis of a project or system already in place which either confirms that the project meets the requisite privacy standards or highlights problems

36 The quote comes from: Information Commissioner's Office (ICO), Privacy Impact Assessment Handbook, Version 2.0, June 2009, chapter I. http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

37 These benefits have been adapted from the ICO PIA handbook, op. cit., and from Stewart, Blair, *Privacy Impact Assessment Handbook*, Office of the Privacy Commissioner, Auckland, June 2007.

that need to be addressed.[38] Another important term to distinguish in this context is "prior checking", which appears in Article 20 of the European Data Protection Directive and which says in part that "Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof".[39]

While the approaches to privacy impact assessment are somewhat similar – i.e., the PIA process aims at identifying impacts on privacy before a project is undertaken – there are also important differences. In December 2007, the UK became the first country in Europe to publish a privacy impact assessment handbook. The Information Commissioner's Office (ICO) published a second version in June 2009.[40] Before publication of its PIA handbook, ICO commissioned a set of studies by some of the world's leading PIA experts, including Colin Bennett, Robin Bayley, Roger Clarke and Andrew Charlesworth.[41] They examined the PIA practices in Australia, Canada, Hong Kong, New Zealand and the US before making their recommendations. Thus, in some ways, the UK has one of the most advanced PIA methodologies. It is especially distinguished by its emphasis on engaging stakeholders at an early stage.

Because organisations vary greatly in size and experience, and as the extent to which their activities might intrude on privacy also varies, the ICO says it is difficult to write a "one size fits all" guide. Instead, it envisages each organization undertaking a privacy impact assessment appropriate to its own circumstances.[42]

The ICO says the privacy impact assessment process should begin as soon as possible, when the PIA can genuinely affect the development of a project. The ICO uses the term "project" throughout its handbook, but clarifies that it could equally refer to a system, database, program, application, service or a scheme, or an enhancement to any of these, or even draft legislation.

The ICO envisages a privacy impact assessment as a process that aims to:

- identify a project's privacy impacts,
- understand and benefit from the perspectives of all stakeholders,
- understand the acceptability of the project and how people might be affected by it,
- identify and assess less privacy-invasive alternatives,
- identify ways of avoiding or mitigating negative impacts on privacy,
- document and publish the outcomes of the process.[43]

38 Warren, Adam, Robin Bayley, Colin Bennett, Andrew Charlesworth, Roger Clarke and Charles Oppenheim, "Privacy Impact Assessments: International experience as a basis for UK Guidance", *Computer Law and Security Report*, Vol. 24, 2008, pp. 233-242.

39 European Parliament and the Council, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Brussels, 24 Oct 1995.

40 Op. cit.

41 Bennett, Colin, Robin Bayley, Roger Clarke, and Andrew Charlesworth, "Privacy Impact Assessments: International Study of their Application and Effects", Report for the Information Commissioner's Office, United Kingdom, Linden Consulting, Inc., 2007. http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_apph_eur_2910071.pdf

42 ICO PIA handbook, op. cit., p. 2.

43 ICO PIA handbook, op. cit., p. 7.

The PIA process starts off with an initial assessment, which examines the project at an early stage, identifies stakeholders and makes an initial assessment of privacy risks. The ICO has appended some screening questions to its handbook the answers to which will help the organization decide whether a PIA is required, and if so, whether a full-scale or small-scale PIA is necessary.

A full-scale PIA has five phases:

In the **preliminary phase,** the organisation proposing the project prepares a background paper for discussion with stakeholders, which describes the project's objectives, scope and business rationale, the project's design, an initial assessment of the potential privacy issues and risks, the options for dealing with them and a list of the stakeholders to be invited to contribute to the PIA.

In the **preparation phase,** the organisation should prepare a stakeholder analysis, develop a consultation plan and establish a PIA consultative group (PCG), comprising representatives of stakeholders.

The **consultation and analysis phase** involves consultations with stakeholders, risk analysis, identification of problems and the search for solutions. Effective consultation depends on all stakeholders being well-informed about the project, having the opportunity to convey their views and concerns, and developing confidence that their views are reflected in the outcomes of the PIA process.

The **documentation phase** documents the PIA process and outcomes in a PIA report, which should contain

- a description of the project,
- an analysis of the privacy issues arising from it,
- the business case justifying privacy intrusion and its implications,
- a discussion of alternatives considered and the rationale for the decisions made,
- a description of the design features adopted to reduce and avoid privacy intrusion and the implications of these features,
- an analysis of the public acceptability of the scheme and its applications.

The **review and audit phase** involves a review of how well the mitigation and avoidance measures were implemented.

Because projects vary greatly, the handbook also provides guidance on the kinds of projects for which a small-scale PIA is appropriate. The phases in a small-scale PIA mirror those in a full-scale PIA, but a small-scale PIA is less formalised and does not warrant as great an investment of time and resources in analysis and information-gathering. An important feature of the PIA as envisaged by ICO is that it should be transparent, accountable, include external consultation where appropriate, and make reports publicly available.

While the UK PIA is very sophisticated, it does fall short of the US requirement that government agencies publish their PIAs on their websites. In Canada, government departments are required to publish summaries of their PIAs. In both countries, government departments are required to include a PIA when making submissions for funding, to the Treasury Board in the case of Canada and to the Office of Management and Budget (OMB) in the case of the US.

In the UK, there is no such requirement. In Canada, if the Treasury Board (which is also the guardian of the PIA policy) does not find a PIA to be adequate, it can turn down funding until the government department improves the PIA. Also in Canada, unlike the UK, government departments are required to send a copy of the PIA to the Office of the Privacy Commissioner (OPC), and the OPC has the power to conduct an independent audit of the government departments' PIA practices – and it has done so, as has the Governmental Accounting Office (GAO) in the US. While ICO does not know who has carried out PIAs, the OPC has called for a central registry of all (government-performed) PIAs.

Issues of balancing

Another procedural principle concerning action in the framework of precaution requires actors to make cost/benefit analyses between the different courses of action (or inaction) possible, and the different values at stake.[44] As indicated above, PIAs also resort to this type of operation. Hence, there is a need to clarify what constitutes a sound proportionality (i.e., balancing) test.

The traditional position regarding the balancing of conflicting fundamental rights and/or values leads to a catch. According to this view, balancing consists in simply opposing two values; it assumes that supporting one interest *ipso facto* weakens the other, that it is only possible to uphold one at the expense of the other.[45]

Such a position, which might be coined as "weak balancing", loses sight of the broader context in which such choices operate: the democratic constitutional State. The mission of such a State is precisely to nurture a wide range of values and principles, some of which (e.g., privacy and security) conflict at times.

Therefore, the aim of any balancing is not to weigh one right against another, but more precisely, to *reconcile* the multiple values that constitute the backbone of the democratic State in such a way that it is possible to organise a *cohabitation* between them that is as respectful as possible of the principles of the democratic constitutional State. In other words, the point of striking a balance between two values (whose antagonism might be irreducible at some point) is to preserve and enforce both of them in the best possible way.

In this respect, lessons can be drawn from the system of the European Convention of Human Rights (ECHR). Within this system, some rights enshrined therein – among which

44 Kourilsky, op. cit., pp. 56-67. See also, European Commission, 2000, op. cit., pp.16-19, especially p. 17.

45 In most of its case law regarding article 8 of the Convention, the European Court of Human Rights has adopted such a stance. When assessing the conformity of measures breaching the right to privacy, it has either refused to undertake a balancing by expanding the legality criteria or, when it has undertaken a balancing, it has only considered the more formal part of the test embodied by the proportionality test, which supports a classical, "weak balancing" perspective, see *infra,* next paragraph. De Hert, Paul, and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action", in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing data protection?*, Springer, Dordrecht, 2002, pp. 20-24; De Hert, Paul, "Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11", *Utrecht Law Review*, 2005, Vol. 1, No. 1, pp. 91-93.

is article 8 which hallows the right to privacy[46] – can only be derogated under certain conditions, namely, that the derogation must be foreseen by law, must respond to one of the legitimate aims listed in article 8.2 (in the case of privacy),[47] be necessary in a democratic society and be proportionate to the aim pursued.[48]

Although all conditions must be fulfilled for a measure to infringe upon article 8, the core of the balancing process lies in the last two parameters: the "necessity in a democratic society" and the proportionality criteria.[49]

The Convention also contains the elements for a better, stronger balancing, which are embodied in the "necessary in a democratic society" condition. This means that when weighing two values, one has to ask whether the proposed measure is acceptable from a constitutional viewpoint since it might harm the very essence of the fundamental right in balance. Rather than bluntly balancing two opposing rights, the question becomes: "How much erosion of a fundamental right is compatible with the democratic constitutional State?" (given that fundamental rights are an inherent part of the latter) or "In which society do we want to live?". Equally, such a substantial, value-loaded test should lead us to ask ourselves whether there are alternative measures that, although leading to the same result (the nurturing of a certain value), do not affect other potentially conflicting fundamental rights. In other words, is there a way to protect and enforce both values without loss at the fundamental rights level? Is there a way to enforce two conflicting values without encroaching upon either? [50]

Such a strong balancing is better equipped to achieve the necessary *reconciliation* or *cohabitation* that must prevail between (sometimes) conflicting values that lie at the heart of the social contract from which stems the democratic constitutional State.

Consulting and engaging stakeholders

A process for engaging and consulting with stakeholders should be put in place to help policy-makers, technology developers and project managers in ensuring that privacy issues

46 Article 8.1 states that "Everyone has the right to respect for his private and family life, his home and his correspondence."

47 i.e., "The interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

48 Article 8.2 only foresees the three first conditions, but the Court of Strasbourg has added the last one through its case law. See, Van Gerven, W., "Principe de proportionnalité, abus de droit et droits fondamentaux", *Journal des Tribunaux*, 1992, pp. 305-309; Ganshof Van Der Meersch, W.J., "Propos sur le texte de la loi et les principes généraux du droit", *Journal des Tribunaux,* 1970, pp. 557-574 and pp. 581-596; Eissen, M.-A., "The Principle of Proportionality in the Case-Law of the European Court of Human Rights" in Macdonald, R. St J., F. Matscher and H. Petzold (eds.), *The European System for the Protection of Human Rights*, Martinus Nijhoff, Dordrecht, 1993, pp. 125-37, especially p. 127.

49 De Vries, Katja, Rocco Bellanova, Paul De Hert and Serge Gutwirth, "The German Constitutional Court Judgment on data retention: proportionality overrides unlimited surveillance (doesn't it ?)", in Serge Gutwirth, Yves Poullet, et al. (eds.), *Privacy and data protection: an element of choice*, Springer, Berlin, 2011 [forthcoming], pp. 14-15.

50 Ibid., p. 15.

are identified, discussed and dealt with, preferably as early in the project development as possible. Of course, companies are not obliged to be as "democratic" and participatory as governments in developed countries have to be. And the involvement of stakeholders in the development is notoriously difficult and costly even if the products, services or policies have the potential for intrusion on privacy or are ethically dubious. Furthermore, competition in the private sector, especially in the development and promotion of new products and services, often involves secrecy in the early stages.

Nevertheless, there are various reasons why project managers should engage stakeholders and undertake a consultation when developing new technologies or projects. For one thing, Article 41 of the Charter of Fundamental Rights of the European Union, entitled the right to good administration, makes clear that this right includes "the right of every person to be heard, before any individual measure which would affect him or her adversely is taken", which suggests that consultation with stakeholders is not only desirable but necessary.

But there are other reasons too. Stakeholders may bring new information that the policy-maker, technology developer or project manager might not have considered and may have some good suggestions for resolving complex issues.[51] Also, technology development is often too complex to be fully understood by a single agent, as Sollie and others have pointed out.[52] Palm and Hansson state that "It would be delusive to believe that technology developers are conscious of all the effects of their products. In many cases, negative side effects come as a surprise to technology developers themselves. If they could have anticipated the negative consequences, they would, in the vast majority of the cases, have done their best to avoid them out of social concern or for commercial reasons, or both."[53] Furthermore, by engaging stakeholders, project managers may avoid subsequent criticism about a lack of consultation. Engaging stakeholders before the project is implemented may be a useful way of testing the waters, of gauging the public's reaction to the project. In any event, "A central premise of democratic government – the existence of an informed electorate – implies a free flow of information."[54] Even if participation does not increase support for a decision, it may clear up misunderstandings about the nature of a controversy and the views of various participants. And it may contribute generally to building trust in the process, with benefits for dealing with similar issues in the future.[55]

51 Stern, Paul C., and Harvey V Fineberg (eds.), *Understanding Risk: Informing Decisions in a Democratic Society*, Committee on Risk Characterization, National Research Council, National Academy Press, Washington, D.C., 1996. See also Oudshoorn, Nellie, and Trevor Pinch, *How Users Matter: The Co-Construction of Users and Technology*, MIT Press, Cambridge, MA, 2003.

52 Sollie, Paul, "Ethics, technology development and uncertainty: an outline for any future ethics of technology", *Journal of Information, Communications & Ethics in Society*, Vol. 5, No. 4, 2007, pp. 293-306 [p. 302]. See also Moor, James H., "Why we need better ethics for emerging technologies", *Ethics and Information Technology*, Vol. 7, No. 3, Sept 2005, pp. 111-119 [p. 118]. Moor also supports better collaboration among ethicists, scientists, social scientists and technologists.

53 Palm, Elin, and Sven Ove Hansson, "The case for ethical technology assessment (eTA)", *Technological Forecasting and Social Change*, Vol. 73, Issue 5, June 2006, pp. 543-558 [p. 547].

54 US National Research Council, Committee on Risk Perception and Communications, *Improving Risk Communication*, National Academy Press, Washington, D.C., 1989, p. 9. http://www.nap.edu/openbook.php?record_id=1189&page=R1

55 Stern and Fineberg, op. cit., pp. 23-24.

The process of identifying, discussing and dealing with privacy (and other ethical) issues should be ongoing throughout the project and perhaps even after it has been implemented, if only because new issues may arise that were not evident at the outset of the project development. Moor has made this point: "Because new technology allows us to perform activities in new ways, situations may arise in which we do not have adequate policies in place to guide us." Ethical problems can be generated at any point, says Moor, "but the number of ethical problems will be greater as the revolution progresses".[56]

The process of engaging stakeholders in consideration of ethical issues that may arise from the development of a new technology or the new use of an existing technology or a new policy or programme is arguably as important as the result. While stakeholders can make a substantial contribution to the decision-making process, at the end of the day, however, it is the policy-maker or technology developer who must take a decision whether to proceed with the technology or to modify it or to build some safeguards into its use in order to accommodate the concerns raised by stakeholders. It is the policy-maker or technology developer alone who will be held accountable for the decision.

Conclusion: PIA as part of risk management

It is in the interests of policy-makers, technology developers and project managers to conduct impact assessments involving stakeholders interested in or affected by the technology, as early in the development cycle as possible in order to minimise risks that may arise once the technology is launched. In some sense, impact assessments (like a privacy impact assessment) can be regarded as a form of risk management.[57]

While some decision-makers may think engaging stakeholders is a hassle or risks delaying development, the benefits of engaging stakeholders are numerous and should outweigh any such thoughts. This engagement also responds to a democratic necessity: if the consequences of new technological developments – which were not yet visible at the moment of the elections – are uncertain, the taking of action and of risks is a question of collective decision-making, and thus becomes a political issue. In addition, stakeholders may have some information or ideas or views or values that the project manager had not previously considered. They may be able to suggest alternative courses of actions to achieve the desired objectives. They may be able to suggest some safeguards which would minimise the risks that might otherwise become apparent after a technology or service is launched. By engaging stakeholders, the technology developer has a better chance of minimising

56 Moor, 2005, op. cit.. In his paper, Moor proposes the following hypothesis, which he calls "Moor's Law: As technological revolutions increase their social impact, ethical problems increase."

57 Verbeek indirectly offers at least two reasons supporting an ethical impact assessment. Two forms of designer responsibility can be distinguished here. First, designers can anticipate the impact, side-effects and mediating roles of the technology they are designing. On the basis of such anticipations, they could adapt the original design, or refrain from the design at all. Second, designers can also take a more radical step and deliberately design technologies in terms of their mediating roles. In that case, they explicitly design behaviour-influencing or 'moralizing' technologies: designers then inscribe desirable mediating effects in technologies." Verbeek, Peter-Paul, "The moral relevance of technological artefacts", Paul Sollie and Marcus Düwell (eds.), *Evaluating new technologies: methodological problems for the ethical assessment of technology developments*, Dordrecht, Springer, 2009, pp. 63–79 [p. 70].

liability. The sooner stakeholders are brought into the process, the better. It will avoid subsequent criticisms and, possibly, costly retrofits downstream.

Many breaches in databases and losses of personal data held by government and industry have received a lot of negative publicity in the media. Undoubtedly, there are more breaches and losses that have not been reported by the media. Even so, those that have been reported take their toll in public trust and confidence. Most people simply do not believe their personal data is safe. There are justified fears that their personal data is used in ways not originally intended, fears of mission creep, of privacy intrusions, of our being in a surveillance society. Such fears and apprehensions slow down the development of e-government and e-commerce, and undermine trust in our public institutions.

As databases are established, grow and are shared, so do the risks to our data. A breach or loss of personal data should be regarded as a distinct risk for any organisation, especially in view of surveys that show most organisations have experienced intrusions and losses. Assuming that most organisations want to minimise their risks, then privacy impact assessments should be seen as a specialised and powerful tool for risk management. Indeed, PIAs should be integrated into the overall approach to risk management, and with other strategic planning instruments.[58]

In a society characterised by the unpredictability of risks that stem from existing as well from future and emerging technologies whose mastery is not totally in our hands, it is important to adopt a sound attitude towards those uncertainties that might have radical consequences. PIAs are a step in this direction. Practical issues such as how best to balance competing values, how best to implement such instruments at all pertinent levels and sectors of the society, or how to integrate stakeholders in the best participatory mode remain. However, this should not impede us from going towards an ethic of decision-making that relies upon its awareness of the radical uncertainty that characterises the world we live in, in order to better act with a view to preserving individual autonomy as well as the other fundamental values that underpin the democratic constitutional State.

58 Office of the Privacy Commissioner of Canada (OPC), Assessing the privacy impacts of programs, plans, and policies, Ottawa, October 2007. www.privcom.gc.ca

CHAPTER 6
Privacy Practices and the Claim for Accountability

Daniel Guagnin, Leon Hempel and Carla Ilten

Introduction

With modern technologies emerging, especially Information and Communication Technologies (ICTs), new problems are gaining relevance, respectively old problems are getting new relevance. The concept of privacy for example is changing over time, which can also be seen as a consequence of changing daily practices in the increasing usage of ICTs. The digital technologies provide a new quality of possible privacy infringements in regard to storage, amount of data, and linking data sets. To make technologies fit for 'good society', ethical concerns like privacy related problems have to be taken into account during the initial state of research and development. Accordingly, Responsible Research and Innovation is an important factor in regards to the implementation of privacy into technologies. It is important to integrate privacy concerns into the development of security technologies as engineers already do with approaches such as Privacy by Design and Privacy Enhancing Technologies. However, besides the technology, law plays an important role as well. Both laws and technologies consist of written rules which structure – more or less – social life. While a characteristic of technology is that the underlying rules are not difficult to enforce, laws are sometimes more onerous to establish.[1] The recent outcomes of the PATS project show the gap between data protection regulations and privacy practices – practices often do not follow the written rules. There is thus a need for measures to guide the transformation of existing rules into practices. Discussion have emerged demanding accountability, which seems to be used as a term to describe the gap between rules and practices. This shows the need for concrete measures to enforce the implementation of data protection rules.

But how can this be done? The implementation of accountability mechanisms has to be part of policy innovations rather than being restricted to the self-regulation of security organisations. From this perspective, it is comparable to the concept of regulative self-regulation: It aims at taking advantage of the dynamics of self-regulation while the state has to fulfil a control function (see section 2.4) to assure the compliance with legal frameworks. Some authors state that it can be seen as a consequence of the information age, that pure regulation by the state is not sufficient any more as legal frameworks are not flexible enough to adapt to fast societal developments; in this context regulative self-regulation is the bridge between the former principle of regulation and the pure self-regulatiove approach which is considered as too arbitrary. (cf. Schulz and Held 2002)

Instruments of accountability can thus complete self-regulative instruments (e.g. codes of conduct) and technological tools (such as PETs and Privacy by Design) with a regulative dimension. The concrete implementation of accountability is still an issue and a great challenge for researchers and policy makers alike and has to be further developed.

The following article will first discuss the issue of accountability. It seems necessary to recall the concept of privacy not as a static phenomenon but as a developing social construction. Privacy is changing over time as we acknowledge today – together with changing practices. Accordingly, privacy can be seen as part of the practice. We will focus

1 Anthony Giddens (1992) describes the role of rules in practice in his theory of structuration. He neglects however the importance of written rules which are more stable than practiced rules (through the written form) and nevertheless have an impact on social practices – e.g. Privacy by Design may manage to avoid abuse of personal data through its function of hardening social norms (cf. Latour 1991), yet laws need to be negotiated, interpreted and executed by social institutions.

on privacy perception and practices within diverse security organisations, based on empirical outcomes of recent research in the PATS[2] project. We witness that in the case of most organisations privacy protection is simply ascribed to the citizens' responsibility. Privacy is still not understood as a precondition for social relations but as an issue of individual decision. After the empirical view on the practice we will shortly review existing privacy measures to reconsider the current debate on the accountability principle. As for the Article 29 Working Party accountability is seen as a key concept for an effective implementation of data protection principles. For both self-regulation and the question of accountability, it is a central issue whether accountability can simply be claimed by an organisation or if accountability actually has to be proven proactively and checked by an external entity. Given the value of selling personal data today, it seems necessary to limit the expectations. Even in the communication of the European Commission regarding the Data Protection Directive (EC 2010) it is repeatedly stressed that the free flow of information within the EU is a necessity. The economic profit however should not restrict the claims for privacy.

The following discussion considers how one can connect the concept of privacy with the actual practice, arguing that the principle of accountability can be seen as a bridge between privacy and practice. Privacy as a whole can be described as a triangle of the concept of privacy, privacy practice and the accountability principle as a measure to influence the practice according to the spirit of the concept.

Privacy Practices

The concept of privacy is not a static phenomenon but a developing social construction. This always has to be kept in mind when thinking of solutions for privacy related problems. Especially if technology is considered as neutral, the effect of technology hardening social practices is disregarded. Social imaginations of how to solve a problem however are implemented in technologies and thus its functions are constructed according to the social views of the designers and engineers. If we consider technology as neutral the inscribed social practice seem given and objective – or even natural.

Privacy as concept is even more, it is a part of the practice – with our daily use of techniques and technologies, which have increasingly included ICTs, our understanding of privacy is also changing. These are the practical rules which constitute the social world, however being related and interconnected with the written rules.[3] With changing concepts of privacy tools, measures and means have to be adjusted – or in other words, with changing practices, the written rules have to be adapted. This is what happens when the recent discussions turns to accountability as we will point out below.

Furthermore the privacy practice affects the daily use of techniques and technologies, and has thus impact on the citizen – which will be the main focus of this section.

2 FP7 Project Privacy Awareness Through Security Organisation Branding; see www.pats-project.eu

3 This is truly only one simple aspect of the theory of structuration of Anthony Giddens (1992), but helpful in this context.

Excursus: data sensitivity

An illustrative example for the change of privacy is the question of what should be considered as sensitive data. As elaborated during an empirical study by Karen Mc Cullagh (2007) in the UK, information regarding which political party or trade union one belonged to was considered as being sensitive data shortly after the Second World War, while today individuals define information regarding their health or wealth as being sensitive. Since 1980, there have been discussions regarding how different grades of sensitivity of personal data should be categorized in the OECD. The debate is based on the assumption that the necessity to protect data varies, depending on the grade of sensitivity. Accordingly, data protection and privacy are related in their understanding of what kind of data has to be protected and to what extent. However, sensitivity is a matter of estimation and thus social negotiation.

There have been different approaches to the categorization of distinct sensitivities of data sets. This leads to the implementation of varying legal regulations depending on the estimated sensitivity of the concerned data. The latest example of changing opinions regarding the definition of sensitive data may be seen in the European Commission's recent communication regarding data protection in the EU (cf. EC 2010: 9). It states that they will have to consider "whether other categories of data have to be considered as 'sensitive data', for example genetic data." (Ibid.)

However, through connecting different sets of data, the sensitivity of data can change. A simple example is the link of non-sensitive data such as name, address – which can be found in every phone book – with the information of somebody's whereabouts. When linked, they may represent useful information for burglars if they know that the person is on vacation and his apartment will be empty (cf. Reuters 2009).

This shows that not only the relevance of the explicit data, but also that the context of the data has to be taken into consideration: Where is the data stored? Who can access it? How can it become linked? This is also related to the question of who the data controller is. Their access to personal data is a further issue why data controllers have to be involved in data protection and have to be held accountable when an infringement occurs, as we will argue in the following. The data controller is able to directly link data or share the data with other data controllers. Consequently, the possibilities of its use and interconnection of data should be included when defining data's sensitivity. However, this becomes increasingly difficult within a digitalized environment.

Security Actors: Organisations

In order to provide an empirical view of the privacy practices of security organisations, we will shortly revisit a number of outcomes of our recent research emerging in the context of the PATS Project[4]. The project focuses on security organisations and how they address privacy issues and practice data protection.

To obtain an overview over the security field, we carried out qualitative interviews with representatives of different types of actors: security service providers, security technology

4 FP7 Project, PATS stands for Privacy Awareness Trough Security Organisation Branding)

producers, system integrators, research institutions, consultancies, public agencies and associations.[5]

The problems we identified may be summarized in three categories: (1) Notions: Data protection is understood in a very limited way, (2) Incentives: Organisations do not seem to have a real interest in privacy, they rather show pragmatic approaches, (3) Performance: There is a performance problem, there are black boxes and lacking mechanisms to ensure an effective data protection.

(1) Notions

Data protection is mainly understood as data security. This is a consequence of a technological approach to the problem and a very limited understanding. Abuse of data is seen as a problem of unsecure data flows which can be solved with data security approaches such as with the encryption of data flows. However, this perspective neglects the democratic dimension of the generation and storage of personal data. On the one hand, even non-sensitive data may become sensitive if it is connected with other data available – the possibility of connecting huge data sets (data mining) has become very easy through modern information technologies. On the other hand, the generation of data gives the owner of the data power – or in other words control over people and time as Giddens (1992) describes it in his theory of structuration[6]. This is strongly related with the problem of function creep: Existing functions of technologies will be used in different ways, and possibly not intended uses will be applied.

(2) Incentives

Organisations do not see any necessity for extensive communication regarding privacy concerns. We found three main types of privacy practices: (a) if there is a high concern of privacy, it is merely communicated. Mostly there is a low interest in enhancing privacy, (b) but this may be changed through public scandals which generate the need for an active remediation. Some of the concerned companies however may attempt to avoid the issue entirely as far as possible. (c) The common attitude however seems to aim on complying formally with the laws in order to avoid any friction with authorities or public scandals (and financial losses) related to these problems.

(3) Performance

In regards to the performance of privacy practices, our findings are obviously related to the two points described.

The narrow notion and low understanding of privacy issues, supports the black boxing of the problem. Privacy is either delegated to technological black boxes, or the data protection

5 To keep it short, we will merely revisit some of the main outcomes related to the question of accountability here.

6 This is the authoritative type of resources. Giddens also mentions that storing data enables the owner of these resources to increase his power; obviously digitalisation and computers provide the possibility of huge storage and fast data processing.

laws work as a black box. "There is data protection law" is a statement aimed at delegating the responsibility to formal instances such as the data protection officer (DPO) of the concerning company. When a company complies with these regulations however, it neither provides a guarantee regarding the quality of the officer's training, nor does it ensure his impartial position towards the company. Beyond the formal law abidance there is the problem of different fields of expertise which are in conflict: Engineering and law are two different realities, and the experts are often not capable to understand each other.

In regards to the pragmatic attitude of stakeholders we can state that there are no incentives for a stronger implementation of data protection. The market logic as only an instrument is not suitable for enhancing privacy in the existing actor relationship. If we try to apply the market logic it is obvious that in the market of security technologies the scrutinized citizens do not have market power: The customers – the ones buying and deploying the security technologies – have market power but no interest in enhancing privacy, because they want to enhance their capabilities for surveillance and control measures rather than strengthening citizen rights. Indeed the argument of a customer's choice is useless here. Even if we consider citizens as customers of the companies buying and deploying security technologies, they merely have a choice. If for example a citizen does not want to be surveilled while taking advantage of public transportation, is it realistic to avoid using the public transportation system? It rather is a limitation of one's mobility.

This leads us to the question of the user's accountability, which will be elaborated in the next section.

Citizens, Users, Consumers

First of all, what is a user in our perspective? Is it the user of security technologies, or the citizen 'benefiting' from them? We suggest seeing the citizen as a consumer or an end-user, because in regards to security technologies he is at the end of the production chain while the companies buying and applying security technologies offer their services to the former one. Accordingly, we suggest naming the latter 'customer'. We therefore have three actors in this market of security technologies: Producers, their customers – buying and applying the products – and the consumer who is at the end of the chain, the citizen consuming services and products of the middle one – passing the monitored spaces.

In regards to the end-users we face two problems. On one hand security organisations attempt to shift their responsibility to these users, on the other hand they actually lack control over their own data.

Consumer's Choice?

As pointed out above, interviewed stakeholders of security organisations repeatedly excused themselves of their responsibility with references to the customer's choice and user's willingness to spread his or her data into the web, but these are two very different subjects. Either the user can choose if he takes advantage of a virtual application, or whether he moves through surveilled spaces. The application may give him control to a certain extent, while the spatial surveillance leaves only the option of avoiding to pass those places. Of course the user also does not exactly know where the data of an online application flows or is stored.

So the question remains: How much of a choice does the user have? He may choose to use the virtual social network his friends are using or decline to use it and consequently lose this access to them. He may use the public transport if he does not want to be filmed by the cameras installed there – but then he has to walk or drive by car (where he will also be observed by traffic observation cameras). It is obvious that users have a strong constraint of few possibilities, some of which are very uncomfortable and limiting.

Moreover, there is another difference: In the case of using an (online) application, the user can actively decide which data he is willing to share. If he however is tracked in a public space, he neither has the possibility to chose whether he is logged in or not, nor which data of him is stored (e.g. at which corner he passes at which time).

The difference between these two situations affecting the end user is neglected by interviewees of security organisations. It shifts the accountability of privacy infringements to the end-user with the "the horse has already bolted"-argument: Why should we (the security organisation) care about privacy if the end-user himself gives his data away voluntarily: It is the user's own fault if privacy does not play a role.

> "Accountability is not present simply because consumers have an option of choosing another company in a competitive marketplace." (Bennett 2010)

(End-)User Empowerment

Even if the shift of accountability from stakeholders to the end-users is unjustified, users have to take responsibility to a certain extent, and it is important for them to gain control over their own data as much as possible and to know where their personal data is stored. This may be challenging however as data controllers use complex structures of generating, processing and storing data.

A further issue is the lack of information regarding the trustworthiness of data controllers which is difficult for end users to realistically evaluate. Furthermore, the end-user's control over his stored personal data, such as its correction or removal, is low or non-existent.The empowerment of the users however should not overstrain them too much, but instead should be simplified. It cannot be expected that every end user becomes an expert of data control and data protection. These problems are also addressed in the communication of the European Commission (EC 2010: 6ff). The Commission supports the effective control of data subjects over their data including having better access to and influence over stored data, increased transparency and easy access to easy understandable information (Ibid.). Practical approaches to enforce a "principle of transparency" could be standardized privacy notices to simplify the understanding of such and limit the complexity or a mandatory breach notification to inform users about abuse of their data. (Ibid.: 6)

Intermezzo

Concluding this section we can state that the awareness of privacy related problems in security organisations is very low. Besides that, the market structures do not give them enough incentives to enhance their privacy efforts at their own responsibility. Consequently, there is insufficient implementation of data protection measures into the daily practices and security organisations are instead shifting the responsibility to the end-users. But

should the citizens be responsible for their privacy alone? Should we burden them with this weight? Or should the responsibility also be distributed to other actors such as the data controllers and security organisations? How can this be put into practice, and is the accountability principle the next step?

To consider answers for these questions we now discuss approaches towards accountability of different perspectives: The (end-)users, organisations and the regulative laws and technologies.

Towards Accountability

How can accountability be implemented? We will present two actual approaches which involve citizens into accountability structures. We will take into account recent discussions regarding accountability, which focus on organisations. Before we close with a summary we will revisit the written rules of law and technology.

Accountability 'from the bottom'

An issue regarding the user's responsibility is the question of how users can become involved in the debate regarding data protection concerns. This requires users to gain insight into privacy practices of security organisations and the possibility of drawing attention to legal infringements. We present two examples, one concrete case of a CCTV lay visitor panel, and a more general example of controlling software functions.

Transparency of CCTV Monitoring

In Wycombe's District Council there is a panel named the "Independent CCTV Lay Visitor Panel". This is a panel of representatives, respectively citizens, controlling the CCTV practice of the Wycombe district.[7] The members are trained in CCTV regulation and Codes of Conducts and are entitled to enter the CCTV monitor rooms unannounced. They can report their findings to the local media and can get in touch with the CCTV manager or a police officer when they observe irregularities. Beyond that, they provide an Annual Report about the CCTV practices, and present it in an annual meeting to the public. (CCTV LVP 2006)

This seems at first glance like a measure to include citizens in the control of privacy rights and may be seen therefore as a model of accountability from the bottom. The Terms of Reference of the panel state: "[the aim is] to safeguard the rights and interests of all the citizens residing in or visiting the areas covered by the CCTV operation". (Ibid.)

Taking a closer look at the panel and referring to its annual report, it seems to be an institution supporting the use and efficacy of CCTV. This is mentioned under the aims of the Terms of Reference as well: " to inform the public of its [CCTV, the author] operation and efficacy."

We do not want to get too deep into the actual practice of the panel and would propose to further analyze its impact and practical functions. However, in any case this is a very

7 http://www.wycombe.gov.uk/council-services/community-and-living/community-safety/cctv.aspx we are referring to the documents provided there, see also the literature section: CCTV LVP

unique institution which is an example of the implementation of a measure enhancing the accountability of both the monitoring employees and the lay visitor, where representatives of the 'watched' citizen are entitled to watch their observers.

Transparency of Software

The practice of free software, also known as open source software, may be seen as a further example of accountability from the bottom.[8] Although only experts know how to read software source code, the open structure allowing anyone to view and modify the code empowers users to take control over the functions of the software program. Especially if we think of "personal computer" as being a main storage system for personal information, we should be concerned of which software is running on it. To clarify: The critical issue with the opacity software functions is that it is impossible to find out what a computer program is actually doing on your computer in the background of the user interface – there may be a lot of functions working on your computer you never will notice. Allowing the code to be scrutinized by other individuals by opening the source code makes the functions of the software transparent and helps undermine and avoid for example unwanted spy functions. One can hence avoid unintended surveillance operated by software through opening its source code. An example for the problem non transparency of a software and its activities may be seen in the discussion regarding a Skype function, which reads unique IDs of personal computers on which it runs. A hacker describes how she randomly ran into a software error and how she managed to track the function via the very complicated method of reverse engineering.[9] Whatever this function was intended to do, the issue shows that it is hardly possible to know what software does on your computer, if you have no access the human readable source code[10].

More specifically, software needs to be transparent in order to allow scrutiny of its functions. Even if normal users cannot read "human readable" software code, there are experts who are able to do it – and are doing it. This is comparable to laws being accessible, but not written in a language understandable for the common citizen. It is however a democratic necessity to open its access. When hackers review code and software for surveillance functions it is a form of enhancing privacy in the realm of software. However, it is not yet a common practice to use free software.

The question arises to what extent it is necessary and possible to enable citizens to be fully aware of all privacy issues. Even if there is potential to empower users and citizens to take control, there is a need to create structures and means in order to enhance the accountability of security institutions and organisations.

8 While Open Source Software stresses the transparent source codes – what is the crucial point in our argumentation – free software is often misunderstood as „free as in beer". However we prefer using the term free software as it is orginally meant as „free as in free speech". More about the definition of the term can be found here: http://www.fsf.org/about/what-is-free-software

9 See http://www.pagetable.com/?p=27 – indeed this example shows, that it is not completely impossible to find out what software does without having its source code. However, this procedure of reverse engineering is a really difficult method, what may be practicable to trace a certain dysfunction, but it is not a useful way to make a complete review of the program.

10 The structure of computers makes it necessary to compile human readable software code into machine readable code consisting of ones and zeroes.

Organisations and the Principle of Accountability

We identified two approaches of involving citizen into structures of accountability. But what are the organisations' responsibilities? Structures are missing to force organisations to comply with privacy practices according to the existing legal data protection frameworks. This is currently discussed under the term accountability. The Article 29 Working Party of the European Commission states in its "opinion 3/2010 on the principle of accountability":

> *"In a nutshell, a statutory accountability principle would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request." (Art 29 WP 2010, §3)*

Besides that, is a current project which is under the coordination of the Centre for Information Policy Leadership (CIPL 2009 and 2010), which recently published its first two reports, namely the Galway and Paris project reports. Colin Bennett (2010) formulated some conceptual thoughts regarding accountability which we will take as a structure when discussing the other approaches.

We will also refer to the recent communication of the EC (2010) formulating intentions for the future amendment of the EU Directive for Data Protection (Directive 95/46/EC).

In the Galway Project report, the authors state that the principle of accountability was already established in the OECD Guidelines from 1980. Additionally, they see it implicit in numerous provisions of the European Union (CIPL 2010:3). Explicitly it is part of the International Privacy Standard of Madrid (Madrid 2009), the Canadian PIPEDA[11], Fair Information Principle of the FTC[12] (US) and the APEC guidelines. (Ibid.)

Bennett (2010) stresses three dimensions of accountability and distinguishes it from *responsibility and responsiveness*. According to his argumentation, accountability implies *who* is accountable *for what* and *to whom*. These three aspects refer directly to the lacking implementation of privacy regulations. It is necessary to have somebody to address for defined issues of data protection which needs to be liable for his area of responsibility. In this understanding, the term is stronger than responsibility which implies not evidently the "for what" and responsiveness which is lacking of the emphasis of the "to whom". The latter is linked to the need of external agents of accountability as this is necessary for an independent measurement of the efficacy of accountability mechanisms.

While in the OECD and APEC guidelines the term accountability is formulated very vague and the "to whom" aspect is missing, (ibid.) it is more explicit in the Article 29 Working Party's Future of Privacy Document and the Opinion 3/2010 on the principle of accountability (WP29 2009, 2010) as well as in the reports from the Galway and Paris project (CIPL 2009, 2010). In "the Future of Privacy" it is made clear that the principle of accountability "[...] would require data controllers to have the necessary internal mechanisms in place to demonstrate compliance to external stakeholders, including national DPAs. [Data Protection Authority, editor's remark]" (WP29 2009) Also, the international privacy standard of Madrid (2009) makes it clear that someone has to be held liable in the case of data protection right infringements against data subjects, following DPAs.

11 Personal Information Protection and Electronic Documents Act

12 Federal Trade Commission

The proclamation of the Galway project report is more specific in the question of who should be held accountable and claims a *shift to organisation's* ability to demonstrate its capacity to achieve specified objectives. This stands in line with the focus of the PATS project to strengthen privacy in a broader perspective,taking into account the security organisations, including companies offering security products and services. It is a justified claim that organisations that collect and control personal data (data controllers) may be held accountable for the non-compliance of law. Furthermore, the Galway project stresses the aim of adaptability: Self-regulation measures should be adaptable to business models in order to provide easy integration and to assure that the implementation process and costs do not generate even more obstacles for companies, especially small and medium enterprises. The Article 29 Working Party aims as well at considering the business models and at providing a flexible framework. (CIPL 2009)

In the Galway project report regarding "the essential elements" of data protection accountability, the authors list five central points, admitting that some of them are already part of existing laws. (Ibid.:4)

> "Organisations commitment to accountability and adoption of internal policies consistent with external criteria
> Mechanisms to put policies into effect, including tools, training and education
> System for internal, ongoing oversight and assurance reviews and external qualification
> Transparency and mechanisms for individual participation
> Means for remediation and external enforcement"

According to the report, the advantages of an accountability based approach are the possibility to bridge approaches across disparate regulatory systems, to heighten confidence, to raise quality and to allow greater flexibility. (CIPL 2009:8) Its wording may be compared with an attractive commercial advertisement. The document however is vague and abstract regarding how this may be achieved. Nevertheless, one must keep in mind that it is just the beginning of the project. In Phase II, the Paris Project, it becomes clear that the striking central issues revolve around three points: remediation and validation mechanisms and the question how to recognise external agents of accountability. It is merely however, a description of the problem rather than a solution. (CIPL 2010: 8ff)

This reflects the very points that Bennett stresses: He claims that external agents of accountability – without that evaluation of processes and liability (remediation) - are merely conceivable.

Additionally, the Galway project stresses the flexibility of the approach and that organisations have to commit and demonstrate the adoption of laws. It is not elaborated how this will be done – however the project is still in progress, and we are looking forward to further outcomes.

Furthermore, there are suggested Binding Corporate Rules (BCRs) which at first seem similar to Codes of Conduct, yet they are described as a binding self-regulated legal basis for various companies within whole branches. This gives the measure an important attribute: If Codes of Conduct become binding rules for various companies they become real instruments for measuring privacy practices and compliance with

regulations. This is an invaluable argument for Codes of Conducts being more of a buzzword without real impact on practice.

Very relevant seems to be the shift of primary responsibility to organisations rather than holding individuals accountable as indicated above. According to the presented outcomes of organisations trying to shift accountability to the users this is indeed a crucial point, which enriches the concept and enhances the practice of privacy. Beyond that, the authors state that it is important to give individuals control over their data. It is obvious that this is another important point (if we think of the discussion of who has property rights on medical data of patients (cf. EC 2010)). In our perspective, to hold organisations accountable and to empower individuals to retain control over their data are the main issues to strengthen data protection. This also includes information about the data controlling organisation which is a need for user's sovereignty. If one for example has to decide to agree to privacy statements one usually does not know anything about the trustworthiness of that organisation. (Ibid.: 13) This could for example be supported by the establishment of privacy seals which are a symbol of trust, given to evaluated companies. Moreover, users often have to choose getting the service with all privacy infringements or denying the whole 'package'. This is a questionable form of "consumer's choice". Another problem that is also addressed by the new EU directive is the complexity of such choices which is also a cause of non-transparency of processes and structures (Ibid.:6). Furthermore, it is claimed that accountability means to require organisations to demonstrate compliance upon by request rather than waiting for failureThe main problems are that it is hard to measure accountability: Especially the three issues raised in the Paris project report: How will remediation work? How to determine the appropriate validation mechanism? On what basis are third-party accountability agents recognized? (CIPL 2010). The latter is a question of the credibility of enforcement bodies and third party accountability programmes which is invaluable to establish an external form of control.

So what is this principle of accountability? It is a term describing the lack of implementation of data protection rules. The several approaches towards accountability claim to provide solutions for this problem, but they stay very vague in the main issues, so it will be necessary to fill this gap. Hereby we can state two main issues for a successful concept of accountability: Failure of accountability must readily result in liability (Bennett 2010) and external agents of accountability are a sine qua non. (cf. ibid.)

Regulative instruments

Different instruments and approaches on enhancing privacy and accountability are already implemented or in progress. We will first reconsider different instruments of some legal instruments followed by self-regulation and strife technological solutions.

Towards a new legal framework

We already implicitly discussed some issues of the recent communication about data protection from the European Commission (2010). Now we want to add some further points out of the document to shape the development towards accountability, before we link to the self-regulation approach aiming beyond the law.

This "comprehensive approach on personal data protection in the European Union", as the subtitle of the referenced document is named (EC 2010), reflects considerations about the new EU directive. The authors refer to the challenges of changing IT infrastructure and globalisation and formulate the central intention as supporting the free circulation of personal data by the legal framework within the European Union (ibid.: 6). As indicated in the introduction, this shows that the cross-border flow of personal data is seen as an important interest of economical value which leads the considerations besides the important principles of data protection as the "data minimisation" and the "right to be forgotten". (Ibid.: 7f)

Under the point of enhancing the internal market dimension of data protection they demand the strengthening of self-regulations and propose European certification schemes as a privacy seal. (Ibid.: 12) They also seek to reduce administrative burden for the companies involved the processing of personal data – another drift towards self-regulation.

However, they also aim on "Enhancing data controllers' responsibility". In this context they state: "Administrative simplification should not lead to an overall reduction of the data controllers' responsibility in ensuring effective data protection." (Ibid. 11f) This is a crucial point in our perspective as pointed out above and also part of the accountability approaches discussed. They want to ensure that "data controllers put in place effective policies and mechanisms to ensure compliance with data protection rules" (ibid.) and refer to the debate surrounding the 'accountability' principle. They also understand the accountability approach as aiming at measures for establishing mechanisms that make data protection compliance more effective. (ibid.)

Furthermore, they make explicit that remedies and sanctions are targeted to provide liability of data controllers. This also implies the extension of the power of data protection authorities and civil associations representing data subjects' interest. (Ibid. 9)

Self regulation and Regulative Self-regulation

The self-regulative approach has various advantages opposing to legal frameworks, resulting in developments towards self-regulation. Obviously the fact that self-regulation is a measure that is of course a more intrinsic motivated form of organisations' regulation which automatically brings it forward. Beyond that, Schulz and Held (2002) argue that especially in regards to fast changing circumstances within certain branches – what is also seen as a general trend of the 'information economy' – self-regulation is more flexible than legal frameworks. They also refer to the white paper on European Governance which stresses the need of new forms of regulation – named co-regulation. Besides other captions this stands for a form of regulation which is controlled to a certain extend by the state. Schulz and Held prefer the term *regulative self-regulation* which describes exactly that: Self-regulation with a regulative control of the state:

> *"[...] we define regulative self-regulation as self-regulation, which is adopted into a governmental legal frame, respectively is based on a legal base." (Schulze & Held 2002)*

They see several arguments for this approach enriching the field of regulations with a concept taking advantages of both legal frameworks and self-regulation. (Ibid.) Mainly regulative self-regulation solves some problems of traditional legal regulation which often lacks information needed to adequately regulate and seems to override the competences

of organisations which are thus not very cooperative in implementing laws. So the concept includes the willingness and creativity of the companies and organisations without getting too non-binding through the regulative aspect which implies a certain control over the self-regulated activities and measures. (Ibid. 13f)

Accordingly, the accountability approach needs to integrate both, the self-regulation aspects of taking into account the activities of the involved organisations and support the compliance and liability through control mechanisms with external agents of accountability. This could be done through evaluating accountability structures, blueprints for those structures to ease its development, privacy certificates and seals and a stronger position of data protection authorities with the power to enforce the implementation of certain rules and demand remedies.

Technology as Regulative Means

Besides legal frameworks and self-regulation structures, does technology also play a role in enforcing privacy? According to the thoughts elaborated above, technology can strengthen social norms as well. If privacy intentions are inscribed in technology, there can be a strong programme of acting according to that (in terms of Latour (1996)). In other words, if a data controlling software e.g. does not allow certain queries, they are difficult to be done, or if there is a certain field in the database non-existent , no one will be able to put information to that field. That sounds trivial, but it is not. Especially if technology is considered to be neutral we should always keep in mind, that decisions about database fields and functions are socially negotiated. Beyond that, the security technology solutions may provide for security problems based on the special perspective on the problem. For example, categorising people is a social act and is inscribed in selecting functions of technologies. Once implemented, the technology follows the rules underlying its construction – if we consider this as neutral, we might believe that things just are as they are.

Privacy Enhancing Technologies can of course strongly support privacy practices, and privacy has to be considered in the initial step of designing technology – which supports the Privacy by Design approach.

To give some examples, PETs can help with the anonymisation and pseudonymisation of data. An electronic safe can provide the technology to store sensitive data online and share specific information with an authorised person via an encrypted connection (Breitenstrom et al. 2008).

So, in all technology can only serve as an assistance and should not be regarded as a neutral, exhaustive tool to enforce privacy.

Conclusion

So – as pointed out – privacy is a changing concept and in practice data protection is often rarely applied. In the European Union, we have far developed legal frameworks and technological measures. PETs and Privacy by Design assist in implementing privacy. However, we need a bridge between the concept of privacy and the practice of data protection. This has been recently discussed under the demand for a principle of accountability. This

'Accountability' needs further development. It is time to fill in the blanks and construct concrete implementation proposals.

Colin Bennett (2010) names some main issues of a concept of Accountability: it is a need to take into consideration the question of how to involve external agents of accountability in controlling the compliance of data protection measures. It should be made sure, that accountability does not become just another framework to enforce the existing framework but instead encourage organizations to introduce and enforce accountability mechanisms which are applied in practice.

We now discussed different approaches towards accountability in the perspectives of technology, law and the user. It seems a simple but useful idea to connect the measures and to apply them simultaneously. The principle of accountability can become a frame to ensure the effective implementation of data protection principles.

Literature

Bennett, Colin J. (2010). "International Privacy Standards: can Accountability be Adequate?." *Privacy Laws and Business International*, Vol. 106: 21-23. URL: http://colinbennett.ca/Recent%20publications/PrivacyLawsand%20BusinessAugust2010.pdf

Breitenstrom, Christian, Marco Brunzel und Jens Klessmann (2008), White Paper „Elektronische Safes für Daten und Dokumente", Fraunhofer Institut für Offene Kommunikationssysteme (FOKUS).

CCTV LVP (2010a): Lay Visitor Panel: Minutes from the Annual panel meeting 2010. URL: http://www.wycombe.gov.uk/Core/DownloadDoc.aspx?documentID=3679

CCTV LVP (2010b): Lay Visitor Panel: Annual Report 2009. URL: http://www.wycombe.gov.uk/Core/DownloadDoc.aspx?documentID=3677

CCTV LVP (2006): Lay Visitor Panel: Terms of Reference. URL:http://www.wycombe.gov.uk/Core/DownloadDoc.aspx?documentID=1080

CIPL (2009): "Data Protection Accountability: The Essential Elements. A Document for Discussion" – Galway Project report, URL: http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

CIPL (2010): "Demonstrating and Measuring Accountability. A Discussion Document. Accountability Phase II" The Paris Project report. URL: http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

EC (2010): European Commission: "Communication from the Commission to the European Parliament, the Council, the Economic and Social committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union." Com(2010) 609

Giddens, Anthony (1992): Die Konstitution der Gesellschaft. Grundzüge einer Theorie der Strukturierung. Frankfurt am Main: Campus Verlag.

Latour, Bruno (1991).: "Technology is Society Made Durable". In: A Sociology of Monsters: Essays on Power, Technology and Domination. Hrsg. von J. Law. London: Routledge.

Latour, Bruno (1996): "Der Berliner Schlüssel". Akademie-Verlag.

McCullagh, Karen: Data Sensitivity: Proposals for Resolving the Conundrum, in: Journal of International Commercial Law and Technology Vol. 2, Issue 4 (2007), S. 190-201.

PIPEDIA: Office of the Privacy Commissioner of Canada: "Self-Assessment Tool – Personal Information Protection and Electronic Documents Act", URL: http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.pdf

Reuters 2009: "Burglars using Facebook, Twitter to find targets-report", URL: http://www.reuters.com/article/2009/08/28/crime-internet-idUSSP49844920090828 (News article, visited 30.3.2011)

Schulz, Wolfgang and Held, Thorsten (2002): "Regulierte Selbstregulierung als Form modernen Regierens".

WP29 (2009) Article 29 Working Party WP186: "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", URL: http://ec.europa.eu/images/language/lang_en3.gif

WP29 (2001) Article 29 Working Party opinion 3/2010: "On the principle of accountability", URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

CHAPTER 7
Code of Conduct for FP7 Researchers on medical and biometric data privacy

Zaharya Menevidis,
Samantha Swartzman,
Efstratios Stylianidis

Introduction

In numerous FP7 projects, medical or/and biometric data are used for research purposes. While flexibility and availability of systems and data in research are extremely important, another crucial aspect is maintaining and ensuring awareness of privacy issues among researchers and other project participants. Researchers may not have control over the disclosure of confidential data that has been collected, used, stored and disposed of during the implementation of the project and in the phase afterwards [1, 2, 3, 4].

Ethical implications of data collection, use and retention affect society both socially and financially [20, 43]. These impacts have been identified and categorised by the ETHICAL Consortium, which also studied the state of the art approaches and skills [21, 22, 24] and analyzed moderated dialogue and consultation results [25], leading to the development of ethical recommendations for EC policy directives [23].

Although EC DG of Research has put forth several measures, regulations and mechanisms for the preservation of ethical requirements and accompanying commitments [6, 8, 9, 10, 14], studies and debates over and over attest that additional articulation and implementation of a code of conduct for FP7 researchers are necessary, in order to provide guidance on data privacy in practical terms in order to minimize misconduct and misuse [1, 7, 8, 10, 16, 18, 37, 38, 47, 52, 53, 56].

Taking into account the findings from initial ETHICAL studies [20, 21, 22, 24, 25] and its international benchmarking studies [26], the ETHICAL Consortium made an attempt to meet this need by providing recommendations for a code of conduct and implementation measures for FP7 researchers with this report on data collection, use and retention in medical and biometric applications [27, 31]. This particular work focuses on providing a practical tool for usage during proposal submission and contract conclusion as well as during the implementation of FP7 projects, which will act as a toolkit for the relevant activities to be implemented, measured and evaluated.

Background

In order to call FP7 proposers' attention to ethical issues, guidance must be put forth. For instance, "Ethical Guidelines for undertaking ICT research in FP7" [15] points out that any proposal which contravenes fundamental ethical principles, including those stated in "The Charter of Fundamental Rights of EU"[13] and the opinions of the European Group on Ethics in Science and New Technologies[14] shall not be selected and may be excluded from the evaluation, selection and award procedures at any time[15] [16] .

13 http://www.europarl.europa.eu/charter/default_en.htm

14 http://ec.europa.eu/european_group_ethics/index_en.htm

15 Decision 1982/2006/EC: Official Journal L412 of 18/12/06

16 article 15 of the FP7 draft rules of participation (Official Journal L391 of 30/12/06

This form, which must be included as an Annex of the proposal, is concerned with:

- Research on Human Embryo/Foetus (Embryo, Foetal Tissues/Cells)
- Research on Humans (children, patients, persons unable to give consent, volunteers, genetic material/biological samples/data collection)
- Privacy (genetic information or personal data, e.g. health, ethnicity, political opinion, religious or philosophical conviction)
- Research on Animals (laboratory animals, farm animals, non-human primates)
- Research Involving Developing Countries (use of local resources (genetic, animal, plant), benefit to local communities)
- Dual Use (Research having direct military use, Research having the potential for terrorist abuse)

The purpose of this guidance, which includes links to several related websites with guidance on ethics, is to assist proposers in identifying potential ethical issues arising from the proposed ICT research [15].

On the other hand, it must be noted that this extensive source of information and guidance is quite time-consuming and work-intensive during the proposal phase. During the implementation of the project, it is likely that new, sensitive applications might come to the fore, and the project needs to have means for timely indications that some ethical violations are about to occur. It will be necessary to dedicate a specific work package of the project to explicitly addressing ethical issues that might be raised by the project.

Codes of Conduct

Codes of conduct are specific rules or sets of guidelines providing individuals (usually professionals) with practical guidance while dealing with themes that have an impact on one or more ethical values or ethical codes of the society [25, 12, 13, 14, 33, 34, 35, 36, 38, 40, 41, 42].

In general, codes of ethics for professionals serve a number of purposes. They:

- provide ethical guidance for professionals working on FP7 projects and using medical and/or biometric data;
- formulate a set of principles against which professionals' conduct may be measured;
- define clearly the boundaries between what must be done and what must not be done by encapsulating the societal perception of ethics into a written code for reference; and
- provide a framework for how individuals can expect to be treated while interacting with professionals.

Goals and Objectives

This work articulates recommendations for a code of conduct and implementation measures for FP7 researchers on medical and biometric data privacy. This report focuses on providing a practical tool for usage during the proposal submission, contract conclusion, and project implementation stages of FP7 projects. These recommendations and implementation measures will act as a toolkit for relevant activities to be implemented, measured, and evaluated.

In the proposal preparation phase, there are already several forms to fill out which include declarations and explanations [Annex I & Annex 5]. However, the project implementation phase is based on the principles of autonomy and good faith, as researchers are expected to respect rules and regulations that are considered to be applicable. An ethical review [6, 16] might uncover instances of misconduct and could be used as a means for remediation [18, 38, 39, 40, 47]. We recommend as a precaution that specific measures should be communicated and documented within the consortium (e.g. in an interim deliverable on quality and risk management). This would ensure that researchers and other project participants are aware of the roles and privacy issues arising from insufficient or non-existent control over the disclosure of data that have been collected, used, stored and disposed of, and confidential data that will be accumulated during the implementation of the project and in any subsequent stages.

The objectives of the work can be summarized as follows:

1. To recommend principles, measures and guidelines that should be taken or followed during the preparation of a project proposal and during the project implementation phase;

2. To recommend ways in which measures and guidelines can be
   - designed and set up,
   - formulated and documented,
   - implemented,
   - used for monitoring and auditing,
   - useful for adjustment and correction.

It is suggested that the principles, measures and guidelines be structured into these groups.

- Formulation of general and common ethical issues,
- Formulation of project specific guidelines, procedures, handling, monitoring,
- Formulation of data specific issues.

Methodology

Overview

Professional codes of ethics exist in many relevant areas [34, 42, 11], including research in general [57, 14, 35, 39, 40, 41, 42], informatics and biometry [49, 50, 51, 54, 55], medical science [43, 44, 45, 46], nanosciences [12, 13, 19] and security [17, 59, 58]. The methodology used was a benchmarking of existing codes in the areas of research and informatics, defining similarities and differences [26, 31].

The International Medical Informatics Association (IMIA) [44] has issued a Code of Ethics for Health Informatics Professionals. This code is based on the identification of fundamental ethical principles, general principles of informatics ethics, and the duties of health informatics professionals towards health care professionals, institutions, employers, society, and the profession itself.

The Declaration of Helsinki [48] states that the research protocol must be submitted for consideration, comment, guidance and approval to a research ethics committee before the study begins. This committee must be independent from the researcher, the sponsor and any other undue influence. It must take into consideration the laws and regulations of the country or countries in which the research project is to be performed as well as applicable international norms and standards.

The Declaration of UNESCO [50] addresses ethical issues related to medicine, life sciences and associated technologies as applied to human beings, taking into account their social, legal and environmental dimensions. It is intended for application by states. As is appropriate and relevant, it also provides guidance for the decisions and practices of individuals, groups, communities, institutions and corporations, both public and private.

The major legislative Directive that affects and monitors the processing of personal data is the European Directive 95/46/EC [11] on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive contains a number of key principles. Anyone processing personal data must comply with the eight enforceable principles of good practice. Due to Code of Ethics for Researchers of the Academy of Sciences of the Czech Republic [41] data must be (Duty of care):

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- processed in accordance with the data subject's rights
- secure
- not transferred to countries without adequate protection

The Directive does not have deficiencies, but an additional code of conduct is necessary to translate the principles of good practice into practical guidelines.

Developing a code of conduct for FP7 researchers on medical and biometric data serves a three-fold purpose: to emphasize in practical terms the importance of data privacy for European citizens; to maintain the position that technological advances are not restraining fundamental human rights but, on the contrary, may enrich and protect them; to define an ethical framework that tackles issues beyond the existing legislation. The code of conduct is complementary to existing regulations and is voluntary.

Formation of the code of conduct

Approach and principles

In order to prevent careless or unintentional violations of these principles, the following recommendations for the conduct of the project itself (purpose, excellence) and for the handling of information are put forth. Existing codes of conduct, recommendations, and rules were reviewed. As a result of ETHICAL's literature review work, five basic principles were initially identified (privacy, confidentiality, security, property and ownership, reliability

and trustworthiness) that can be easily flouted or avoided during the project implementation phase [20, 32]. Subsequently, public dialogue with experts was facilitated.

Applying ETHICAL recommendations to FP7 research

Over the course of the ETHICAL project, several sets of ethical recommendations were made. This section describes how these recommendations were adapted for inclusion in the code of conduct. Recommendations were put forth in the following ETHICAL deliverables, and were adapted for use in the code of conduct.

- D3.2.2: Guide on government-industry collaborations [28]
- D3.3.2: Ethical requirements for international data sharing [29]
- D4.2: Ethical recommendations for EC policy directives [23]
- D2.2: Dialogue consensus results [30]

Firstly, any recommendations from the above that are not applicable to research were eliminated (i.e., "It is unethical to keep biometric identifiers after a person has been found not guilty of a criminal offense"). Then the recommendations were summarized and made relevant to FP7 researchers.

Developing an outline of the code of conduct

In 2008, the European Commission put forth a code of conduct for responsible nanosciences and nanotechnologies research [12, 13, 19]. This code of conduct contains a description of its scope and aims, relevant definitions, a set of principles with their associated recommendations, and finally a set of guidelines on actions to be taken. To construct the present code of conduct, these same headings were used to organize ETHICAL's recommendations. Finally, in order to reflect the subdivisions of work undertaken over the course of the ETHICAL project, the recommendations were divided into recommendations for all FP7 research, recommendations for FP7 research involving government-industry collaborations, and recommendations for FP7 research involving international data sharing.

Code of Conduct and Ensuring Measures

Set of guidelines

Scope and aim

The following recommendations are intended for all researchers undertaking research sponsored by the European Commission's Seventh Framework Programme[17]. It is intended to provide an ethical framework for the collection, use, and retention of medical and biometric data by such researchers, in general and in research projects involving collaboration between government and industry or international data sharing.

17 http://cordis.europa.eu/fp7/home_en.html

The code is intended to uphold human rights to privacy, dignity, and confidentiality, among others, while providing guidance so that medical research and the development of biometric technologies can take place ethically.

Definitions

Medical data: Medical data refers in this context to all facts or information about an individual's health status, mental health status, genetic history, medications, and medical history.

Biometric data: Biometric data in this context refers to all information gathered by biometric sensors, such as iris pattern, fingerprints, or vein patterns.

Government-industry collaboration: Any research project that involves the exchange of data between a government group or organization and a private sector industry individual or group.

International data sharing: Any instance in which data are available to individuals or groups in more than one country.

Project specific guidelines

Purpose

Research involving the collection, use and storage of medical and biometric data should be meaningful and purposeful. It has to contribute to the Strategic Research Priorities described in the FP7 programme.

Measures to take during project proposal preparation phase:

- Communicate and ensure that EC issues (Annex I Ethical Issues in FP7, Annex II Ethical Guidelines for undertaking ICT research in FP7 [15]) are explicitly understood and accepted by all consortium members.
- Declare that a work package specifically concerned with ethical issues has to be created. An interim deliverable would supplement the initial documents such as the consortium agreement and management guide that:
  - highlights the initial declarations as project accompanying measures,
  - identifies, defines, and addresses other project-specific ethical issues in a way that is feasible for the duration of the entire project cycle, and
  - is supplemented by the advice of an external expert.

Measures to take during the project implementation phase:

- Preparation of a specific Project Ethics Guide with links and references to chapters and regulations of relevance to this endeavour.
- Commitment to an internal audit and, where appropriate, an external audit plan. Carry out an internal audit of the implementation every six months, and when indicated consult an external expert.
- Determination of several risk avoidance approaches.

- Specification of regulations and measures for preservation of the public access to contents of web sites and maintenance of the web sites, especially if personal data are being published.
- Installation of a password-protected common information platform where confidential data can be only accessed by registered project members.

This particular work focuses on providing a practical tool for usage during the proposal submission and contract conclusion stages in FP7 projects. It will act as a toolkit for the relevant activities to be implemented, measured and evaluated.

Rights and responsibilities (roles), legal responsibility

All businesses have a legal responsibility for the products and services they develop, implement and offer. In a consortium where researchers and other technical personnel are working together, roles and responsibilities have to be clearly defined and access to sensible information has to adhere to multilayered security architectures.

Excellence

The research conducted should aim for excellence and the data used for research purposes should be accurate and integral [45].

Innovation

Research involving the collection, use and storage of medical and biometric data should foster innovation so as to justify risks to privacy arising from such activities.

Sustainability

Data collection, use, and storage should contribute to ethical and sustainable development, in line with the sustainability objectives of the European societies as set out in the EC Sustainability Strategy [18].

Handling information

Recommendations

Below are principles for ethical medical and biometric data collection, use, and retention and recommendations on how to observe them in FP7 research.

Enforcement

These recommendations should be upheld by independent ethical committees at the researcher's organisation. Deterrents should be in place to ensure compliance to these

18 Brussels, 26.1.2011, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS- A resource-efficient Europe – Flagship initiative under the Europe 2020 Strategy http://ec.europa.eu/resource-efficient-europe/pdf/resource_efficient_europe_en.pdf

recommendations, which should apply to data at any stage of data collection, use, distribution, retention, or archival.

Privacy

Data should be de-identified as effectively as possible whenever possible.

Consent

Ethical collection of identifiable medical or biometric data should be carried out with informed consent, including consent to the length of the data retention period. If the data are de-identified, independent ethical approval has been obtained, and the data use is in line with the data subject's original consent, then data may be used without further consent. Data subjects should be able to give broad consent so that their data can be re-used; otherwise, consent must be sought for each instance of data collection, use, or retention, or if the purpose has been modified. If consent is not obtained, the data must be removed from any databases.

Purpose

Researchers must only collect, use, or retain data for an explicit, legitimate, clearly defined, documented, and specified purpose. Data may only be reused for a different purpose if consent is obtained. Data subjects should be able to request information about how their data has been used. Only the relevant amount of data needed to fulfil the purpose should be kept. After the purpose has been served, identifiers must be erased. Public health data should be retained for epidemiological purposes.

Data minimization

Only the necessary amount of information should be collected.

Data subjects' rights

The underpinning principle of all medical research should be that the rights of the individual take priority over the needs of the researcher. Data subjects should be informed about how their data are used, and they should be able to access, withdraw, request changes to, and have control over their data. Data subjects should not be disadvantaged if they refuse to let researchers collect their data, but they should be informed of possible consequences of this refusal.

Responsibilities

Researchers must ensure that data subjects understand the implications of taking part; data collectors must be maximally transparent. Researchers collecting data and the organizations in which they are based are ethically accountable for the data and to the data subjects. This means that they must ensure the data are accurate and reliable. In the event of a data breach, researchers must be able to inform the data subjects involved and to conduct a review to identify the cause of the breach. Researchers who transfer data must be aware of the level of data protection afforded by the recipients. A document containing all important metadata and security requirements should be created and everyone accountable for the data should adhere to it.

Access

Researchers should not have unrestrained access to all data; only those with an authorized mandate to use the data should be granted access. Data subjects should be allowed access to their data. Ease of access should be balanced with security requirements.

Security

Researchers and the organizations in which they are situated are responsible for data security. The level of security should be determined by the impact of data misplacement or disclosure. Security measures should balance security and ease of access. Data should be encrypted so that they are only usable for one particular application. A document containing all important metadata and security requirements must be created and everyone accountable for the data must adhere to it. Security measures should not expire until the data are destroyed; after data are disposed of, they should not be recoverable or at risk of disclosure.

Quality

Researchers are responsible for the accuracy and reliability ("data quality") of the data they use. Data should be corrected, updated, or revised when requested to do so as well as during regular audits and reviews.

System quality should also be monitored. Biometric error rates should be measured and acknowledged to data subjects and to users.

Independence

Research subjects should always have the right to receive a verbal explanation from a third party not connected with the research about how their information will be used.

Ownership

The data subject should be considered the rightful owner of their data.

Recommendations for research involving government-industry collaborations

Below are principles for ethical medical and biometric data collection, use, and retention and recommendations on how to observe them in FP7 research involving government-industry collaborations.

Purpose and proportionality

Researchers within government-industry collaborations should use data for a defined purpose in line with public opinion and the public interest. Inhumane procedures for collecting data and excessive data collection should be avoided. With appropriate consent, previously existing data should be used.

Security

Researchers within government-industry collaborations should ensure that data are stored securely and destroyed once the research is complete. Security safeguards preventing disclosure and preserving data quality should be in place.

Responsibility

Researchers within a government-industry collaboration should ensure that all members of the collaboration have basic, accurate, and up-to-date knowledge of relevant privacy laws. Written agreements and clear chains of command should be created so that it is clear what data protection principles are being enacted in the collaboration and who is accountable for their implementation.

Consent

Data may only be shared between government and industry researchers when the data subjects have given informed consent.

Commercial considerations

Commercial interests in medical research should be declared and limited when found to unduly influence the conduct of the research. However, it is acceptable to profit from the use or reuse of data when the data subjects are aware of this, the data subjects have consented to this, and the data are used for a legitimate purpose that is consistent with the purpose for which it was originally collected. Data subjects have a right to receive non-monetary compensation for their data, unless the use of their data will benefit society as a whole.

Access

Researchers within a government-industry collaboration should determine at the beginning of a collaboration who has access to which data. The researchers providing the data to the collaboration should ensure its distribution and reuse meets their institution's ethical codes. Government databases should simultaneously maintain privacy and confidentiality while remaining accessible and open to scrutiny.

Cooperative teamwork

Researchers within a collaboration should define rules for data sharing and management at the outset of the collaboration. Partners should work together to ensure the highest level of data protection.

Recommendations for research involving international data sharing

Below are ethical principles for FP7 research involving international medical and biometric data sharing.

Legitimate purpose
Privacy
Equity
Property
Trust
Security
Data quality
Autonomy
Responsibility
Non-maleficence

Confidentiality

Below are recommendations on how to observe these and other ethical principles in FP7 research involving international medical and biometric data sharing.

Transparency

Data subjects should be informed when their identifiable data are sent abroad or compromised abroad. Researchers should not send data abroad to circumvent data protection laws or practices. Consent should be obtained for sharing identifiable data or for sharing data across an unsecured network.

Access

Researchers should ensure that data subjects are able to access their data. Access should be limited to those with a legitimate purpose; all others' access should be limited via technical mechanisms.

Purpose

Only those with a legitimate purpose should be allowed to access the data; data may only be sent abroad for the purposes for which it was originally collected. Adequate consent for the purpose of the international data sharing should be obtained whenever identifiable data are shared.

Minimization

Researchers should only send abroad the data necessary to answer a specific question unless there are strong moral reasons to send more. The data should not be retained abroad longer than is necessary.

Quality

Researchers should ensure that data quality (including accuracy and completeness) and system quality are of a high standard and sufficient for purpose before, during, and after the international sharing of data.

Equal protection

Researchers should ensure that data quality, system quality, data protection, and security are maintained before, during, and after the sharing of data. Rules that apply to medical data in the data subject's home country should apply to that data anywhere in the world. Researchers sending data abroad must review and audit the recipient's security status. Data should not be shared abroad if they do not know how the data will be handled there.

Accountability

Researchers sharing data are accountable for the data.

Security

If a researcher undertakes a project that involves sending data abroad, this data must not be sent via an unsecured network. They should ensure that data exchanges are secure and uninterrupted by interference from third parties. Data security should be preserved through anonymisation, risk mitigation techniques, encryption, and regulation of the medium of transfer. Security should be maintained throughout the process of international data sharing.

Free movement

Researchers should share data across borders when there is an urgent need or strong moral reason to obtain data; for instance, if the data transfer will prevent loss of life or enable life-saving research.

Control

Data subjects should still have control over their data even if researchers send it abroad. They should be able to withdraw and access their data. They should also, where feasible, have the opportunity to rank different parts of their data in terms of sensitivity.

Equitable benefits

Allocation of benefits for the international sharing of medical data must be decided in advance. Medical or biometric data should not be shared when the researchers will be disproportionately benefited, unless there is compensation for the data subjects in the form of public goods.

Discussion and Conclusions

The principles stated above set out guidelines that provide a practical set of rules for what one must or must not do. The added value is that they create a sense of awareness of and engagement with this important issue. This code of conduct serves the purpose of being simple and easy to implement. These guidelines address the stages of data collection, use, retention, processing, and disposal.

These guidelines represent a final result of the ETHICAL project, derived from stakeholder consultations such as interviews, surveys, and a Delphi process. The code has been developed to balance universality and specificity. However, the code should not be considered rigid and unchangeable. It should be further validated by taking into account the opinions of members of the public across Europe. It should evolve over time to make sense to current stakeholders and data subjects as well as interpreted for different situations. In short, though the code of conduct above gives a snapshot of the opinions and perspectives captured by the ETHICAL project, it should evolve and adapt to varying circumstances, technologies, and cultures that are simultaneously pulling Europe closer together and farther apart.

References

1 EC European Research Area Science in Society (ERA SiS), European Textbook on Ethics in Research Studies and reports 2010, EUR 24452 EN, DG for Research, Science, Economy and Society, http://ec.europa.eu/research/science-society/document_library/pdf_06/textbook-on-ethics-report_en.pdf

2 EC European Research Area Science in Society (ERA SiS), Syllabus on Ethics in Research, Addendum to the European Textbook on Ethics in Research, Studies and reports 2010, EUR 24451 EN, DG for Research, Science, Economy and Society, http://ec.europa.eu/research/science-society/document_library/pdf_06/syllabus-on-ethics_en.pdf

3 ETHICS for Researchers EUROPEAN COMMISSION, Facilitating Research Excellence in FP7, Eleonore Pauwels, 10/2006-02/2007. http://europa.eu.int/comm/research/science-society

4 Pauwels E, ETHICS FOR RESEARCHERS, Facilitating Research Excellence in FP7, European Communities, 2007, ISBN 978-92-79-05474-7

5 EUR 23906 — Commission recommendation on A code of conduct for responsible nanosciences and nanotechnologies research & Council conclusions on Responsible nanosciences and nanotechnologies research

6 Zilgalvis P, Fitzgerald M, Hirsch F, Pauwels E, Integrating Ethics in EU Research 2009, EC Research DG, Unit L 3, Governance and Ethics, ftp://ftp.cordis.europa.eu/pub/fp7/docs/integrating-ethics.pdf

7 Fitzgerald M, The EU gets tough on ethics, 2007, Technology Ireland 03/07, 27-30

8 Ethics in FP7, http://www.fp7ireland.com/Page.aspx?SP=160

9 Ethics for Researchers, Facilitating Research Excellence n FP7, ftp://ftp.cordis.europa.eu/pub/fp7/docs/ethics-for-researchers.pdf

10 Pauwels E., Activities of the Unit "Governance and Ethics" Unit , "Governance and Ethics" section of the "Science, Economy and Society" Directorate's portal: http://europa.eu.int/comm/research/science-society

11 The European Parliament and the Council of the European Union. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Retrieved from http://ec.europa.eu/justice/doc_centre/privacy/law/index_en.htm#directive

12 European Commission. (2007). Towards a Code of Conduct for Responsible Nanosciences and Nanotechnologies Research. Consultation Document: http://ec.europa.eu/research/consultations/pdf/nano-consultation_en.pdf

13 COMMISSION RECOMMENDATION of 07/02/2008, On a code of conduct for responsible nanosciences and nanotechnologies research, Brussels, 07/02/2008 C(2008) 424 final

14 EUROPEAN COMMISSION, The European Charter for Researchers , The Code of Conduct for the Recruitment of Researchers, 2005, Human resources and mobility EUR 21620, ISBN 92-894-9311-9

15 FP7-Information and Communications Technologies Guide for Applicants, Annex 5: Ethical Guidelines for undertaking ICT research in FP7, ftp://ftp.cordis.europa.eu/pub/ist/docs/rn/070202-global-info-dayv3-annex2_en.pdf

16 Karatzas I, Ethics Review and FP7 Ethics Framework, Head of the Ethics Review Sector, Unit for Governance and Ethics, Directorate L: Science, Economy and Society, European Commission, Research Directorate-General

17 Kautz Ch, Deputy Head of Unit Security Research and Development, EC, 2010, Security and Ethics in FP7 The example of Security Research, http://ec.europa.eu/enterprise/security/index_en.htm

18 EC CORDIS, Research Ethics: A comprehensive strategy on how to minimize research misconduct and the potential misuse of research, 2010, ftp://ftp.cordis.europa.eu/pub/fp7/docs/misconduct-misuse_en.pdf

19 Von Schomberg R, Understanding Public Debate on Nanotechnologies, Options for Framing Public Policy, 2010 DG for Research, Science, Economy and Society EUR 24169 EN, http://ec.europa.eu/research/science-society/document_library/pdf_06/understanding-public-debate-on-nanotechnologies_en.pdf

20 D3.1 The ethical implications of data collection, use and retention, http://www.ethical-fp7.eu/index.php?option=com_docman&task=doc_details&gid=14&Itemid=78

21 D3.2 Guide on Government – Industry collaborations, http://www.ethical-fp7.eu/index.php?option=com_docman&task=doc_details&gid=15&Itemid=78

22 D3.3 Ethical requirements for international biometric and medical data sharing, http://www.ethical-fp7.eu/index.php?option=com_docman&task=cat_view&gid=34&Itemid=78

23 D4.2 Ethical recommendations for EC policy directives, http://www.ethical-fp7.eu/index.php?option=com_docman&task=cat_view&gid=34&Itemid=78

24 D4.3 Report on social and financial impact of data collection, use and retention in medical and biometric applications, http://www.ethical-fp7.eu/index.php?option=com_docman&task=doc_details&gid=16&Itemid=78

25 D2.1 Dialogue Consensus Results , http://www.ethical-fp7.eu/index.php?option=com_docman&task=cat_view&gid=34&Itemid=78

26 D4.4 International Benchmarking Report on code of conducts in specific area, http://www.ethical-fp7.eu/index.php?option=com_docman&task=cat_view&gid=34&Itemid=78

27 D4.1 Code of conducts for FP7 researchers in the areas of medical and biometric research, http://www.ethical-fp7.eu/index.php?option=com_docman&task=cat_view&gid=34&Itemid=78

28 D3.2.2: Guide on government-industry collaborations, http://www.ethical-fp7.eu/index.php?option=com_docman&task=cat_view&gid=34&Itemid=78

29 D3.3.2: Ethical requirements for international data sharing , http://www.ethical-fp7.eu/index.php?option=com_docman&task=cat_view&gid=34&Itemid=78

30 D2.2: Dialogue consensus results, http://www.ethical-fp7.eu/index.php?option=com_docman&task=cat_view&gid=34&Itemid=78

31 Tavlaki, E.: Code of conducts for FP7 researchers in medical and biometric data privacy, eChallenges e-2010 Conference Proceedings, Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, 2010, ISBN: 978-1-905824-21-2

32 Siew, Mohd-Nor, Swartzman, Lim, Cox, Yeo, Menevidis: Ethical Implications of Digitised Medical and Biometric Data eChallenges e-2010 Conference Proceedings, Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, 2010, ISBN: 978-1-905824-21-2

33 ESF-ORI Workshop, "Responsible Conduct of Research:, Good research practices and research integrity training", 27/28 October 2009, REPORT, www.esrif.eu

34 ESF-European Science Foundation, SUMMARY OF ESF INTERNAL CODE OF CONDUCT, October 2010, http://www.esf.org/index.php?eID=tx_nawsecuredl&u=0&file=fileadmin/be_user/Communications/code_of_conduct/ECOC_docs/Summary_ESF_Internal_Code_of_Conduct.pdf&t=1288378862&hash=b1114864cdc6c05c624eba97d06c5162

35 ESF-European Science Foundation and ALLEA (All European Academies) , European Code of Conduct for Research Integrity, 2010, http://www.esf.org/activities/mo-fora/research-integrity.html

36 ESF Code of Conduct, http://www.esf.org/index.php?eID=tx_nawsecuredl&u=0&file=fileadmin/be_user/CEO_Unit/MO_FORA/MOFORUM_ResearchIntegrity/AffichetteA3_CodeOfConduct.pdf&t=1300446849&hash=b74a82c20d93b6e4ba1d422302186399

37 ESF-European Science Foundation, Fostering Research Integrity in Europe, A report by the ESF Member Organisation Forum on Research Integrity, December 2010, http://www.esf.org/activities/mo-fora/publications.html

38 ESF-European Science Foundation, TABLE OF GAP ANALYSIS: EUROPEAN CHARTER FOR RESEARCHERS AND CODE OF CONDUCT FOR RECRUITERS OF RESEARCHERS, 2010 ESF, http://www.esf.org/index.php?eID=tx_nawsecuredl&u=0&file=fileadmin/be_user/Communications/code_of_conduct/ECOC_docs/Table_of_gap_analysis_Code_of_Conduct_for_Researchers_FINAL.pdf&t=1288378862&hash=3aed80160fe54c70598ab11486c5189b

39 Code of Conduct for Responsible Research Practice and Guidelines for Dealing with Allegations of Research Misconduct http://sydney.edu.au/ab/policies/Rsch_Code_Conduct.pdf

40 Code of Conduct for Researchers http://www.correctiveservices.wa.gov.au/_files/about-us/statistics-publications/students-researchers/research-code-conduct.pdf

41 Code of Ethics for Researchers of the Academy of Sciences of the Czech Republic At its XXVIII session held on 20 April 2006, the Academy Assembly approved the following Code of Ethics of Researchers of the Academy of Sciences of the Czech Republic.

42 Schneider JL, Professional Codes of Ethics : Their Role and Implications for International Research, Journal of Contemporary Criminal Justice 2006 22: 173, , http://ccj.sagepub.com/content/22/2/173.full.pdf+html

43 Butrous, E., Faber, B., Gupta, C., Haggart, C., Jawad, M., and Patel, S. (2010). A study to define the international guidelines of ethics concerning electronic medical data. Unpublished manuscript, Imperial College London.

44 Yearbook of Medical Informatics, Quality of Health Care: the role of informatics, 2003, pages 135-140

45 e-Health Ethics Initiative. e-Health Ethics Draft Code. J Med Internet 17/6/09, http://www.jmir.org/2000/2/e9/ C. Boyer, M. Selby, J.-R. Scherrer, R.D. Appel, The Health On the Net Code of Conduct for medical and health Websites, Pergamon, Computers in Biology and Medicine 28 (1998) 603±610

46 Hutton, JL, Ethics of medical research in developing countries: the role of international codes of conduct, Statistical Methods in Medical Research, http://smm.sagepub.com/content/9/3/185

47 HEALTH-NCP-NET, Ethics Advisory Workgroup (EAWG), Mistakes made and how to avoid them, http://www.healthncpnet.eu/jahia/Jahia/pid/25

48 World Medical Association, Declaration of Helsinki, Ethical Principles for Medical Research Involving Human Subjects

49 International Biometric Industry Association (IBIA) Statement of Principles and Code of Ethics

50 Universal Declaration on Bioethics and Human Rights, UNESCO, 19 October 2005

51 InterNational Committee for Information Technology Standards, INCITS Secretariat, Information Technology Industry Council (ITI) , Study Report on Biometrics in E-Authentication, 2007, M1.4 Ad Hoc Group on Biometric in E-Authentication (AHGBEA)

52 Irish Council for Bioethics 2009, Biometrics: Enhancing Security or Invading Privacy?, Proceedings of the Irish Council for Bioethics' Conference 26th November 2008, Dublin

53 Mordini E, Biometrics, Human Body, and Medicine: A Controversial History, Chapter XI in, Duquenoy P, George C, Kimppa K, Ethical. Legal and Social Issues in Medical Informatics, 2008, IGI Global

54 Human Genetics Commission, The forensic use of DNA and the National DNA Database, Cosultation Questions, 2009, Human Genetics Commission, Department of Health , www.hgc.gov.uk , 6th Floor North, Wellington House, 133-155 Waterloo Road, London SE1 8UG

55 Mohd.Salleh N, Mohd.Saat R, Ethical codes of conduct and practices using human subjects, WCLTA 2010, Procedia Social and Behavioral Sciences 9 (2010) 2021–2025, Available online at www.sciencedirect.com

56 Van der Wall EE, Summa cum fraude: how to prevent scientific misconduct, Neth Heart J (2011) 19:57–58 DOI 10.1007/s12471-010-0062-4, Published online: 14 January 2011 , The Author(s) 2011. This article is published with open access at Springerlink.com

57 The MASIS report, Research Policy, Challenging Futures of Science in Society , Emerging Trends and cutting-edge issues, EC- European Research Area (ERA), EUR 24039, 2009

58 European Security Research & Innovation Forum (ESRIF), Final report, December 2009

CHAPTER 8
Privacy Perception in the ICT era and beyond

Aharon Hauptman, Yair Sharan and Tal Soffer

Introduction

> *"The personal life of every individual is based on secrecy and perhaps it is partly for that reason that civilized man is so nervously anxious that personal privacy should be respected". (Anton Chekhov).*

Contemporary and future developments in science and technology put the state of privacy in a great uncertainty. Our "secrets" are uncovered layer by layer by more and more intruding technologies. How will we perceive privacy in this changing technological environment? How would society cope with these developments in this future era?

The majority of the population does not question privacy as a basic right. Most people take the protection of personal data and the respect of the personal space within their houses for granted. The fact that privacy is granted in Article 12 of the United Nations Universal Declaration of Human Rights[1] supports this view and stresses the importance of private realms. Taking a closer look at how privacy is defined, we find that there is no consistent definition of what privacy is. As the article on privacy in the Stanford Encyclopedia of Philosophy states, the term 'privacy' is used frequently in ordinary language as well as in philosophical, political and legal discussions, yet there is no single definition or analysis or meaning of the term." (DeCew and Judith 2008). Generally, we can state that privacy is closely related to the concept of intimacy including physical integrity, but there are a lot of other dimensions of privacy (spatial, emotional/inner life of a person) that privacy incorporates that cannot be discussed in greater detail at this point. The probably most famous definition was given by the American judge Thomas M. Cooley, who defined privacy as the 'right to be let alone' (Cooley, 1888). This broad definition included the protection of life and (intellectual) property as well as feelings (Kleve and de Mulder 2008) and is the starting point for many definitions of privacy that were developed later.

Another famous definition of privacy that includes the nowadays important aspect of communication is given by Alan Westin. He describes privacy as informational self-determination when he says that "privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1970). This definition already includes the currently most important dimension of data protection that in the age of information technologies dominates the discussion on privacy.

As we can see, the concept of privacy is not a universal one and changes with time, adapting itself to the necessities and constraints of a society. Kleve and De Mulder write that "the scope of the concept of privacy, and its interpretation, must be seen against a background of technical and social developments" (Kleve and de Mulder 2008, 230). Therefore, privacy seems to be a socio-cultural construct, depending on dominant values of a society, its socio-cultural heritage and contemporary technological developments. According to this understanding the ideas and perceptions of privacy can change in time with technology being an important driver in shaping our concept of privacy, as it directly influences our daily lives and our values.

1 United Nations 1948, Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Emerging technologies and privacy

Imagine the year 2050. Or, if you like, 2040. Advances in brain-computer interface have led to "radio-telepathy" enabled by direct conversion of neural signals into radio signals and vice versa. Everyday gadgets are operated "by thought", and "mind reading" is readily available. How would this affect privacy? Certainly it could become be the ultimate intrusion to privacy, when even one's thoughts are not secret anymore! Or would it? Perhaps in a society where a direct brain-to-brain communication is common and natural, "reading" one's thoughts would be as natural as looking at that person? It is important to note that "mind reading" and "synthetic telepathy" are not farfetched ideas. It could be one of the next steps of brain-computer interface (BCI), enabled by direct conversion of neural signals into radio signals and vice versa. First gadgets with limited features of operation "by thought" are already on the market. According to a Delphi foresight survey conducted by the Japanese National Institute of Science and Technology Policy (NISTEP report No. 97), it is likely that by the year 2029 computers will be able to read the information recorded in the human brain. A report by a think tank of the UK MOD foresees that *"By 2035, an implantable information chip could be developed and wired directly to the user's brain. Information and entertainment choices would be accessible through cognition and might include synthetic sensory perception beamed direct to the user's senses. Wider related ICT developments might include the invention of synthetic telepathy, including mind-to-mind or telepathic dialogue."* What would be the societal implications, including privacy? The famous physicist Freeman Dyson speculated about a system of such implantable chips and its potential to become a powerful instrument of social change, for good or for evil purposes. Even present day brain scanning technologies, still far from "real" synthetic telepathy, already raise non-trivial questions related to privacy. Consider functional MRI (fMRI), and in particular real-time fMRI, already in use for research and for medical diagnosis and therapy. Although "reading thoughts" by fMRI is impossible, it is possible to "read" emotional states and to detect lies in a reliability much higher than the old-fashioned polygraphs. Such advancing capabilities made researchers think whether this may lead to a new frontier: mind privacy:

> *"The foreseeable ability to read the state of a person's brain and thereby to know aspects of their private mental experience, as well as the potential to incorrectly interpret brain signals and draw spurious conclusions, raises important new questions for the nascent field of neurotics. One can imagine the scenario of someone having their private thoughts read against their will, or having the contents of their mind used in ways of which they do not approve"* (deCharms and Christopher 2008)

The impact of new technologies on privacy, and technology-driven changes in privacy perceptions are not new phenomena. Consider the long history of photography. After the invention of the first cameras that used light-sensitive chemicals, the first photographic portrait image of a person was produced in 1839. This new technology was then mostly used to produce private portrait photographs of wealthy people in special studios – a complicated, lengthy and costly process involving cumbersome static cameras. The photographed person had full control of the result, and it was unheard of that photo-portrait is reproduced (not to mention distributed in public) without the permission of that person. After a few years, technology advances led to smaller hand-held cameras, by which a picture could be taken without its subject even knowing that a camera was present. "Detective cameras" became increasingly popular in the 1880's, followed by a rapid spreading of journalistic snapshot photography, which was enthusiastically used by journalists in public (and often in private) locations. In a way it was "the end of privacy" by the 19-th century standards, at

least for celebrities. No wonder that the first publication advocating privacy was written in 1890 largely in response to this new trend. It was "The Right to Privacy" by Warren and Brandeis (Warren and Brandeis, 1890), considered by many as one the most influential law review articles ever published. With regard to "the unauthorized circulation of portraits of private persons" and "the evil of invasion of privacy by the newspapers" Warren and Brandeis asserted that in the intense life of an advancing civilization *"solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."* They referred not only to the technology of photography but also to other so-called "modern devices":

> *"the existing law affords a principle from which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds".*

More than 120 years passed since Warren and Brandeis called for protecting by law "the right to privacy" endangered by the abuse of "modern devices" such as cameras. What would the authors say about the descendants of the inventions that they witnessed the widespread digital photography of the 21st century and the routine sharing of billions of photos on the Internet? The technology-enabled online social networks phenomenon, in particular Facebook with its photo-sharing and other features, is of course a present-day example of changing attitudes to privacy, especially among young people. But this is just a hint about what may be lying ahead. As the technology evolution continues, "Augmented Reality" (AR) incorporated in smart phones with cameras and face-recognition features will enable to point your smart phone at a person, and the face recognition system will recognise and "label" him or her based on information available online. But what if that person doesn't want to be automatically identified in that particular time and place? And this is just one example of the new challenges to the very notion of privacy. Unprecedented challenges may arise from other not only from the information and communication technologies (ICTs), but also from other fields of science and technology. Some forward-looking examples are described below, based on the "horizon scanning" activity undertaken within the EU FP7 project PRACTIS.

Imagine the year 2040 again, or, if you like, 2030. Anthropomorphic household robots are people's companions. Machines resembling humans, speaking with humans, behaving almost like humans, are part of our daily life. The Ministry of Information and Communication of South Korea has estimated that every South Korean household will have a robot by 2020 (BBC News 2007). Besides the obvious privacy concerns related to the surveillance capabilities of robots (the ability to sense, process, and record their surroundings), there are less obvious social and psychological implications. Would you feel comfortable to undress in front of a friendly smiling robot? Or would you speak about your intimate secrets while the robot is listening? Why not, don't you do it in front of your cat? The answer is not simple. Studies have shown that that people tend to react to anthropomorphic technologies such as robots as though a human being were actually present, including the sensation of being observed and evaluated. According to researchers in this area (Calo, forthcoming paper), "the privacy challenges of social robots will require an in depth examination of human-robot interaction within multiple disciplines over many years."

If intelligent humanoid robots seem to you as nothing special, imagine invisibility. Although Harry Potter's style "invisibility cloak" looks like pure fantasy, scientist have recently shown that by tailoring the light-refraction index of special nano-structured materials it is

possible to make tiny objects invisible (in certain wavelengths), or even make them look like completely different objects. More progress in this exciting area could turn the "invisibility cloak" from fantasy to reality. The ongoing EU FP7 project iKnow has described an "invisibility spray" sold in supermarkets as one of possible future technological "wild cards" (events with low likelihood but high impact). Imagine being invisible: a perfect privacy protection, isn't it? Or maybe it is a perfect privacy intrusion, if an invisible person (or invisible device, for that matter) spies on you?

In the project PRACTIS attempt is made to understand and evaluate three kinds of potential impacts of emerging technologies on privacy: threats to privacy, privacy enhancement, and changing of our perceptions of privacy. The first kind of impact is rather straightforward. It refers for instance to technologies that make it easier for information about people to be collected and analysed. The second kind of impact refers mainly to Privacy Enhancing Technologies (PETs), or to emerging technologies that could enable new PETs, such as methods for anonymisation of databases before analysing them. Certain emerging technologies have both a potential to pose new threats to privacy as well as to enhance privacy (sometimes indirectly), depending on the specific application. The third kind of impact (change of perception) is the most complex, and is hard to attribute to any one technology by itself. People may get used to "intrusive" technologies such that they no longer consider them a threat to their privacy. Similarly, people may be willing to accept certain privacy violations and even not to perceive it at all as a threat to privacy, if the benefits brought by the new technologies are concrete. In other words, people may be willing to "sacrifice" some of their privacy for concrete benefits such as improved security, lower insurance costs, better health services and the like.

The next "big things" in the information and communication field are the closely related visions of Ambient Intelligence (AmI), "Internet of Things" (IoT) and "ubiquitous computing". They pertain to an idea of "invisible" computers embedded everywhere, and a multitude of interconnected objects. Thanks to a variety of sensors, such system will react appropriately to changes in its environment, particularly to human behaviors. Consider, for instance, the visionary project initiated by HP labs, called CeNSE (Central Nervous System for the Earth) (see www.hpl.hp.com/news/2009/oct-dec/cense.html). It aims to build a worldwide network composed of billions of tiny, cheap, and exquisitely sensitive detectors integrated in buildings to warn of structural damages, scattered along roads to monitor traffic and road conditions, and embedded in everyday electronics to track equipment or "recognize" the user and adapt accordingly. A "sniffing and tracking" worldwide system like CeNSE, with all its potential benefits, raises obvious questions and concerns about privacy, especially if combined with the emerging capabilities of so-called "Reality Mining". This term has been coined by MIT researchers as a new paradigm in data mining based on the collection of machine-sensed data from mobile phones, cellular tower identifiers, GPS signals and host of other sensors, to discover patterns in daily user activity and possibly to predict what a group (or even single user) will do next. Such capabilities hold the promise of "socially aware" applications and technologies (this is part of the AmI vision), but massive collection of data pertaining to human social behavior obviously raises privacy questions. Moreover, much of the computing performed today entirely on computers owned and controlled by users will shift in the near future to "the cloud". Cloud computing, namely the provision of computing resources as a service over the Internet, was selected by Gartner as one of the "top 10 strategic technologies" for 2011. A great promise, but whenever somebody shares information in the cloud, privacy or confidentiality questions are likely to arise, and convincing answers are yet to come.

Although most privacy threats discussed nowadays are usually related to the Internet, or more generally to information and communication technologies (ICT), PRACTIS pays special attention to other areas, such as nanotechnology, biology, robotics, and cognition-related technologies. Nanotechnology advances may significantly improve our quality of life, but they are also likely to enable unprecedented capabilities of surveillance and information-gathering – with obvious privacy implications. Indeed, surveys have shown that "losing personal privacy" is the public's biggest fear about Nanotechnology. One of the emerging nanotechnology developments are ultra-sensitive nanosensors, which will have a dramatic impact on medicine and security – and on privacy. Molecular nanosensors can detect a single molecule and distinguish between different molecules. It is expected that such sensors will be able, for example, to detect drugs from saliva samples of people, or to detect where a person has been by quickly sampling minute environmental clues on clothes. No wonder that researchers have expressed growing concerns about so-called 'nano-panopticism'. In a recent article published in the prestigious journal "Nature"(Toumey, C., 2007), Toumey, one of the scientists active in this field, called the emerging molecular nanosensors "plenty of eyes at the bottom" (Feynman, R. 1959) and expressed his worries about a "molecularly naked patient" whose insurance company knows more about his body than himself:

> *"with so many huge databases of personal information, plenty of eyes at the bottom, molecularly naked patients and more, it is hard to imagine how multiple developments in nanotechnology will not intrude further into our privacy".*

Interestingly, from a different point of view the same ultra-sensitive nanosensors may actually protect privacy rather than threaten it, at least in the context of law enforcement. Why? Because highly accurate sensors, with no false alarms, can curb arbitrary collection of private information irrelevant to a legitimate interest (information that policemen often arbitrarily collect while searching for suspects) and thus protect the privacy of most people (Rubel, 2010). This is one example that shows how a technology can potentially enhance privacy as well as to pose a threat to privacy, depending on the context of application.

Similar nanodevices will bring the vision of personalized medicine closer to reality, by providing better genetic diagnostics. This would certainly be beneficial to our health. But personalised medicine is based on comparison of diagnostic information about one's body with similar information about other people. This implies storing vast amounts of personal medical information in centralized systems. How would this affect people's sensitivity about their privacy?

Major trends and their generational impact

The thoughts and findings described above signal significant trends which will have a future impact on the ethical as well as legal frameworks dealing with data protection and privacy as we know them today. Understanding these trends as early as possible would help society be better prepared to this emerging future. These trends are in fact defining some of the challenges society has to cope with while adapting these frameworks to the actual state of affairs.

First trend to be evaluated is the shift from data collection and storage for future use to real time application of the data collected. This phenomenon is interesting since on the one hand all the data protection problems connected with security of databases, for example

are suddenly solved since no need of storage exists. But on the other hand our control of our personal data might be lost, a situation which might impact principal values of liberty and human dignity. This trend is further strengthened by the second one which is the developed ability to collect and process data on humans themselves rather than on human activities only. We approach the era in which emotional and biometrical data are broadly monitored, identified and stored. Our genetics, our feelings and emotions and finally our thought could be exposed without our permission, against our will, without our knowledge. Our control of the most sensitive and personal kind of data would be slowly lost. Even if this trend seems far reaching no doubt that the third trend knocks on our doors – technology is omnipresent. Sensors become smaller and smaller and data collection becomes possible everywhere and from greater distances. A person should take into account that one can learn much on her or him from a distance without his knowledge. Public space would be flooded with diversity of sensors collecting many sorts of data to be analysed in sophisticated ways. Our control on our personal data becomes even more difficult and data protection more problematic. These developments are accompanied by yet another trend, which is the increase of sensing and data accuracy. This might reduce the need of collecting unnecessary information on people since fewer mistakes are expected. Privacy will be thus enhanced. Moreover, it will reduce the need for profiling procedures and practices which prevail in many systems and are problematic and criticized because of equality as well as dignity points of view. This trend has advantages in societal needs like security. Looking at it from a responsible innovation point of view this development reduces intrusion into human privacy to a minimum need, if at all, helping secure people in a more efficient and less objectionable way.

The impact of these envisioned technological trends will be mainly experienced by the present young generation, in whose adulthood years these changes will be realized, and who will probably undergo changes in their perception of privacy. "Privacy is no longer a social norm" announced the founder of Facebook Mark Zuckerberg in January 2010 and provoked wide debate about youth and privacy. Is the idea about young people eager to reveal and expose their private lives to the world more than a myth? Will the future generation give up privacy under the influence and perceived benefits of emerging technologies?

Currently, changes in the perception of privacy are mostly understood in terms of a decrease in the importance ascribed to privacy as a value, or a gap between privacy as a value and a displayed self-revealing behavior. Many surveys show that privacy remains an important value. Nevertheless, personal data has become a commodity which could be traded with perceived benefits. In this context, privacy, defined as control over personal information, is at risk and declines due to new business models and technologies (Rust et al 2002).

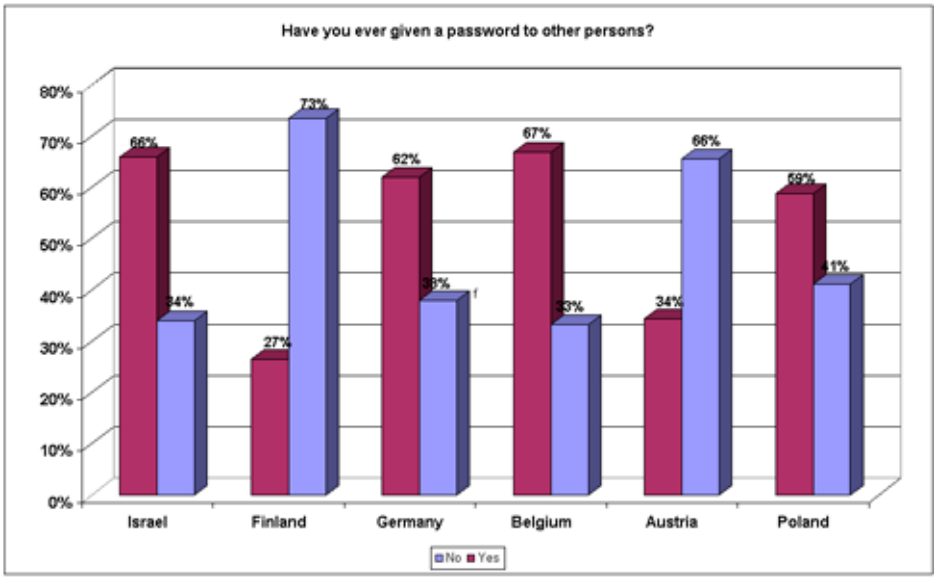
Emerging technologies in various fields play an important role in this development. Most of the empirical data on this issue concentrates on the use of the Internet and Social Network Sites (SNS), or on surveillance technologies such as CCTVs. As this technology is accessible only since recent years to a broad public, researchers are contemporarily very interested in how the Internet changes people's behavior and attitudes. Especially interesting is a comparative analysis of the behavior and attitudes of parents and contemporary adolescents and young adults who grew up within the Internet age . In his book "Born Digital" (Prensky 2010), Prensky distinguishes between "Digital Natives" and "Digital Immigrants": "Digital Natives" grew up being surrounded by and using all kinds of digitally based information and communication technologies. This has changed their way of learning/thinking compared to "Digital Immigrants" who did not grow up with these new technologies. "Digital Natives" are used to quick information access, networking, parallel processes and

multi-tasking, immediate gratification, frequent rewards and a game-like access to tasks they have to complete. "Digital Immigrants" rather prefer individually solving problems by slow and serious step-by-step processes. Recent studies such as the PRACTIS project go further and explore attitudes towards more sophisticated applications such as RFID and body scanners which intrude privacy even more. In order to study these emerging trends, especially in the context of generational gap, a study was conducted in the framework of the recent EU PRACTIS project. (www.practis.org)

A wide range European school survey was realised among more than 1400 children, 15 to 20 years old. In addition a survey among control group of 200 parents (answering the same questionnaire) was conducted. The results could assist in gaining understanding of perceptions of privacy among adolescents ("digital natives") and adults ("digital immigrants") as well as shed light on attitudes towards new and emerging technologies, of the ICT era and beyond. In addition it could highly contribute to future responsible policy design taking into account different scenarios of future societies balancing the relationships between privacy and emerging technologies. This survey as well as results from other studies revealed some important findings:

(1) **The concept and perception of privacy is important to adolescents but is transforming.** The PRACTIS school survey results show that most of the adolescents think that data protection is important or very important (75%) although more than 55% of them are willing to give their password to others (mainly to friends and family members). In that sense we can see differences between the teens' attitudes based on their country belonging. Adolescents from Finland and Austria are more conservative and most of them do not give their password while most of the adolescents from Israel, Germany, Belgium and Poland tend to give their password (see figure 1).

Figure 1: Password given by adolescents by countries



They are also very sensitive about their privacy and would like to have control on their personal data and those who it. An interesting US-study found that expressed attitudes towards privacy by young adults (aged 18-24) are not nearly as different from those of older adults as many suggest. An important part of the picture, though, must surely be the finding that higher proportions of 18-24 year olds believe incorrectly that the law protects their privacy online and offline more than it actually does. This lack of knowledge in a tempting environment may be an important reason why large numbers of them engage with the digital world in a seemingly unconcerned manner (Hoofnagle et al 2010).

(2) In the context of SNS we can see that **most adolescents (88%) have and use Social Network Sites (SNS)** (PRACTIS, 2011), however the meaning of privacy develops towards a so called flexible audience management. This means that teenagers decide which kind of information they want to share with whom. (Boyd 2008; Madden, Smith 2010). According to the PRACTIS survey, adolescents use SNS mainly for communicating with friends and staying in touch with them (see figure 2). The kind of information they post online is usually their name, gender, school, relation status, age, hobbies, photos (usually of themselves) and comments. They do not post their real address, phone number or e-mail (see figure 3). According to Brüggen. (2009), SNS are considered as private space because the user can exclude specific persons from certain information. In the PRACTIS survey we found that the adolescents' profile is partially public, in most cases to their friends.

Figure 2: Importance of SNS' activities

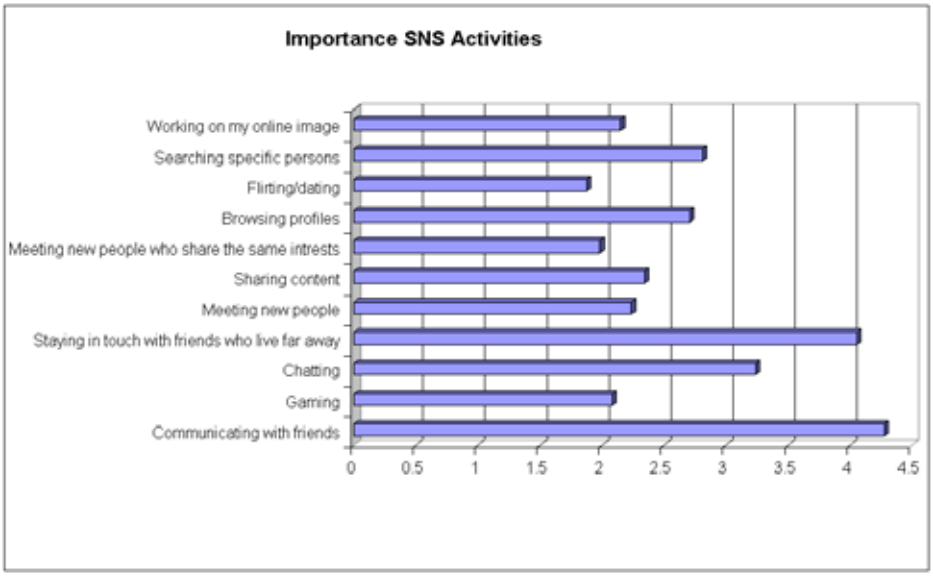
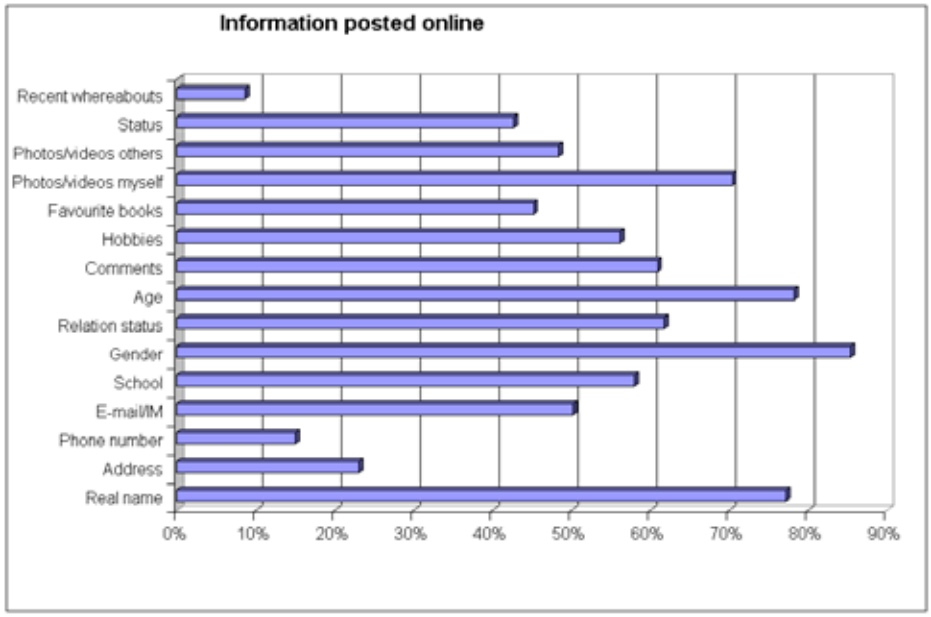


Figure 3: Information posted online



(3) **Many users have little knowledge or even misconceptions about visibility and privacy policy.** According to a study of 2006 users have little knowledge or even misconceptions about visibility and privacy settings on Facebook (Acquisti and Gross 2006). In a study conducted by Dwyer (2008) 19 percent of the test persons, who used SNS very frequently, experienced privacy incidents like inappropriate personal messages, spam mails or pornographic content being posted on their profile. Only about half of those reviewed and changed their privacy settings, many users did not even really know how to change their privacy settings (Dwyer and Hiltz 2008). Furthermore a study with 674 Austrian university students shows that there's only little knowledge about online surveillance and privacy policy but high awareness of privacy and security problems online. This awareness results only partially in an adequate online practice although students do not really trust their SNS-providers. (Fuchs 2009). When they are confronted with possible risks, most students show true consternation but privacy settings are only changed when the self-representation on the SNS stays attractive (Wagner et al 2009). Teens usually know that there might be persons browsing their profile to whom their content might seem inappropriate but their relevant reference is their peer group. Long-term consequences of data revelation are often underestimated (Ofcom 2008). In the PRACTIS survey we found similar results. When you inform the kids that by using apps which are offered by Facebook, for example, they are making their profile information available and usable for others, they refuse to use these apps.

(4) **Students' privacy settings on SNS are affected by their lifestyle.** The more friends someone has with a private profile the more likely he will have a private profile too. The more frequently someone visits his profile the more likely he will make use of privacy settings. Women are more likely to have a private profile than men are.

Students who have a private profile have different preferences concerning movies, music and books. So there might be a connection between cultural preferences and attitudes towards privacy, i.e. privacy settings seem to be an expression of a certain lifestyle (Lewis et al. 2008)

(5) **Students using SNS are aware of potential risks like privacy intrusions or misuse of personal data but they are not concerned about privacy invasion and data abuse.** Most of the teens felt that they did not experience misuse of personal data (92%) and do not feel that they need more protection (75%) in the Internet. They feel quite safe using the Internet but they would like to have control on their personal data and keep their privacy (PRACTIS school survey 2011).One reason is that according to their self perception they know how to help themselves by using privacy tools on SNS (Borreson Caruso and Salaway 2008). Teenagers are aware of risks linked to online data revelation so they use different tools and techniques to manage who gets access to their information. Teens would not give as much information to people online as in an offline situation (Lenhart and Madden 2007). According to a study by Tufekci (2008) there is no relationship between privacy concerns and information disclosure on SNS. Tufekci generally distinguishes between instrumental (e.g. shopping) and expressive (e.g. SNS) internet use. Only in the first case data security is a relevant aspect. In the other case people want their information to be seen. The main reason to hide certain information is not a general privacy concern but fear of unwanted visitors. Both fears lead to audience management through privacy settings or the posting of incorrect information that is search relevant, but they do not cause less disclosure. Although students are trying to control their data by reducing the number of persons who have permission to enter their private area, they are less aware of long-term problems of data-revelation (Tufekci 2008). Generally, the security awareness of high intensity users of SNS leads to higher security knowledge as is the case with a higher level of education. All in all negative experiences with web usage are relatively unimportant (Schmidt et al 2009).

(6) **Adolescents are willing to use new technologies but they are balancing between the advantages of using new technologies and protecting their privacy/personal data.** They are more sensitive to privacy concerning their own private domain (home, body) compared to public domain. In various scenarios which were presented to adolescents within the PRACTIS school survey we found for example that in ascenario called "Rock Concert" most teens would use personalized electronic bracelet in order to receive benefits such as: lower entry price , lower price for drinks or free drinks, shorter waiting times etc. However in another futuristic scenario called "Health monitoring sensors" where the teens were asked if they would use medical sensors (on the wrist or implanted under the skin) to measure all their health personal data continuously, in order to improve their health condition, and receive better and cheaper medical treatment, they were more sensitive to their privacy and most of them answered that they will use it only if they could have control on the data (when and to whom to send it). Furthermore, a study from 2008 found out that people are quite careful with biometrical data. There are high trade-offs especially if data might be given to private parties. Technological security techniques are often preferred to physical ones; people are somehow used to and thereby tolerant towards CCTV. Additionally the study on the use of personal sensing devices shows that people make trade-offs between the perceived value of an application and the costs (potential privacy intrusion) (Klasnja et al 2009).

Challenges and conclusions

In conclusion, privacy in the era of information and communication technologies and beyond is more and more challenged by increasingly intruding technologies risking privacy as we perceive it today. Technology will be present everywhere, potentially driving society to be constantly watched with no place to be let alone. The basic right for privacy which is the basis for the present data protection and privacy laws and ethical societal behavior is threatened.

Society actors as well as policy makers are thus confronted with some significant challenges which are at the center of their mutual responsibility. The first challenge is that these technological trends should be carefully assessed in a long range perspective in order to anticipate negative as well as positive impacts and early identify risks and breaches of present legal and ethical frameworks. This will enable better preparation of society to the possible shift from information society to the so called ubiquitous society (which in fact means "ubiquitous networks society"). Second challenge resulting from the first would be the possible need to control technology proliferation in order to find ways to prevent those risks from being realized. The clash between two assumed basic principles should be assessed: Privacy on the one hand and the freedom of science and innovation on the other hand. Privacy by design principle would be widely considered as a necessary measure in the R&D and production processes to minimize the risks involved if not prevent them altogether. The third challenge would be an even more proactive one which involves changing the role of the data protection agencies from watchdogs to partners of citizens to protect their privacy in a broader sense. Would these agencies be active in governments only? In businesses? Will they help activity to prevent misuse of technologies through unneeded privacy intrusions? A final challenge concerns the generational gap. Is privacy generation dependent? Will present youngsters perceive privacy differently in the future? Will they adapt themselves to the changing technology environment? The constant dialogue between societal actors as well as decision makers should evaluate and discuss these issues regularly. Decisions taken at present impact and shape society of tomorrow. The future societal actors and decision makers are the adolescents of today. Thus acceptability and sustainability of these processes should be ensured and guarantied taking into account attitudes of present and future actors.

Empirical data shows that users are aware of possible risks and develop different strategies to handle them. The ability to respond to potential risk increases with rising awareness for such risks. Privacy is not different in this respect. The individual's responsibility in handling her or his personal data on the Internet, for example, seems to be a basic measure for reducing the risk of privacy intrusion. Nonetheless one can deduce from the empirical data found that a change of privacy perception is underway. This doesn't imply that privacy is less important to the "Digital Natives" then to the "Digital immigrants". General studies and research on the topic of privacy indicate that awareness for privacy intrusions and support for the right for privacy have not diminished in the past decades.

Awareness-raising is thus one of the most important measures to minimize existing risks of privacy intrusions and abuse of personal data. Such educational programs must include general information about the long-term risks of posting personal information as well as more detailed information on how to use existing privacy settings on SNS. In this context thinking on the future SNS should take place to possibly remedy the weaknesses of the present ones. This raising of the children's awareness cannot be done only by their parents

but also must be a new task for teachers and educators. Given the entire aspects raised in this paper this step would be the tip of the iceberg but will be a modest step forward in coping with the challenges society is facing.

References

Acquisti, Alessandro; Gross, Ralph. 2006. "Imagined Communities. Awareness, Information Sharing, and Privacy on the Facebook". Carnegie Mellon University. URL: http://petworkshop.org/2006/preproc/preproc_03.pdf, found 07.05.2010.

BBC News (Ed.) (2007): "Robotic age poses ethical dilemma". http://news.bbc.co.uk/2/hi/technology/6425927.stm

Borreson Caruso, Judith; Salaway, Gail. 2008. "The ECAR Study of Undergraduate Students and Information Technology". ECAR. URL: http://net.educause.edu/ir/library/pdf/ers0808/rs/ers0808w.pdf, found 07.05.2010.

Boyd, Danah. 2008a. "Facebook's Privacy Trainwreck. Exposure, Invasion and Social Convergence". Harvard University and University of California-Berkeley. (Convergence: The International Jurnal of Research into New Media Technologies, Vol 14(1). URL: http://www.danah.org/papers/Facebookprivacytrainwreck.pdf,found 07.05.2010.

Boyd, Danah. 2008b. Taken Out of Context. American Teen Sociality in Networked Publics. University of California. URL: http://www.danah.org/papers/TakenOutOfContext.pdf, found 07.05.2010.

Brüggen, Niels. 2009. "Auf den Online-Spuren von Jugendlichen und ihren Vorstellungen von Privatsphäre". In: (K)ein Ende der Privatheit. Strategien zur Sensibilisierung junger Menschen beim Umgang mit persönlichen Daten im Internet. Berlin: RabenStück Verl., p. 117–126.

Calo, M. R., "Robots and Privacy," *in Robot Ethics: The Ethical and Social Implications of Robotics* (P. Lin, G. Bekey, and K. Abney, eds., Cambridge: MIT Press, forthcoming) Downloadable at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1599189

Cho, Hichang; Rivera-Sanchez, Milagros; Sun Sun Lim. 2009. «A multinational study on online privacy. global concerns and local responses». In: new media & society, 11, 3, p. 395–416. URL: http://nms.sagepub.com/content/11/3/395, found 07.07.2010.

Cooley, Thomas M., COOLEY ON TORTS 29 (2d ed. 1888), quoted in http://cyber.law.harvard.edu/privacy/Gormley--100%20Years%20of%20Privacy--%20EXCERPTS.htm

DeCew, and Judith. "Privacy." http://plato.stanford.edu/entries/privacy/ (March 07, 2011).

deCharms, R. Christopher, "Applications of real-time fMRI", Nature Reviews, Neuroscience, Vol. 9, September 2008, p.721

Dwyer, Catherine; Hiltz, Starr Roxanne. 2008. "Designing Privacy Into Online Communities". (Proceedings of Internet Research 9.0). URL: http://csis.pace.edu/~dwyer/research/DwyerAOIR2008.pdf , found 07.05.2010.

Feynman, R., A paraphrase of the famous lecture "Plenty of Room at the Bottom" given by in 1959, which is considered as a milestone in visionary nanotechnology.

Fuchs, Christian (2009): Social networking sites and the surveillance society. a critical case study of the usage of studiVZ, Facebook, and MySpace by students in Salzburg in the context of electronic surveillance. Salzburg, Vienna: Forschungsgruppe "Unified Theory of Information" - Verein zur Förderung der Integration der Informationswiss. (ICT&S Center (University of Salzburg) research report), p. 136 Bl. URL: http://fuchs.icts.sbg.ac.at/SNS_Surveillance_Fuchs.pdf, found 07.05.2010.

Hoofnagle, Chris; King, Jennifer; Li, Su; Turow, Joseph. 2010. "How different are young adults from older adults when it comes to information privacy attitudes & policies". URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864#, found 25.05.2010.

Klasnja, Predrag; Consolvo, Sunny; Choudhury, Tanzeem; Beckwith, Richard; Hightower, Jeffrey (2009): Exploring Privacy Concerns about Personal Sensing. URL: http://dub.washington.edu/djangosite/media/papers/Klasnja_et_al_2009_-_Exploring_privacy_concerns_about_personal_sensing.pdf, found 07.07.2010.

Kleve, Pieter, and Richard de Mulder. 2008. "Privacy protection and the right to information. In search of a new balance." Computer Law & Security Report 24 (3):223–32. http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VB3-4S39MRT-2&_user=10&_coverDate=12%2F31%2F2008&_rdoc=1&_fmt=high&_orig=gateway&_origin=gateway&_sort=d&_docanchor=&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=b84559eb3dfa0a48b860056bd176fc24&searchtype=a (Accessed March 07, 2011).

Lenhart, Amanda; Madden, Mary. 2007. "Teens, Privacy & Online Social Networks. How teens manage their online identities and personal information in the age of MySpace". Pew Internet & American Life Project. URL: http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Society_and_the_Internet/PIP_Teens_Privacy_SNS_Report_Final.pdf, found 07.05.2010.

Lewis, Kevin; Kaufman, Jason; Christakis, Nicholas. 2008. "The Taste for Privacy". An Analysis of College Student Privacy Settings in an Online Social Network. (Journal of Computer-Mediated Communication, 14). URL: http://www.wjh.harvard.edu/~kmlewis/privacy.pdf, found 07.05.2010.

Madden, Mary; Smith, Aaron. 2010. "Reputation Management and Social Media. How people monitor their identity and search for other online". Pew research Center's Internet & American Life Project. URL: http://pewinternet.org/Report/2010/reputation-Management.aspx,found 09.06.2010.

NISTEP, Science and Technology Foresight Survey, Delphi Analysis, NISTEP Report No.97. www.nistep.go.jp/achiev/ftx/eng/rep097e/idx097e.html

Ofcom (Ed.). 2008. "Social Networking". A quantitative and qualitative research report into attitudes, behaviours and use. URL: http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf, found: 07.05.2010.

Prensky, Marc. 2001. "Digital Natives, Digital Immigrants." (On the Horizon, 5), URL http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf (May 10, 2010).

Robinson, Neil; Potoglou, Dimitris; Kim, Choo Woo; Burge, Peter; Warnes, Richard (2010): Security, At What Cost. Quantifying people's trade-offs across liberty, privacy and security. RAND Europe. URL: http://www.rand.org/pubs/technical_reports/2010/RAND_TR664.pdf, found: 07.05.2010.

Robinson, Neil; Potoglou, Dimitris; Kim, Choo Woo; Burge, Peter; Warnes, Richard. 2010. "Security, At What Cost". Quantifying people's trade-offs across liberty, privacy and security. RAND Europe. URL: http://www.rand.org/pubs/technical_reports/2010/RAND_TR664.pdf, found: 07.05.2010.

Rubel, A., "Nanotechnology, Sensors, and Rights to Privacy", Public Affairs Quarterly, Volume 24, Number 2, April 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1661971

Rust, Roland; Kannan, P; Peng, Na (2002): The customer economics of internet privacy. In: Journal of the Academy of Marketing Science, 30-4, p 455-465. URL:

http://comm.psu.edu/about/centers/don-davis-program-in-ethical-leadership/09customer.pdf,found:10.5.2010.

Toumey, C. "Plenty of eyes at the bottom", Nature Nanotechnology, VOL 2, April 2007, p.192-193, www.nature.com/nnano/journal/v2/n4/full/nnano.2007.93.html

United Nations. "The Universal Declaration of Human Rights." http://www.un.org/en/documents/udhr/index.shtml#a12 (March 07, 2011).

Tufekci, Zeynep. 2008. "Can You See Me Now. Audience and Disclosure Regulation in Online Social Network Sites". University of Maryland. (Bulletin of Science, Technology & Society, Vol. 28, No. 1). URL: http://userpages.umbc.edu/~zeynep/papers/ZeynepCanYouSeeMeNowBSTS.pdf, found: 10.05.2010.

Wagner, Ulrike; Brüggen, Niels; Gebel, Christa. 2009. "Web 2.0 als Rahmen für Selbstdarstellung und Vernetzung Jugendlicher". Analyse jugendnaher Plattformen und ausgewählter Selbstdarstellungen von 14-20 Jährigen. Unter Mitarbeit von Peter Gerlicher und Kristin Vogel. JFF - Institut für Medienpädagogik in Forschung und Praxis. URL: http://www.jff.de/dateien/Bericht_Web_2.0_Selbstdarstellungen_JFF_2009.pdf, found: 07.05.2010.

Warren, Samuel D., and Louis D. Brandeis. 1890. "The Right to Privacy." Harvard Law Review Vol. IV (5). See also http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Westin, Alan F. 1970. "Privacy and freedom". London: Bodley Head.

CHAPTER 9
Telecare and Older People: Re-ordering social relations

Maggie Mort, Celia Roberts
and Christine Milligan

Introduction

In policy and technical discourses, telecare systems are described as 'solutions' to what is then defined as the 'problem' of demographic ageing. This paper draws on results from EFORTT (Ethical Frameworks for Telecare Technologies) an FP7 Science in Society project on telecare in Europe. Specifically below we draw from our detailed ethnographic study of the implementation of telecare in Northshire, England. We ask how the promotion and implementation of telecare shapes understandings of what care means for frail older people living at home. We suggest that telecare discourses attempt to divide care work into three distinct domains of practice: monitoring; physical care; and social-emotional care. Telecare, in this logic, deals only with monitoring and leaves the other elements untouched. This tripartite division of care, we argue, both diminishes the kinds of care (potentially) offered in telecare and fails to account for the complexities of all kinds of care (physical, social-emotional and telecare). Telecare introduction is thus infused with ethical issues, we suggest that if it is to make a positive contribution to the lives of older people and those who care for and about them, then it must be carefully and inclusively designed and integrated into wider policy.

The free newspaper posted to all residents' homes within a county in England that we call 'Northshire', carried as its lead story a report about older people and telecare.

> "GOING into a care home and losing your independence is the greatest fear for people's old age, according to new research by the county council. But there is another way..." (Northshire County Council, 2007: 1).

Referring to a survey of 1,700 residents, the headline tells us: 'High-tech home scheme provides solution: support and peace of mind'. The article describes moving into a nursing home or residential care as a fearful spectre, equating this move with 'losing your independence'. Being able to live independently is apparently synonymous with 'staying in their own home' for the sample of older people (over 65 years old) questioned.

The survey results were released as part of the launch of the council's 'Telecare Service'. This service provides 'extra support at home' for older people who have become 'vulnerable', for example after falling over or after discharge from hospital:

> Using high tech gadgets, the service can detect if a person has fallen and needs assistance, whether taps have been left on unattended, if the gas has been left on or if there is a build up of carbon monoxide, if the house is too cold and can also assist residents in reminding them to take their medicine... (Northshire County Council, 2007:1).

In this article, we critically analyse the portrayal of telecare[1] as a solution to the difficulties experienced by older people living at home in particular for preventing their loss of

1 Telecare here refers to a system where alarm devices/detectors are installed around the home, connected to a central hub which transmits information and sound to a monitoring centre. In Northshire, telecare is defined as the hub plus a minimum of two from a range of devices: pendant alarm, smoke detector, fall detector, gas detector, flood detector, bed sensor, medication dispenser, door sensor, refrigerator monitor etc. Following the activation of an alarm, the older person would be telephoned and if a positive response was not obtained, a carer either from the older person's family/friends or from the local authority service would be called to respond in person. We are not here concerned with telemedicine, which enables health professionals to collecting data about the person's health status, vital signs or to carry out treatment at a distance e.g. as in telesurgery.

'independence'. Drawing on our ethnographic study of telecare systems in Northshire and informed by the findings of the larger FP7 project of which this is one part (EFORTT) [2], we begin to see how a mismatch can occur between the promise of telecare and its material realisations. We argue that corporate and policy documents discursively separate the care of older people into three categories, one of which – monitoring – can be effectively achieved by telecare systems. The other two categories – personal physical care and social/emotional care – are only reductively represented in these discourses. Using insights from health geography, disability studies and feminist studies, we suggest that this discursive tripartite division of care (which telecare providers try – unsuccessfully in our view – to realise materially in order to meet specific government targets) both seriously misrepresents the complexities of care, and runs the risk of materially reinforcing oppressive labour relations in the care field.

Background

That populations in Western societies are growing older is routinely figured in European and national policy documents and research reports in terms of an impending crisis for health and social care services. In descriptions of this 'coming global wave of elderly people', apocalyptic forecasts are common:

> ...governments and healthcare officials are beginning to recognise that current medical models of elderly care are insufficient to deal with the coming global wave of elderly people. In nearly every country in the world, the percentage of people over the age of 65 will increase dramatically over the next 50 years. The model of care that has frail elders being sent to live in nursing homes will cause the collapse of healthcare due to the sheer number of people it will need to support in this manner (Lundell & Morris, 2005: 1).

Demographics are used to support claims about unsustainable future demand on health services: recent population projections for Europe indicate that the proportion of the population aged over 60 is set to rise from 15.9% in 2005 to 27.6% 2050 (UN World Population Prospects, 2005), and the European Commission has highlighted the projected rise of the 'old old' (those over 80 years of age) where consumption of health services is said to be well above the average (Watson, 1996). The European Commission's Thematic Portal, for example, notes that:

> Europeans are living longer than ever thanks to economic growth and advances in health care. Average life expectancy is now over 80, and by 2020 around 25% of the population will be over 65. Fortunately, the Information Society offers older people the chance to live independently and continue to enjoy a high quality of life. (http://ec.europa.eu/information_society/activities/einclusion/policy/ageing/index_en.htm, accessed 16 Feb 2011)

2 This ethnography is funded by the European Commission in a Framework 7 project entitled 'Ethical Frameworks for Telecare Technologies' (EFORTT), a project that compares telecare systems in the UK, Spain, Norway and The Netherlands. In the UK, our ethnography included observations of Northshire's Telecare Steering Group, two local telecare monitoring centres, telecare installation work, social work practices around needs assessment and telecare referrals, and technology-related, medical and policy-related conferences. In each arena we conducted interviews with key informants, including talking with older people either using or considering telecare systems, both individually and in groups. In each country involved in EFORTT, ethnographic studies are supplemented by citizen's panels which discussed existing and future telecare systems and responded to the findings of our ethnographies.

For policy makers and clinicians, telecare and smart home technologies appear to offer solutions to rising demand by increased monitoring (surveillance), speed of referrals (efficiency), and better informed health management decisions (Dept of Health 1998; Kendall 2001; Audit Commission 2004). The EC's portal continues:

> ICTs can help older people overcome isolation and loneliness, increasing possibilities for keeping in contact with friends and also extending social networks.... Products like smart homes technologies (to control heating, lighting, and even food stocks remotely), electronic alarm systems and tele-health facilities can also help older people live in their own homes, ensuring that they keep their independence for longer. (http://ec.europa.eu/information_society/activities/einclusion/policy/ageing/index_en.htm, accessed 16 Feb 2011)

Telecare technologies and smart home developments, in other words, constitute practical attempts to ameliorate the 'problems' of the ageing population, increasing levels of chronic illness, rising demand for health and social care, shortage of staff and financial strains on health and welfare budgets.

For European governments, then, health and social care service users are seen as a problem in that they are ageing in greater numbers; becoming sick and increasingly demanding. Such groups – at least at first glance – also provide a conveniently large population for new technologies. Without doubt, the most significant population groups targeted by the telecare and smart home industry are frail older people, their carers and care providers (Schmitt 2002; Harmo et al 2005). The EC describes the size of this market and the potential cost savings to 'society':

> Europe's over 65s are estimated to be worth over €300 billion and the smart homes market is expected to triple between 2005 and 2020. New markets such as tele-health could help older people to get out of hospital and back home more quickly, thereby improving the sense of well-being and reducing society's health costs. (http://ec.europa.eu/information_society/activities/einclusion/policy/ageing/index_en.htm, accessed 16 Feb 2011

However while older people are the target group here, many devices and systems seem to be designed to meet the needs of professionals or care managers, either in relation to managing client demand or monitoring older people's movements. Paradoxically, then, older people can be allotted a passive role whilst ostensibly maintaining the autonomy associated with staying in their own homes (Mort et al 2009:14).

In England a key response of the Government to this 'problem' of population aging was to introduce the Preventive Technology Grant (ODPM/DH 2006), an £80 million initiative which aimed to 'kick-start' telecare services for older people living in their own homes. Northshire received £1.7 million as it share of this initiative and was charged with creating 1,800 telecare users in its geographical area over the three years of the grant's operation.

Telecare in Northshire involves a remote alarm system (a pendant alarm worn around the neck or on the wrist which, if pressed, will alert a monitoring centre) plus one or more sensors, which work through a central 'hub'. This hub, which resembles a large, telephone-answering machine, is connected to a 24 hour monitoring centre that receives and stores digital information about the older person's ongoing activities in the house, as

well as relevant details about his or her medical history and current living situation. The installation of telecare into someone's home, then, involves a central location for the hub (usually next to the telephone in a living room or hallway) and sensors placed around the home or on the body of the older person to collect information about household conditions (temperature, presence of smoke, flooding) and the behaviour of residents or others (has the front door been opened? Has someone gotten in or out of bed? Has medication been taken? Has the device-wearer fallen over?). Sensors are set to trigger when 'normal' conditions or behaviour patterns are breached: the lounge room is too cold; the medication box has not been used; the front door has been left ajar for twenty minutes; there is smoke in the kitchen, or flooding in the bathroom. (Not everyone gets the 'full package' of devices, but a selection is made for individuals.) A triggered alarm produces an automated call through the hub which connects the older person to an operator at a monitoring centre. The operator introduces him/herself, informs the older person which alarm has been triggered, and asks if there is a problem. If the older person fails to answer or needs assistance, a known carer (neighbour or family member) is alerted by telephone and asked to go to the house to check what is going on. In the absence of a suitable person, the service will call on staff from a care agency or as a last resort, the emergency services to perform this check.

The paradox of telecare systems is that they introduce a new sense of scale and a new form of distance into home care work, whilst simultaneously making care appear more immediate. The 'carer'[3] can be located far away and can therefore 'care for' multiple clients, whilst the availability of instant or continuous signs and signals about the client means that care appears proximal and continuous. We are not here arguing that 'home' should be seen (or has ever been seen) as an 'ideal' space, or one in which only face-to-face interactions have value. But home telecare assumes that by bringing together the home and the monitoring centre through a range of devices, some form of 'care' is provided. It assumes that 'care at home' is brought about by means of actions taken in a remote call centre. The connection between the older person at home and 'care', in other words, is enacted through an information system that is figured as 'high-tech' and innovative (and therefore important and beneficial). The benefits of such technical innovation are asserted by the European Commission in statements on e-inclusion. These statements also insist, however, that technologies should be (re)designed so that older people can access them:

> The Commission recognises the power of ICTs to support older people and the community around them....Many older people face barriers in exploiting ICT products, services and applications to their full potential... Ageing is not always considered when designing mainstream products and there can be a distinct lack of industry awareness about older users' capabilities. Even when assistive technologies are developed to help vulnerable groups, a lack of interoperability can hamper uptake. (http://ec.europa.eu/information_society/activities/einclusion/policy/ageing/index_en.htm, accessed 16 Feb 2011)

3 Who is or is not a carer is a complex issue. Most of the older people we spoke with have either been carers in the recent past or are actually still caring for another person. In this way 'care recipients' can also themselves be carers. Again, there are paid carers (such as domiciliary home care assistants) and unpaid carers, such as family members. Sometimes these are termed 'formal' and 'informal' carers respectively, but that in itself does not do justice to the range of tasks being carried out in either case.

Telecare systems, to summarise, foreground technical 'solutions' to the material problems of ageing: forgetting to take medication; not preparing meals; leaving the gas cooker or bathroom taps on; falling down; 'wandering' outside the home at night. This foregrounding, leads to particular kinds of 'solutions', which we suggest may in turn impoverish both the design and implementation of care services for older people. Indeed, as we argue below, this foregrounding ultimately redefines or reshapes what 'care' means.

Less, but more effective, care?

In England, although health care is provided without charge at the point of delivery to all citizens through the National Health Service, social care costs (which, somewhat controversially, encompass the care of older people) are assessed by ability to pay. Most people, then, have to pay something towards the cost of receiving care at home, even those who have relatively low incomes. Care is provided through individually planned 'care packages', which may involve a combination of personal care, help with medication and some basic food preparation, and more recently, telecare. For many people, additional care is provided by family, friends or neighbours: when someone's care needs are seen to be 'too high' for this combination of state and familial care (and if they are unable to buy in more care themselves), they are advised or persuaded to move into a residential care facility. Care packages, then, rely most heavily on the older people themselves: they have to be able to manage their own lives, homes and bodies well enough not to overtax either the state care system or their families and friends.

As discussed above, in the gloomy and panic-inducing descriptions of demographic ageing – announcing 'the coming global wave of older people' – it is frequently implied that existing care systems will not be able to meet the needs of all the older people making demands on them. New forms of care that are more affordable and 'realistic' must be produced, able to triage needs and increase the number of clients any one carer can take on. But what does this mean for care as a practice or form of work? We argue that the telecare systems currently being promoted in the UK (and many similar systems elsewhere in Europe) attempt to divide care work into three distinct activities:

a) Monitoring or checking
b) Physical care
c) Social and emotional care.

These separations, we argue, re-order what counts as care and reduce the complexity of care work, rendering particular elements of it as lacking in meaning or significance, for both carers and those they care for. Each of these divisions produces arbitrary distinctions between kinds of care and types of carers, and discursively over-simplifies care experiences in an attempt to render them 'more cost-effective'. Little attention is paid in policy and commercial telecare discourses, we show, to the effects of such reductive approaches on older people's physical and psychological well-being and actual safety. Emphasis is placed instead on the somewhat falsely reassuring (but highly contemporary) promise of '24-7' availability of 'care'.

The tripartite division of care.

Monitoring or checking

Monitoring is the work that telecare systems attempt to automate, providing a technologised form of safety checking[4] to make sure that the older person is moving about appropriately and not leaving their house in the middle of the night; has not fallen down; has taken (or at least accessed) their medication; has entered the bathroom. Each sensor in the home telecare system collects data about one of these activities: sensors are built into medication dispensers, or attached to the house front door, in the bed, or above the cooker, and send relevant data to the hub which produces an alert if a norm is transgressed. Of course, this kind of monitoring cannot be done by machines in isolation: the point of telecare is that the machines are linked to humans at a distance, humans in monitoring centres or (if alerted), paid domiciliary carers or (unpaid) family carers or friends. Telecare monitoring systems are able to produce 'data' about what is (or is not) happening in an older person's home and relay this to a remote computer, but action still depends on humans.

This kind of work (monitoring at a distance) is poorly paid and is largely undertaken by women in monitoring centres.[5] As a form of care work, it does involve new skills: monitoring centre workers have to be able to decipher information sent by the system and to make appropriate decisions about what kind of intervention to make. As is true for other kinds of call-centre work, this includes developing skills of visualisation (see, in the nursing context, Pettinari and Jessop 2001); dealing with clients' negative emotions (see, for example, Korczynski 2003); and knowing when to adhere to and when to deviate from practice protocols (see, for example, O'Cathain et al 2004). Despite these skill requirements, this part of the 'telecare service' tends to be seen in policy and technical discourses as unproblematic and straightforward. An Audit Commission report for example, describes as highly-desirable the element of 'scalability' in telecare (i.e. the idea that any one carer will be able to care for more people than ever before because such care is 'merely' done on the telephone):

> Scalability
>
> When a telecare alarm is triggered the signal is received at the call-centre. Similarly, when a patient wishes to send monitoring data to a carer it is sent first to the call-centre. At the call-centre an appropriate response is made. Because the call-centre has multiple incoming telephone lines and several operators, it can handle a large number of calls, in other words it can be available to a large number of people at any one time. In this way one provider can provide services to a large number of people. This facility is often referred to as 'service amplification'. ....The telecare service can easily be scaled up to accommodate new users as well as increased functionality (Audit Commission, 2004: 18. Emphasis added).

4 In contemporary discourse, the term 'monitoring' is most often used for automated forms of 'seeing' such a via electronic signals, computerised surveillance, etc; as in the telecare case, it has lost much of its human connotation which survives in terms such as 'watching', 'checking'. For this reason, we use both terms here.

5 Interestingly, in both of the monitoring centres we studied in this project, some operators also work as telecare installers or emergency wardens (who go out to visit older people using the service in an emergency). They thus bring particular sets of knowledge to the monitoring centre encounter which may be missing in other cases (where the operator may not have this experience).

There is no mention here of the demanding kinds of communication skills required by monitoring centre staff: to be able to talk to an older person who has fallen down and is in distress until help arrives; to ascertain if failing to access their medication dispenser means they have had no medication; or deciding if the 'bogus caller' at the front door poses a real risk to the older person.[6]

As a form of care work, the labour of the monitoring centre operator is certainly far removed from more traditional forms of 'hands on' or co-located care. Contact is limited to that which is audible and there is limited time to spend with each client. Operators in the monitoring centres we observed are, working in pairs, responsible for more than 1000 clients, which lessens the opportunity to depart from established protocols of verbal engagement. Although monitoring centre workers do establish meaningful relationships with some clients via the telephone (these tend to be 'high need' clients who call several times a day or week), the lack of face-to-face or hands-on contact is limiting (e.g. is there smoke in the kitchen or is it a false alarm?).[7]

To explore experiences of telecare, we facilitated a series of citizens' panels with older people. One panel involved older people living in a 'sheltered housing' scheme: a block of purpose designed apartments with shared social space and a paid daytime manager. Members of the group all used an alarm system (X-line), involving a series of pull cords in each room of their apartments (and sometimes additionally a pendant worn around the neck) connected to a remote monitoring centre. Most of the group viewed placing sensors around the home as a strong 'intrusion'), however these older people were very happy with the basic alarm system, noting particularly that monitoring centre responders were courteous, friendly and helpful. As is clear in this extract, it took people some time to get used to 'speaking to a box', but once this became familiar, they found it reassuring.

Betty: ...but so far as X-line are concerned I think they're admirable. As long as I've got X-line I'm quite happy.

Kathleen: me too.

Nancy: I think the reassuring thing about X-line is they use your name. They speak to you, 'Hello Mrs Jones'. It's like as though there's a person there.

Betty: I think they must have to look us up on the -

Nancy: Well it must come up on a computer mustn't it?

Ethel: Something like that.

6 'Bogus caller buttons' can be placed at the front door to monitor any suspicious or worrying visit to the house. These silently send a call through to the monitoring centre via the hub. Monitoring centre operators can then listen in to the conversation between the visitor and the older person and monitor the older person's safety.

7 In order to address this problem, some telecare systems use webcams linked to the operator's computer and the older person's television, so the call can include visual contact. Northshire's budget does not run to such technology.

There was a clear sense in this discussion that older people valued the 'personal' relationship established over time with workers at the monitoring centre (who can 'look you up on the computer'), and considered the communication skills of the workers to be central to the provision of quality 'care' at a distance. One user had concerns about future telecare expansion where monitoring centre work could be outsourced globally and where workers' first language would not be English and who might not be so easy to understand and/or relate to.

So the significance of these relationships is, we suggest, notably undervalued in the telecare commissioning literature, with monitoring centre work seen as an unproblematic element of the technical aspects of monitoring (the operator is merely one part of a technical apparatus that includes the sensors, the hub, the phones and the computers at the monitoring centre).

Physical aspects of care

In their exclusive focus on monitoring, telecare systems run in parallel to the physical aspects of care: washing, feeding, dressing and helping people move about their environment. Such aspects of care are well outside the purview of any existing telecare system. While this is sometimes acknowledged by those attempting to implement telecare systems, it is not addressed in government or industry documents. At a local level, a recent talk by Northshire's telecare team at a meeting of care professionals, the leader stated that the municipality's governing principles affirmed the need for human contact and the aim for telecare to supplement, rather than replace, face-to-face care work.

However such statements are rare in the English commissioning literature, and the underpinning logic of telecare, (as was also evident in the European Commission statements quoted above), is at least partially oriented around cost saving. Although physical care is, of course, still seen as necessary for some (it is part of the professionally assessed package of care), there is hope that telecare might reduce 'unnecessary elements' of it. A commonly cited example of this relates to medication provision. Automated pill dispensers attached to telecare hubs can mean that carers do not have to undertake home visits to dispense medication. Automated dispensers, unlike face-to-face carers, cannot ensure that clients actually take their medication: they only 'know' that the container has been turned over at a relevant time (a gesture that would tip the correct pills out). Telecare in this case, then, relies on the client taking the medication once reminded by the box, so is only suitable for some users.

In other cases, telecare can have little impact on an older person's personal care needs: telecare cannot wash bodies, prepare food or clean a house. Indeed, as we describe below, such care tasks have simply been left to one side by technology designers: there are no telecare systems available that undertake these necessary forms of labour. Much research has shown that in the UK and Europe more broadly (with notable national differences), this kind of domestic work remains the responsibility of women, either unpaid or paid. For older people unable to do their own domestic work, this work tends to be done by female relatives or friends or poorly paid workers (for example, through a carer's allowance paid by the state). Importantly, Julia Twigg (2000), amongst others, has demonstrated the emotional and social complexity of this work: physical care is always emotional labour, and has a profound impact on the ways in which the older person experiences their own home as intimate space.

By design, then, telecare runs in parallel to physical care for those who require hands-on assistance. Although telecare providers may promise that telecare systems are not intended to replace hands-on care, members of our citizens' panels expressed concerns about social isolation:

> I think one of the things that's coming out with telecare is the fact that people are feeling isolated and, because they [families and neighbours] think they're safe, they are not going round to see them.

This concern is also evident amongst social workers in Northshire, many of whom appear to be reluctant to include telecare in their clients' care packages, despite their managers' insistence that telecare should be part of care (and therefore something that clients should rightfully be offered).[8] In its portrayal as a cost-saving measure, telecare comes to be equated (or conflated) with diminished care. Whether or not telecare ends up reducing the amount of hands-on care received by particular clients is a complex longitudinal question. However, the way in which telecare discourses simply ignore the question of hands-on care (except to insist that it will not be affected) creates a worrying void for many actors, and fails to recognise the very material limits of the kind of 'care' telecare constitutes.

Social and emotional care

The third framing of care in telecare discourses consists of everything that remains when monitoring/checking and physical care are taken out: the social and emotional side of care (e.g. expressing familial love and respect, taking older parents out for a meal, sitting and chatting about daily life). As we show below, telecare promises to free families from the responsibilities of endless visiting (recalling here that physical care is simply absent in such rhetoric) and to create more opportunity to spend quality time with older family members. Again, the Audit Commission report provides an example of this logic:

> Telecare could relieve carers of some simple, tedious and often intrusive tasks and provide valuable reassurance. Home safety and security packages and medication reminders in particular can supplement their efforts, ease their burden and provide valuable reassurance (Audit Commission, 2004: 36).

In Northshire, a new system has recently been trialled which is designed to help meet the needs of older people with early stage dementia. The system involves a more advanced range of sensors that can detect movement in every room of the house, turning the collected data into a graph which can be emailed to a family carer and monitoring centre daily. Adult children, it is promised, could use this technology to reduce the time they had previously spent checking on parents (this work can be done remotely via the internet). In compensation, they can store up time to spend longer with their parents and to improve the quality of their interactions.

The industry brochure for this technology portrays checking or monitoring work as burdensome and of 'little social value' to the older person. Technology provides carers and older

8 At meetings of the Northshire 'Telecare Steering Group' we have observed, numbers of telecare referrals consistently fail to meet agreed targets, and workers are criticised for not understanding or implementing referral procedures.

people with respite from 'unnecessary visits' and is discursively linked with the promise that that the older person using it will be able to stay in their own home for longer. With new care technologies, then, visits by family carers become purely 'social' and can provide more 'social value' for the older person. The direct promise made by this system is that this will reduce stress for the family carer, allowing them to continue their caring role for longer.

In Northshire, the use of this system is at an early stage, however, it should be emphasised that there is an important difference between frequency of visits and quality of interactions. Vigilance is an inevitable part of caring for an older person with dementia, a part that would be quite difficult to 'switch off' during any particular visit. The family carer would, we suggest, most probably still check the fridge to see if there was adequate food and evidence of eating, and/or check whether mum or dad were wearing appropriate clothing or had been outside for a walk. The number of visits may be reduced, in other words, but it seems unlikely that the implicit promise to remove the complex experience of caring for a person with dementia (so you can simply enjoy a meal together) would be realised.

As in the other categories of care produced in telecare literature, then, the attempt to split off emotional and social care from other (in this case, supposedly more 'mundane' forms) of care is unconvincing. We argue that telecare designers and promoters are producing a fantasy of care in which all the supposedly unpleasant or tedious tasks are done by others (machines or paid workers), leaving only the best of care to be undertaken by families. This claim, we suggest, undervalues the monitoring and checking work undertaken by monitoring centre staff and conveniently 'forgets' those providing physical care (who also do checking and monitoring). Although these claims conjure a landscape of care in which telecare 'makes sense', this is a flattened landscape which would be unrecognisable to most people trying to enact care, either as carers or care-receivers. But what effects do such claims have for how care work itself is understood?

Gendering care work

As we have shown, these systems make no attempt to deal with the physical elements of care, leaving this labour to those who have traditionally undertaken it: women (either low paid or unpaid). Such work, as the European Commission's 'Strategy for Equality between Men and Women' (2010) clarifies, has significant impact on women's ability to participate in other paid work. In response, as others have shown (see, for example, Ehrenreich and Hochshild, 2003; May et al, 2006; Williams 2001), wealthier women in Europe and elsewhere are increasingly employing women from resource-poor regions to do what used to be 'their' domestic labour: Arlie Hochshild (cited in Williams, 2001: 485) calls this 'the global care chain'. Whilst much of this research focuses on childcare, caring for older people is also a significant element in this process. By setting aside physical care, then, telecare 'innovations' leave the ancient history of the gendered division of care labour untouched and make no positive impact on the burgeoning 'transnationalisation' or 'migrantisation' of domestic labour. Indeed, one could argue that the fragmentation of care work described above how care work is understood, actually reinforces and strengthens the gendered, 'racial' (transnational or migrant) and classed divisions of labour. The work of the physical carer is arguably diminished by the removal of parts of her role (the monitoring or checking and social and emotional aspects): the job becomes 'merely' physical care: something that is perceived as functional and therefore fundamentally degraded.

In the extract below, four older women, who are all involved in caring for others or lobbying for greater voice for older people in local decision making, discussed the significance of physical human contact and observation. Giving someone a hug, or observing someone, they argue, 'says so much' and provides rich information about health and well-being:

Elsie: They're trying to do away with human contact...

Brigit: I couldn't agree with you more on the human contact, that's what I said [when describing voluntary work earlier]: I like to hold hands or do that [she pats Elsie's arm] to somebody's arm. .... I think, maybe my generation still wants the hug and the touch. I don't think you will ever, ever... I mean, it's said isn't it: 'You can say so much in a hug'?

Irene: And also what about 'One picture's worth a thousand words?' If they just look at you they can tell very often, far better than talking to you.

Telecare, then, in its attempt to split care tasks, substantially removes the 'social' element of daily monitoring/checking work, leaving older people in the company of sensors which unlike human callers can function 24 hours a day.[9] Sensor-based technologies also produce a non-reciprocal landscape of care: they bring no news of the outside world and little potential for two-way chat or caring; as the women above argue, they constitute a significantly reduced opportunity for meaningful social engagement.

The meaning of care work

So in dividing care work in the context of older people living at home, telecare attempts to produce a rational, cost effective and streamlined system in which:

a) monitoring or checking is reduced to a 'purely technical' procedure that can largely be done by machines, backed up by monitoring centre staff when alerts are triggered;
b) 'physical' care is seen as basic labour and is left in the hands of poorly paid women, often migrants; and
c) 'social and emotional' care is performed by loving, but busy, family members.

In practice, this attempt to reshape care tasks denies several complexities, and discursively (and at least partially materially) works to sustain, and even deepen, a gendered, racial and classed division of care labour. This happens in several ways. In telecare documents, the emotional work of the monitoring centre operators is minimised and rendered invisible. This kind of work is seen as protocol-based, mechanical, and not included in what counts as 'care'. Physical, personal care work, conversely, is denigrated through being separated from checking work. It is no longer seen as an essential part of vigilance and so is positioned as less important than it was previously. Personal care (already poorly regarded and profoundly feminised) is thus further degraded and potentially subject to increased rationing by the state. Finally, the social-emotional care of older people performed by relatives is no longer understood as work. 'Visiting mum'

9 Monitoring centre operators tell us that certain sensors, in particular the falls monitor, are so sensitive to movement that they give rise to large numbers of false alarms.

is simply a social activity – the machines, monitoring centre staff and the poorly paid workers are doing all the labour. [10]

Discussion

Why does this matter? In each of these areas, the meaning of care labour is impoverished; care becomes a set of tasks, rather than of ongoing relations. In arguing for the complexity of homecare and the perspective cast on it by telecare, we draw from a central insight of science and technology studies (STS) which has demonstrated that as we shape technology, so we build society (Bijker, Hughes & Pinch 1992) and that nothing is purely social or purely technical (see for example MacKenzie and Wajcman 1999). Attempts to make such divisions have been heavily critiqued as part of social or political projects (Suchman and Bishop 2000), just as earlier critiques of divisions of labour made visible their conservative outcomes (Rose 1994).

Because it is not clinical, homecare involves lower paid (and unpaid) workers who enjoy less visibility and attention than do doctors or nurses. It also appears to involve technological forms in which interactivity is kept to a minimum: monitoring or surveillance-based systems are not meant to be altered or experimented with. However, the practices which paid and unpaid carers and older people themselves carry out are no less heterogeneous or complex than those in clinical care (and one could argue they are less predictable!). Installing a telecare system does not mean that 'good care' is necessarily going to be any more available or even recognisable.

Telecare seeks to intervene in a landscape that is already fraught with trouble and complexity. Each of the elements of caring for older people at home (monitoring, physical and social-emotional care) we have discussed here rely on long histories of embodied practices which are, in European and other Western cultures, as well as in many other parts of the world, deeply gendered, classed and racialised.

There are assumptions in telecare discourse about the nature of space and place and the character of 'information', which is seen as the basis of telecare's workability. Data collected by sensors and monitors are blind to difference, as they cannot attend to place (locale, location and culture), affect (embodied feeling, identity, relationality), or social differences (such as gender, race and class). Yet people's homes in particular, but also workplaces, are sites made up of these differences and interrelations, rather than empty spaces onto which care systems can be placed unproblematically. In the context of care or medicine at a distance, place is understood to mean something multidimensional, contestable and holding different meanings for different groups and as a site of social relations. Researchers who have listened to the accounts of care recipients for example, illustrate the ways that care policies 'reach far into the intimate spaces of everyday life' (Angus et al, 2005: 169).

10 Our ethnographic work shows that the relationships between monitoring centre staff and carers are, in practice, more complex than this. Monitoring centre staff regularly contact nominated carers (usually family members and/or neighbours) to ask them to physically check on an older person who has triggered an alarm and is either not responding or who requests help. Over months, this can itself become a somewhat personalised relationship.

Applying this thinking to telecare in the European context means challenging the tripartite division of care into areas that consequently appear to 'belong' to different groups. Instead, in the introduction of telecare, the ethical, political, affective and spatial dimensions of care need to be understood, valued and supported. The tripartite division of care performed in telecare promotion, fails to take into account these complex dimensions of care, and in so doing risks reinforcing an oppressive situation in which the labour of particular groups is exploited. Telecare designers and promoters promise that it will reshape care: our concern is that this reshaping will be a hardening of existing problematic relations rather than the kinds of liberatory change figured in industry and government documents.

A Responsible Innovation approach we argue would mean that attention would to be given to the potential of telecare to reorder social relations. Rethinking care itself as relational practice and applying this in the design of care technologies may help to refocus the policy lens and then to imagine substantive change in the lives of older people living at home and those who care for, and about them. Ways to achieve this require inclusive design, ongoing engagement with older people as users of new care technologies and public involvement to assist policy in understanding changing relations and aspirations for care itself. If older people want to stay in their homes rather than move into residential care, societies need to think more creatively about how to provide care that is meaningful, sufficient and dignified.

Acknowledgements

We would like to thank the following members of the EFORTT team for their contribution to our work: Josephine Baxter, Elham Kashefi, Miquel Domenech; Blanca Callen, Daniel Lopez, Tomas Sanchez Criado, Ingunn Moser, Hilde Thygesen, Jeannette Pols and Dick Willems.

References

Angus, J., Kontos, P., Dyck, I., McKeever, P. and Poland, B. (2005) 'The personal significance of the home: habitus and the experience of received long term-home care', *Sociology of Health & Illness* 27(2): 161-187

Audit Commission (2004) *Implementing Telecare*, London

Bijker W, Hughes T and Pinch T eds. (1992), *Shaping Technology/Building Society: Studies in Sociotechnical Change* Camb, Mass, MIT Press

Department of Health (1998) Information for Health: An information strategy for the modern NHS 1998 – 2005, *London*

Department of Health (2005) *Building Telecare in England*, London.

Ehrenreich, B. and Hochschild, A.R. (eds). (2003) *Global Woman: Nannies, maids and sex workers in the new economy*. Granta Books: London

European Commission (2010) *Communication from the Commission: Strategy for equality between women and men* (2010-2015), European Commission, 21 September

European Commission (2010) eInclusion: Ageing Well Action Plan, http://ec.europa.eu/information_society/activities/einclusion/policy/ageing/index_en.htm (Acessed 16 Feb 2010)

Harmo, P., Knuuttila, J., Taipalus, T., Vallet, J. and Halme, A. (2005) *Automation and Telematics for Assisting People Living at Home*, Helsinki (IFAC): Automation Technology Laboratory, Helsinki University of Technology.

Kendall, L. (2001) *The Future Patient*. London: Institute of Public Policy Research

Korczynski, M. (2003) 'Communities of coping: collective emotional labour in service work', *Organization* 10(1): 55-79

Lehoux P. (2006) *The Problem of Health Technology: policy implications for modern health care systems*, New York, Routledge

Lundell J. and Morris M. (2005) 'Tales, tours, tools, and troupes: A tiered research method to inform ubiquitous designs for the elderly' *People and Computers XVIII – Design for Life,* 165-177, BCS Conference Series

MacKenzie D & Wajcman J (1999) 'Introduction' in *The Social Shaping of Technology*, Maidenhead, Open University Press

May, J. et al (2006) 'Keeping London working: Global cities, the British state and London's new migrant division of labour', *Transactions of the Institute of British Geographers* 32(2): 151-167

Mort M., Finch T & May, C. (2009) 'Making and Unmaking Telepatients: identity and governance in new health technologies', *Science, Technology & Human Values,* Vol 34, 1 , 9-33.

NHS Confederation (2006) 'Briefing: Telecare and Telecaring', Issue 13, London Dept of Health & Care Services Improvement Partnership

Northshire County Council (2007) *Vision*, Sept: 1

Northshire County Council (2008) 'Telecare, *The Northshire Way'* presentation to the Care Services Improvement Partnership Network, Manchester, February 2008

Office of the Deputy Prime Minister/Dept of Health Local Authority Circular, (2006) Preventive Technology Grant, LAC March 2006: 5

O'Cathain, A. et al (2004) 'Nurses' views of using computerised decision-support software in NHS Direct', *Journal of Advanced Nursing* 45(3): 280-286

Pettinari, C. J. and Jessop, L. (2001) '"Your ears become your eyes": Managing the absence of visibility in NHS Direct', *Journal of Advanced Nursing* 36(5):668-675

United Nations (2005) UN World Population Prospects Online, http://esa.un.org/unpp/p2kodata.asp

Rose, H. (1999) *Love, Power & Knowledge*, Cambridge: Polity Press.

Schmitt J. M. (2002) 'Innovative medical technologies help ensure improved patient care and cost-effectiveness', *International Journal of Medical Marketing,* 2(2):174-178

Suchman, L. and Bishop, L. (2000) 'Problematising Innovation as a Critical Project', *Technology Analysis & Strategic Management*, 12(3): 327-333

Twigg, J. (2000) *Bathing- the body and community care*. London: Routledge

Watson, R. (1996) 'Europe's Aging Population', *British Medical Journal,* June 8, 312 (7044): 1442.

Williams, F. (2001) 'In and beyond New Labour: Towards a new political ethics of care', *Critical Social Policy* 21: 467-493

ANNEX I:
Policy Brief on:
Whole Body – Imaging at airport checkpoints: the ethical and policy context

February 2010 (updated March 2011)

Author: Emilio Mordini,
email: emilio.mordini@cssc.eu

Centre for Science, Society
and Citizenship (CSSC)

http://www.cssc.eu

HIDE & RISE Partnership

- Centre for Science, Society and Citizenship (Italy) – Coordinator HIDE & RISE
- Aristotle University of Thessaloniki (Greece) RISE
- Centre for Policy on Emerging Technologies (United States) RISE
- Data Security Council of India (India) RISE
- European Biometric Forum (Ireland) RISE
- Eutelis (Italy) HIDE
- Fraunhofer Institute (Germany) HIDE
- Global Security Intelligence (United States) RISE
- International Biometrics Group (United States) HIDE
- Lancaster University (United Kingdom) HIDE & RISE
- National Cheng Chi University (Taiwan) RISE
- National University of Singapore (Singapore) HIDE
- Optel (Poland) HIDE
- Sagem Sécurité (France) HIDE
- The Hasting Center (Unite States) HIDE
- The Hong Kong Polytechnic University (Republic of China) RISE
- University of Ljubljana (Slovenia) HIDE
- University of Tartu (Estonia) RISE
- Zuyd University(The Netherlands) HIDE

Executive Summary

Conclusions

WE BELIEVE that the primary aim of security is to safeguard the human person in his or her physical, mental, and social integrity. Respect for human dignity, body integrity and privacy (both physical and informational) are thus essential components of any security policy. Security measures which impair human integrity of those which should be protected are self-contradictory and eventually are also less effective. The primary purpose of WBI technology and systems is only to detect prohibited items concealed on the body. We think that WBI is legitimate as far as it fulfils its original purpose. Any different goal, like people identification or profiling, or detection of anatomic and/or medical details, is not legitimate and is not respectful of personal integrity.

WE ARE CONCERNED that body scanners could humiliate people by unravelling anatomic and/or medical details, and by hurting their feelings of modesty. We are concerned by the lack of clarity about WBI operating procedures, and by confusion and inconsistencies about primary and secondary screenings, voluntariness and compulsion. We are also concerned that body scanners can be used to discriminate against certain groups of travellers. Moreover, we are concerned that WBI technologies and systems can be (mis)used for wider purposes than the detection of concealed objects.

WE REGARD the European Charter of Fundamental Rights as the general framework for the introduction in the EU of new technologies for passenger screening and aviation security.

WE RECOMMEND that respect for the primacy of the human person and attention to his or her needs are the leading principles followed in the establishment of aviation security. We also recommend that the European Commission should propose a specific framework for detection, profiling, and identification technologies for aviation security. We recommend that WBI operating procedures should be subject to a public, democratic scrutiny. Appropriate exemptions can be provided only for those parts of SOP manuals which directly deal with technically sensitive details. We finally recommend that the European Commission should encourage the use of codes of practice and ethical codes at MS level, and promote the establishment of a system of complaints and remedies at EU level.

WE WELCOME the regular use of privacy enhancing and "privacy-by-design" technologies in WBI system design. We also recommend that technologies should be selected and systems should be designed in order to make it practically impossible to fulfil illegitimate purposes. We recommend that the European Commission, in conjunction with the European Data Protection Supervisor and the Art.29 Working Party, promote independent, publicly available, Privacy Impact Assessments (PIAs) prior to the adoption of any new WBI technology and system.

WE URGE the European Commission to commit to a plan of action to promote further research on ethical, legal, and social implications (ELSI) of technologies for aviation security, their likely effect on public trust and their communicational and symbolic dimensions. In particular we recommend that the European Commission and the European Parliament promote the adoption of an ethical framework for trials with new WBI technologies.

Messages to European policy makers

1. Practices which concern the body are unavoidably invested with cultural values, and in their turn produce new values. **WBI impact assessment should consider the symbolic dimension**, which is often more relevant to policy setting than conventional technology assessment.

2. In order to make WBI technology consistent with respect for human dignity, integrity and physical privacy **WBI should not show the "naked" body but merely the objects the person is holding**. This general tenet implies two converging strategies. First the officer viewing the image should not see the scanned person. The use of modesty filters is also advisable. Second, WBI systems should be selected according to their capacity to detect prohibited items without providing anatomic and medical details. In any case the adoption of WBI technology for routine screening is ethically tenable only if its effectiveness and proportionality are convincingly demonstrated.

3. Assuming all other conditions equal, **there is no reason to adopt X-ray backscatters**, which expose the subject to an additional – although negligible – source of ionizing

radiations. Other WBI technologies should be preferred for standard use.[1] The use of X-ray transmission systems for selected checks (i.e., explosives hidden inside the body) should be avoided and alternative technologies using non-ionizing radiations should be investigated.

4. **All forms of modesty deserve to be fully respected**– no matter how far they are from the western ethos. Some people could perceive WBI screening as an humiliating experience. Their objections should always be taken into account. No one should ever be obliged to undergo any security measure that he feels humiliating and degrading. In particular no one should be offered the option to accept such a measure in exchange for a benefit. This would make it still more humiliating.

5. **Emerging WBI technologies should be addressed as soon as possible**. In this field technology evolves very rapidly and once the use of WBI systems becomes standard in airports, there is a concrete risk that more advanced and privacy intrusive systems would then be introduced, and that they could also be used for more mundane applications.

6. **Privacy Enhancing Technologies (PETs) can alleviate privacy concern only if PETs cannot be "switched-off"**. The "privacy-by-design" approach is the right approach. In addition, given the highly sensitive policy area, it would be advisable to introduce an independent and legally binding control that PETs are properly implemented. In terms of communication with the public, it is paramount that any privacy complaint – although unrealistic – is seriously considered and overtly discussed.

7. Although images are not retained, there is no doubt that **WBI systems are generating data**. Reaching an international consensus about whether these data are personal and to what extent they are sensitive is certainly important. Yet it is still more important to find a consensus about 1) what data are actually generated; 2) how they should be protected. WBI systems could be hacked and there is a common interest from both security agencies and privacy advocates to improve body scanner security and to build more and more secure systems.

8. If we want to implement trusted body scanners, we should **define a legal framework** and describe attributes, capabilities, characteristics and qualities which allow users to verify whether the systems are trustworthy. This should be substantiated in appropriate standards and certification procedures. If WBI has to be implemented, **European standards and certifications** must be developed as soon as possible.

---

1 "*The radiation levels used in body scanners is negligible. Accordingly, the threshold that must be overcome to justify the radiation exposure is also extremely small. On the other hand, the operational issues of body scanners are anything but small. Consider the situation of a government agency deciding what passenger screening procedures to implement in their airports. The list of issues is long and difficult: the cost of the hardware, the availability of the floor space, the cost of additional personnel, the inconvenience of removing the shoes and other clothing, the health hazards of touching passengers bodies, delays in passengers travel, passenger compliance, lawsuits, how to resolve false alarms, the consequences of missing a bomb, and on and on. My point is, if a government agency evaluates these many difficult factors and decides that backscatter is the best choice based on operational concerns, the threshold to justify the radiation usage will always be overcome. On one hand there is a minuscule threshold to be met, and on the other hand there are massive operational issues in play. The disparity between radiation protection and operational concerns is so large, it is unreasonable to suggest that radiation protection should be a part of the decision.*" (Steven W. Smith, Ph.D., Comments to the HIDE-RISE Policy Paper, letter sent to the author on July 17, 2010)

9. **Reviews of WBI technologies** and the rationale which justifies their use, notably as far as the proportionality principle is concerned, must be carried out on regular basis. Citizens input during the system application phase should also be part of the total review system. Although specific contents of these reviews could be partly restricted, **review results should always be public**.

10. Selective screening procedures are hardly consistent with fundamental rights and should be avoided. We welcome the EDPS and Art.29 WP suggestion that **body scanner screening should be universal**, say, no specific subgroup of travellers should be targeted or exempted on the basis of considerations about nationality, race, ethnicity, religion, gender, and age. Yet we understand that **specific security conditions could oblige the selection of specific categories of people** for body scanner screening. Such a procedure should always be convincingly justified and should be temporary.

Contents

WHOLE BODY IMAGING AT AIRPORT CHECKPOINTS: THE ETHICAL AND POLICY CONTEXT

CHAPTER 1: Introduction

Background

1. One of the main tasks of security checkpoints (e.g., border checkpoints, airport checkpoints, mobile, random, checkpoints) is to screen people for detecting objects and materials, like weapons and explosives. The main methods used for object and material detection rely both on non-technological (e.g., physical observation; hand searches, also including body orifice search; explosive detection dogs) and technological methods (e.g., hand-held metal detectors, HHMD; walk-through metal detectors, WTMD; explosives trace detection, so called "puffer machine"; sensors for the detection of chemical and biological contaminants). Not all these methods are routinely used in all kinds of checkpoints – selection is based on various factors, including portability (e.g., in case of mobile checkpoints), intrusiveness (e.g., in case of large scale applications), risk evaluation (e.g., airports, access to critical infrastructures). In the early 2000s[1] a new class of technological devices was introduced for the detection of objects and materials hidden on the bodies of individuals, the Whole Body Imaging (WBI) devices - also known as *body scanners*, or *Advanced Imaging Technology* (AIT) - where improving security is of paramount importance[2].

2. According to Regulation 2320/2002[3], and then Regulation EC 300/2008, the EC is allowed[4] to adopt measures designed to amend non-essential elements of common basic standards on aviation security. These measures include inter alia "methods of screening, individually or in combination, as a primary or secondary means and under defined conditions"[5]. Draft Regulation 300/2008 included WBI systems amongst allowed European airport screening technologies. Following the EP Committee on

1 The first backscatter X-ray security screening system (The Secure 1000) was developed in 1992 by Steve Smith and commercialized by RAPISCAN, http://www.dspguide.com/secure.htm

2 Ironically enough, in 2005 the European Parliament bought six WBI scanners "following a security-risk analysis and on the advice of an outside consultant" (C6-0416/2008 – 2008/2276(DEC), EP Committee on Budgetary Control) that were never used but could have been installed in the event of a serious terrorist alert. Three of them were delivered to the parliament's seat in Strasbourg, the other three to the Brussels Chamber. Following the EP Resolution banning WBI technology, the Committee on Budgetary Control asked the Secretary-General "to look into the possibility of selling the scanners".

3 Prior to September 11, aviation security in Europe was managed on a national basis, and no EU common policy existed until 2002.

4 Article 4(3) of Regulation 300/2008

5 Ibid.

Transport and Tourism's request for more details[6], the EU Commissioner for Transport, Mr Antonio Tajani, clarified that body scanners were to be considered "only as an additional option for the screening of passengers, not as an obligation", and agreed on the need to examine more closely "some aspects such as impact on health and, in particular, the question of passengers privacy"[7].

3. The European Parliament was not completely satisfied and with a Resolution of the 23 October 2008[8] MEPs blocked Regulation 300/2008, and called for a full ethical and legal impact assessment of WBI technologies on the basis that "the measures in question cannot be considered mere technical measures relating to aviation security, but have a serious impact on the fundamental rights of citizens". MEPs asked the Commission to "carry out a fundamental human rights impact assessment", and to "consult the EDPS, the Article 29 Working Party and the FRA". The EP also asked the competent authorities to carry out medical and economical assessments, in order to provide a clearer picture on the possible impact on health, and a costs/benefits analysis. Further to the EP resolution, the Commission carried out a comprehensive public consultation (also including Art.29 WP, the EDPS the FRA)[9]. In addition to a questionnaire, the Commission also launched a 'public-private dialogue' that took the form of a "Body Scanners Task Force", which in December 2008 convened a workshop to exchange information. Eventually the EC decided to skip mentioning WBI in the final version of Regulation 300/2008, and to postpone any decision about WBI until its privacy and health impacts were fully assessed.

4. After the failed 2009 Christmas day attack on a flight from Amsterdam to Detroit[10], WBI systems again became a priority on the political agenda. Although it is arguable that they might have headed off the attack, the fact that explosive was hidden in the would-be terrorist's underwear revived the attention on body scanners at airport checkpoints. In the US, the Transportation Security Administration (TSA) ordered 300 more WBI machines to be added to the 40 scanners being currently used at 19 US airports. The Netherlands announced they would immediately begin using this technology for screening passengers of flights heading to the United States. British Prime Minister Gordon Brown announced that the UK was going to include WBI among airport security measures, and the French government did the same. The Italian government also decided to install WBIs at three airports, in Rome, Milan and Venice. Yet other EU Member States (MSs) such as Finland, Spain and Germany, remained uncommitted and expressed scepticism about the need for this technology.

6 TRAN/D/2008/57605, 26.09.2008

7 Mr A. Tajani Letter to Mr. P. Costa, 7.10.2008

8 European Parliament, Resolution on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection, RSP/2008/2651

9 http://ec.europa.eu/transport/air/consultations/2009_02_19_body_scanners_en.htm

10 On Christmas Eve, December 24, 2009, a 23-year-old Nigerian, attempted to set off plastic explosives concealed in his underwear as the plane in which he was travelling was on its final descent. The plane made an emergency landing in Detroit without any fatalities. At the Amsterdam airport, the Nigerian guy was subjected to the same screening as other passengers—he passed through a metal detector, which didn't detect the explosives that were sewn into his clothes. see http://en.wikipedia.org/wiki/Northwest_Airlines_Flight_253

5. On Jan 21, 2010, the Spanish Presidency of the European Union convened in Toledo an informal meeting of Ministers of Justice and Home Affairs of the EU (JHA), jointly with the United States Secretary of Homeland Security, Janet Napolitano, to discuss boosting airport security. At the end of the meeting the Ministers agreed with Ms Napolitano that aviation security priorities include 1) *To identify individuals who pose a risk to our security as early as possible by bolstering the security of and our confidence in travel documents, the use of biometrics, and passenger screening*, and 2) *To identify the illicit materials that such people may be carrying, sending via cargo, or transporting, including through enhanced technologies, to prevent the entry of such materials onto aircraft*.[11] Ministers also agreed that decisions about the deployment of WBI in European airports are to be made by general consensus.

6. On Jan 14, 2010, in his hearing before the European Parliament's Transport Committee, Commissioner Siim Kallas backed the idea of a single EU regulation on body scanners and deplored that some MSs already use WBI in the absence of EU common standards. Although "body scanners are not the panacea for airline security" – added Mr Kallas – EU citizens' fear "must be addressed" and he called for common rules to be adopted.[12]

7. In the light of these developments, the HIDE and RISE projects decided to undertake an inquiry into the ethical and policy context of the adoption of WBI technology at airport check-points in Europe. The Coordinator of the two projects, Prof. Emilio Mordini, and the staff at the Centre for Science, Society and Citizenship, took the responsibility to physically write this report. Some of the questions we sought to answer included:

   - What do we know about the likely health and privacy impact of WBI technology?
   - To what extent do WBI for people screening in airports comply with the Charter of Fundamental Rights and respect for privacy?
   - What technical provisions (if any) are necessary to make WBI consistent with ethical and privacy principles?
   - What is the appropriate level of governance for WBI?

8. We acknowledge that many of these questions are far reaching, and that finding answers to them may not be easy. With this policy report, the HIDE and RISE projects aim to contribute to the wider debate on WBI launched by the European Commission, and to convey some messages to European policy makers.

11 EU-US Joint Declaration on Aviation Security, http://www.eu2010.es/en/documentosynoticias/otrasdeclarac/jaieuusa.html

12 EP Hearings , Summary of the hearing of Siim Kallas -Transport

Timeline of main events	
1992	The first X-ray backscatter (The Secure 1000) is developed by Steve Smith
2002	Backscatters are tested in a few US airports for secondary screening
2002	MM-waves machines are tested in UK at Gatwick Airport
2004	Backscatters are tested in UK at Heathrow Airport
2004	US National Council on Radiation Protection and Measurements, *Presidential Report on Radiation Protection Advice: Screening of Humans for Security Purposes Using Ionizing Radiation Scanning Systems*
2006	Final report of the FP5 project "Tera-Hertz radiation in Biological Research, Investigation on Diagnostics and study of potential Genotoxic Effects"
2007	Committee on Assessment of Security Technologies for Transportation of the US National Research Council, *Assessment of Millimeter-Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapons*
2007	MM-waves are tested in NL at Schipol Airport
2007	Backscatters are tested in Finland
2007	The US TSA starts piloting MM-wave technology in 19 US airports
Oct 2008	US Department of Homeland Security, *Privacy Impact Assessment for Whole Body Imaging*
Oct 2008	Draft EC Regulation 300/2008 on aviation security including body scanner as allowed screening method
Oct 2008	EP Resolution of the 23 October 2008 calls for a full ethical and legal impact assessment of WBI prior of their adoption
Dec 2008	The EC launches the public consultation *The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection* and set up a "Body Scanners Task Force"
Feb 2009	MM-wave systems are used in lieu of WTMD in six of the biggest US airports, in order to evaluate the operational efficiency of WBI for primary screening.
Feb 2009	Joint Opinion on body scanner issued by the Art.29 Working Party and the European Data Protection Supervisor
March 2009	Privacy Commissioner of Ontario, *Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy*
March 2009	EC Regulation 300/2008 on aviation security is approved by the EP. The chapter on "methods of screening allowed" is suppressed.
Oct 2009	Canadian Air Transport Security Authority, *Privacy Impact Assessment in anticipation of the deployment of MM-Wave technology at selected Canadian airport*
12 Dec 2009	Failed Christmas day attack
Jan 2010	The US TSA orders 300 WBI machines to be employed in US airports. Some EU MSs declare their will to adopt a similar decision (e.g., UK, NL, FR, IT), while others remain uncommitted (e.g., FL, ES, DE)

Jan 2010	US Government Accountability Office (GAO, *Homeland Security: Better Use of Terrorist Watch list Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security*
14 Jan 2010	Confirmation hearing of Commissioner Siim Kallas, who backs the idea of a single EU regulation on body scanners and deplores that some MSs use WBI in the absence of EU common standards
21 Jan, 2010	EU-US jointly declaration on aviation security stating that "enhanced technologies" will be used to identify the illicit materials that people may be carrying
28 Jan 2010	EC Commissioner responsible for Justice, Fundamental Rights and Citizenship, Viviane Reding, declares that "I cannot imagine this privacy-intrusive technique being imposed on us without full consideration of its impact"
Feb 2010	UK Department for Transport, *Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology*
15 June 2010	EC Communication on the Use of Security Scanners at EU airports (COM(2010) 311 final, Brussels, 15.6.2010)
9 Nov 2010	Committee on the Environment, Public Health and Food Safety, DRAFT OPINION on air safety, with particular reference to body scanners, 9 November 2010
14 Feb 2011	Committee on Civil Liberties, Justice and Home Affairs, DRAFT OPINION on aviation security with a special focus on security scanners (2010/2154(INI)), 14 February 2011
16 Feb 2011	European Economic and Social Committee, TEN/429, Opinion on the Use of Security Scanners at EU airports, Brussels, 16 February 2011
23 Feb 2011	European Parliament Committee on Transport and Tourism, 2010/2154(INI) 23 February 2011, DRAFT REPORT on aviation security, with a special focus on security scanners

CHAPTER 2: The technological context

Technologies and Systems

9. **Whole Body Imaging** is an umbrella term that includes various technologies that can produce images of the body without the cover of clothing. These screening systems increase the threat detection spectrum from weapons and "single threats" to "multi" or "all-threats", including explosives, and even biological and nuclear contaminants. All WBI technologies can detect metallic objects, plastic and ceramic weapons, explosives and other threats hidden beneath the clothes without the need of a pat down or strip search: they can indeed reveal types of material that a conventional WTMD can't detect - such as prohibited non-metallic items, which at present, can be found only through hand searching procedures. Another important asset of a WBI system is that – at least theoretically - it provides a comprehensive body search in just a few seconds.

10. There are two main categories of WBI[1]: "*walk-in" cabinets,* which scan one person at a time; and "*stand-off" scanners,* which are pointed at crowds. In their turn, each category can use different technologies, based on different kinds of electromagnetic waves. The walk-in systems typically use the reflection of the waves off the skin to detect any unusual shapes on the body. They are active systems, say, they project beams on the subject. Stand-off scanners can be either active or passive (passive systems collect waves emitted, or reflected from the environment, by the body). WBI systems include various technologies with different levels of maturity. Technologies at validation and demonstration phases include *ultrasound imagers*, *SQUID* and *quadrupole resonance analyzers*, *T-ray imagers*. More mature technologies include millimetre-wave holographic imagers, and x-ray scanning systems.

11. **Ultrasonic imaging technology** is largely used in medicine to investigate internal organs (for such an application it must work in contact mode). For security purposes ultrasounds are widely used for object detection and motion detection.[2] Ultrasonic detectors for remote detection of concealed weapons have also been commercialized[3]. JAYCOR has recently developed and demonstrated an Ultrasound Imaging Sensor for detecting and imaging weapons concealed under a person's clothing. The sensor includes a source of high-power ultrasounds suitable for remote imaging in air.[4] The producer claims the "sensor can detect metallic and non-metallic weapons concealed on a human body under heavy clothing at ranges up to 8 m and can image concealed weapons at ranges up to 5 m with a centimetre-resolution"[5].

1 www.newscientist.com/article/dn18343-deployment-of-airport-full-body-scanners-could-be-delayed.html

2 NCRP (2004) Presidential Report on Radiation Protection Advice: Screening of Humans for Security Purposes Using Ionizing Radiation Scanning Systems (National Council on Radiation Protection and Measurements, Bethesda, Maryland).

3 Costianes, P.J. (2005) An overview of concealed weapons detection for homeland security, *Applied Imagery and Pattern Recognition Workshop*. Proceedings. 34th, 5- 6

4 Felber FS, and al. (1996), Fusion of radar and ultrasound sensors for concealed weapons detection, in *SPIE Proceedings Vol. 275, Signal Processing, Sensor Fusion, and Target Recognition*, Ivan Kadar; Vibeke Libby, Editors, pp.514-521

5 http://www.jaycor.com/eme_sens_ultra.htm

12. **SQUID**, which stands for *Superconducting Quantum Interference Device*, and **Quadrupole Resonance Analysis**, provide images similar to magnetic resonance imaging. They are currently used chiefly for medical imaging, and are being investigated for the detection of explosives in checked luggage[6]. In principle they could also provide body imaging for security screening purposes, with the advantage of being able to also detect and test different chemicals and substances, including minimal traces of explosives. One potential problem arises from the fact that they can interfere with the function of implanted medical devices (e.g., pacemakers and defibrillators).

13. **T-ray technology**[7] uses electromagnetic radiation from 1,000 GHz to 10,000 GHz, in the so-called tera-band. Terahertz are non-ionizing radiations, thus without the health risks entailed by x-rays. Most T-ray scanners are active systems, say, they emit radiation and detect objects by noting differences in absorption /reflection. Instead a few T-ray scanners, known as passive imagers, rely on the small amount of T-radiation emitted by all warm bodies[8]. They find objects beneath people's clothing by noting the difference in the amount of radiation emitted between the warm body and the cooler objects. T-ray technology can also detect the nature of hidden objects and materials.[9] Many materials have unique spectral profiles in the terahertz range. This offers the possibility to combine spectral identification with imaging. For instance, plastic explosives reflect terahertz waves in a very specific way, that make them distinguishable from all other materials. T-ray passive systems can be consequently used for "stand-off" scanners, which could remotely detect explosives, and weapons, hidden under clothing by an individual in a crowd. Most current T-ray imagers are still short-range (a few metres) and spectroscopy is often too slow for real life applications[10]. Yet technologists predict that T-ray scanners that can do both imaging and spectroscopy at 50 meters or more will be available within five years.

14. **Millimeter Wave (MM-wave) Technology** is based on radiation belonging to the millimetre (from 30 GHz to 300 GHz) and submillimetre (from 300 GHz to 1,000 GHz) regions of the electromagnetic band.[11] Imaging technologies can be either passive or active. **Active MM-wave systems** use non ionizing radio frequency energy to generate an image based on the energy reflected from the body.[12] The waves penetrate clothing but are reflected from the skin and other objects. The three dimensional image resembles

---

6 www.securitymanagement.com/article/new-views-airport-screening-004586?page=0%2C2

7 Costianes, P.J. (2005), ibid.

8 Zandonella C (2003), Terahertz imaging: T-ray specs Nature 424, 721-722 (14 August 2003) | doi:10.1038/424721a

9 Committee on Assessment of Security Technologies for Transportation (2007) *Assessment of Millimeter-Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapon*, National Academies Press

10 *Thruvision Systems* sells scanners (T5000 and T8000) that can be used effectively when the person being screened is between 6 m and 25 m away., yet these devises lack spectroscopy capacities http://www.thruvision.com/index.html

11 Costianes, P.J. (2005), ibid.

12 Committee on Assessment of Security Technologies for Transportation (2007) , ibid.

a photograph negative. **Passive MM-wave systems** are used to scan remotely, overtly or covertly, large numbers of people as they move in a continual stream through restricted or controlled areas, such as border checkpoints, airport terminals, or outdoor arenas[13]. Images are low resolution body images in which clothing and other materials appear transparent. Some passive systems (e.g., a scanner called SPO, produced by the UK company Qinetiq) activate warning messages when they detect any concealed object.[14] MM-wave receivers can also be coupled with infrared receivers. The two receivers used in tandem, and linked with a computer imaging system, would have a higher discriminating power than MM-wave passive system alone.[15]

15. MM-wave technology also includes a technology consisting of arrays of **microwave dielectrometers** in a portal (*People Portal Full Body Scanner*, produced by the US company Global Security Solutions).[16] The system performs and maps a large number of measurements, which are compared to expected values in order to detect extraneous objects. A material's density and absorption abilities are the criteria for making the decision to declare a material 'offensive'. According to the producer, "the computer takes no action as long as the instant information compares favorably with that stored in the computer. The definition of 'favorable' is operator selectable as the systems sensitivity adjustment. If, during the scanning process, the computer detects an unfavorable comparison it red flags the offending location upon a generic wire-frame figure". This would imply that "unlike competing technologies, no picture of an individual's actual anatomy is ever produced, seen or exhibited. The operator sees only a wire-frame image indicating by red arrows the exact location of the anomalies".

16. **X-ray scanning systems** include backscatter systems and transmission systems. **X-ray backscatter systems** use low intensity x-rays scanned over the body surface, and reflected back from the body. Backscatter produces a narrow beam that scans the subject at high speed ("flying spot") left to right and top to bottom. Most of the radiation is scattered near the surface of the skin, this makes the system effective in imaging objects hidden under clothing. The low intensity x rays can hardly penetrate through the skin and cannot detect objects hidden in body cavities. A typical scan lasts about eight seconds, during which a person is scanned twice, once from the front and once from the back. The resulting image is a two dimensional one, similar to a chalk etching.[17]. Backscatter X-ray can be also used for partial body scanner to screen persons with casts, bandages and prosthetic limbs for concealed weapons and contraband[18].

13 Duncan WD et al. (2008), An Optical System for Body Imaging from a Distance Using Near-TeraHertz Frequencies, *Journal of Low Temperature Physics*, 151, 3:777-783 http://www.springerlink.com/content/j3w220228n21v1g5

14 http://www.qinetiq.com/home/aboutqq.html

15 Currie NC, et al. (1996) Infrared and millimeter-wave sensors for military special operations and law enforcement applications, International Journal of Infrared and Millimeter Waves, 17, 7:1117-1138 http://www.springerlink.com/content/t7t70184np215897

16 Appleby R, Wikner DA (2007) Passive Millimeter-Wave Imaging Technology, Proceedings of SPIE Volume: 6548

17 NCRP (2004), ibid.

18 http://www.tek84.com/castscope.html

Backscatter permits rapid inspection without imposing too much stress, and discomfort to the disabled person. **Transmission systems** are closer to medical x-rays, in the sense that the radiation traverses through the body. Transmission systems can detect objects that have been swallowed or hidden in body cavities and have been used to screen workers in diamond mines in order to replace orifice search.[19]

Trials and Standards

17. The first WBI machines using backscatter technology were deployed in 2002[20] in a few US airports. In February 2007, the US TSA decided to test WBI as an "*alternative to personal searches for secondary screening*"[21]. The initial test involved systems based on x-ray backscatter technology, used for passengers selected for additional screening. In October 2007 the TSA started piloting the MM-wave technology in 19 US airports. In February 2009, the TSA started piloting MM-wave systems *in lieu* of WTMD in six of the biggest US airports[22], in order to evaluate the operational efficiency of WBI *for primary screening*[23].

18. In Europe, the technology was first tested in London airports, in Amsterdam's Schiphol and Helsinki's Vantaa. In the UK, MM-waves were tested at Gatwick in 2002 and backscatters at Heathrow on October 2004[24], as part of an initiative of the Department of Transport over a three year period. Passengers sorted out for enhanced inspection had the option of a standard pat-down search or a scan with the WBI technology, and the latter was selected by approximately 90% of passengers. On February 6th 2009, Rapiscan Systems announced that it had received an order from the British Airport Association to purchase the three backscatter machines that were used in the trial[25]. In the Netherlands, at Schiphol Airport a trial with three active MM-wave scanners started in May 2007. Passengers could select between WBI and standard procedures. Most persons, from 85 to 90 %, accepted the scanner, as "*a more client friendly procedure*"[26]. Finally, in Finland, one WBI system has been tested at Helsinki Vantaa Airport "*during the busiest periods in the mornings and evenings since 7 November 2007*"

19 Smit KJ (2003), *Regulatory Control of X-ray Equipment Used in the Mining Industry in South Africa to Screen Workers for Security Purposes*. Proceedings 35th National Conference on Radiation Control, (South Africa Department of Health, Bellville, South Africa), quoted by NCRP (2004), ibid.

20 Masterson U (2010), Airports seek hi-tech security, http://www.msnbc.msn.com/id/3071573

21 See David Biello, "The Naked Truth: is New Passenger Scanner a Terrorist Trap or Virtual Strip Search?", Scientific American, March 1st 2007.

22 San Francisco, Miami, Albuquerque, Tulsa, Salt Lake City and Las Vegas.

23 However passengers could still opt for standard procedures through WTMD and physical inspection, http://www.tsa.gov/press/happenings/mwave_continues.shtm

24 D. Gadher, *Plane Passengers shocked by their x-ray scans*, The Sunday Times, November 7, 2004

25 *See* the Rapiscan release available at http://www.securityinfowatch.com/root+level/1279579

26 Schiphol airport website.

according to a Finavia release[27]. After the failed Christmas day attack, a number of further trials started in Europe (Italy[28], UK[29], Germany[30], and others), in the US, in India, and Japan.

19. To date there is not a common European legal and ethical framework for WBI trials in airports.

20. Millimetre wave scanners are more frequently deployed at airports rather than backscatter systems[31] for two main reasons: they generate non-ionizing radiation and consequently they pose minimal health risks, and they are faster passenger processing machines[32]. According to the US Transportation Security Administration (TSA)[33], WBI speeds up the overall scanning process, as "*it takes a passenger about 15 seconds to undergo the screening, as opposed to the several minute pat down procedure*"[34]. According to a report on trials at Schiphol Airport[35], one of their main weakness was the false alarm rate, which was very high (about 50%), mainly due to objects forgotten in the pockets.

21. WBI also reduces the need of hand searches, making the process less embarrassing and intrusive. However, since both MM-wave and backscatter devices create images showing the surface of the skin and revealing objects that are on the body, and not inside the body, they can't replace body orifice search.

27 Available at http://www.finavia.fi/finavia_release?id=69470 . Finavia is the managing body of 25 airports in Finland.

28 On March 4 2010 the first trial of full-body scanners took place at Fiumicino Airport in Rome, with similar equipment being installed at Milan's Malpensa airport a few days later. Two kinds of body scanner will be tested: backscatter scanners and millimetre wave scanners. Both trials were suspended after a few weeks because the scanner slowed down dramatically the overall passenger screening process.

29 Manchester and Heathrow

30 Hamburg

31 "*Both back-scatter and mm-wave scanners are generally effective; however, they operate on different physical principles and therefore have significantly different characteristics. For instance, most users would agree that backscatter has better image quality and lower false alarms. On the other hand, mmwave is often cited as being more compact and better at detecting a few specific threats. These types of differences lead end-users to select one or the other based on their particular situation. For instance, the U.S. military operates over 300 backscatter units in Iraq and other war areas, with almost no use of the mm-wave systems. Likewise, backscatter systems far outnumber mm-wave units in prisons and similar correctional facilities. In U.S. airports there are currently more backscatter scanners installed than mmwave units. These usage statistics demonstrate that backscatter is better suited for some applications that mmwave, as determined by government officials tasked with protecting the public. And of course, this is the appropriate group to evaluate the efficacy, which is often confidential and not released to the general public.*" (Steven W. Smith, Ph.D., Comments to the HIDE-RISE Policy Paper, letter sent on July 17, 2010)

32 Ontario Information and Privacy Commissioner white paper on "Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy", March 2009

33 A component of the Department of Homeland Security, created by the Aviation and Transportation Security Act (ATSA) two month after the September 11 attacks.

34 See www.tsa.gov

35 See http://www.homelandsecurityresearch.net/2009/04/27/schiphol-airport-security-new-screening-technologies-designed-to-improve-passenger-and-luggage-screening

Needs addressed by WBI

22. According to the European Economical and Social Committee (EESC) opinion on *Aviation security for passengers*[36], adopted at its 448th plenary session, "*considering the significant increase of passengers travelling by air forecast for the upcoming years, the current security screening of passengers and luggage does not propose a sustainable model*" (art. 6.1). Improving aviation security, notably the detection of prohibited items, while softening the "burdensome process"[37] of people screening is a worldwide priority in airport management.

23. Today passengers who have to undergo to full-body pat down belong to two broad categories: 1) they are passengers holding passports from countries included in a (unofficial) list for enhanced screening, or taking flights that originated or passed through any of these countries; or 2) they have set off the metal detector alarm. As more people have surgical implants (e.g., hip replacements, prosthetics, cardiac implants, etc) and more people are travelling from and through "risky" countries, the number of people who need to undergo to physical search is increasing.

24. Hand searches are time-consuming (they take from two to four minutes) and labour-intensive procedures. They are also only partly effective. In order to perform appropriate pat down search, screeners must avoid touching sensitive areas (e.g., genitalia, breast, etc.) with anything except for the back of the hand and any excessive squeezing or groping of sensitive areas. They must also avoid requiring a passenger to expose private areas of the body, and there is indeed evidence that physical pat-down is not effective in locating items concealed in sensitive body areas[38]. As a consequence – although no systematic studies are available – it is realistic to argue that pat downs can be unreliable.

25. There is also anecdotal evidence that passengers feel pat-down procedures embarrassing and invasive because they involve screeners touching people near sensitive body areas. In particular female travellers have been complaining about pat-downs. Although very specific guidelines and boundaries have been established by national airport authorities, inappropriate pat-down searches are still episodically reported.

36 OJ C 100, 30.04.2009, "Opinion of the European Economic and Social Committee (EESC) on *Aviation Security for Passengers*", p.41.

37 Ibid.

38 United States Government Accountability Office, *Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process*, http://www.tsa.gov/assets/pdf/gao_report.pdf

CHAPTER 3: Health and privacy impact assessment

26. Further to the EP Resolution of 23 October 2008, the EC public consultation on body scanners (January-March 2009) and the EU-US Joint Declaration on Aviation Security of Toledo (Jan 21, 2010), the EC Commissioner responsible for Justice, Fundamental Rights and Citizenship, Ms Viviane Reding, declared before the Parliament (keynote speech at the Data Protection Day on 28 January 2010) that "body scanners have a considerable privacy-invasive potential. Their usefulness is still to be proven. Their impact on health has not yet been fully assessed. Therefore I cannot imagine this privacy-intrusive technique being imposed on us without full consideration of its impact".[1] Earlier, during the parliamentary confirmation hearing, Ms Reding had also told that scans must be voluntary, not mandatory, and authorities should guarantee that these systems pose no health hazard and their images must be quickly destroyed.[2]

27. As per x-ray scanning systems, the reference document is the ***1990 Recommendations of the International Commission on Radiological Protection***, issued by the *International Commission on Radiological Protection* (ICRP) in 1991[3], which states that "In radiation protection, no exposure is *justified* unless it produces a positive net benefit". This philosophy "is part of radiation protection regulations of all agencies in the United States and the European Union and is almost universally adopted throughout the world. In the case of screening passengers, visitors, or prisoners, the benefit is increased security and the possibility of preventing terrorist attacks".[4] One of the first comprehensive reports assessing health impact of x-ray scanning systems was the ***Presidential Report on Radiation Protection Advice: Screening of Humans for Security Purposes Using Ionizing Radiation Scanning Systems*** published in 2004 by the *US National Council on Radiation Protection and Measurements*[5]. The report recommends that scanning systems that utilize ionizing radiation are classified into two broad categories: *general use systems* (e.g., backscatter systems) and *limited-use systems* (e.g., transmission systems). "*General-use systems* should adhere to an effective dose of 0.1 mSv or less per scan, and can be used mostly without regard to the number of individuals scanned or the number of scans per individual in a year [...] *Limited-use systems* include all other ionizing radiation scanning systems that require effective doses per scan greater than 0.1 mSv and less than or equal to 10 mSv. These systems should be used with discretion in terms of the number of individuals scanned and the number of scans per individual in a year".

28. Although a recent study[6] indicates that tera radiations could lead to DNA instability, to date there is no evidence that they could damage biological tissues, on the contrary other

1 http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/16&format=HTML&aged=0&language=EN&guiLanguage=en

2 EP Hearings, Summary of hearing of Viviane Reding - Justice, fundamental rights and citizenship

3 ICRP Publication No. 60, 1991, Annals of the ICRP 21(1-3).

4 Health Physics Society (2205) *Screening Individuals with Backscatter X-Ray Systems* http://www.hps.org/hpssc/N43Status.html

5 http://www.ncrppublications.org/

6 Alexandrov B. S., et al. (2010), DNA Breathing Dynamics in the Presence of a Terahertz Field. *Physics Letters A*, 374, 10: http://arxiv.org/abs/0910.5294

evidences show that they cannot. The reference study is the final report of ***THz-BRIDGE*** *- Tera-Hertz radiation in Biological Research, Investigation on Diagnostics and study of potential Genotoxic Effects*, [7]a project funded in the scope of the EC FP5 Quality of Life. Aim of THz-BRIDGE was to investigate the potential damage of electromagnetic radiation on biological systems in the millimetre, submillimetre, and tera spectral ranges. After three years research, the project established the safety of millimeter-wavelength/ terahertz energy. On the basis of *THz- BRIDGE*, in 2007, the *Committee on Assessment of Security Technologies for Transportation of the US National Research Council* published the report ***Assessment of Millimeter-Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapons***,[8] which addresses MM-wave and T-ray scanning systems. The report concludes that "Millimeter-wavelength/terahertz technology has potential for contributing to overall aviation security, but its limitations need to be recognized. It will be most effective when used in conjunction with sensor technologies that provide detection capabilities in additional frequency regions". The report also recommends that "as with x-ray-based passenger imaging, the TSA needs to address issues associated with personal privacy raised by millimeter-wave/terahertz imaging".

29. Eventually in October 2008, the first comprehensive ***Privacy Impact Assessment for Whole Body Imaging*** was published by the *US Department of Homeland Security*.[9] The report examines WBI used in the TSA pilot program in the light of the Fair Information Practice Principles (FIPPs). In particular the report focuses on the operating protocol, notably;

- Sample images are available to individuals at the location of the WBI device to show the image to individuals deciding whether they choose the WBI visual inspection instead of the physical pat down inspection.
- Transportation Security Officer (TSO) viewing the image is isolated from the TSO interacting with the individual. The TSO viewing the image communicates with the TSO at the checkpoint through a red/green light system, or via radio, or by highlight an anomaly location on a generic figure that is displayed on a monitor that the checkpoint TSO can read. The TSO at the checkpoint then conducts a physical pat-down that is focused on the particular area and not necessarily of the individual's entire body.
- The image does not present sufficient details to be used for personal identification.
- The image storage functions is disabled by the manufacturer before the devices are placed in an airport and cannot be activated by operators. Images are maintained on the screen only for as long as it takes to resolve any anomalies. The equipment does not retain the image.
- TSOs are prohibited from bringing any device into the viewing area that has any photographic capability, including cell phone cameras.
- Rules governing the operating procedures are documented in standard operating procedures (SOP), and compliance with these procedures is reviewed on a routine basis.

7 http://www.frascati.enea.it/THz-BRIDGE/

8 Assessment of Millimeter-Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapons http://www.nap.edu/catalog/11826.html

9 US DHS, Privacy Impact Assessment for TSA Whole Body Imaging October 17, 2008

The report ends by stating that "WBI technology used in the pilot program has the potential to improve threat detection capabilities for both metallic and non-metallic threat objects, while improving the passenger experience for those passengers for whom a physical pat-down is uncomfortable. The operating protocols of remote viewing and no image retention are strong privacy protections that permit security benefits to be achieved".

30. Between December 2008 and March 2009, the EC DIRECTORATE GENERAL FOR ENERGY AND TRANSPORT (DG TREN) carried out a public consultation on ***The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection***.[10] After stating that "the quality of hand searches is very variable at Community airports, as has been seen by the Commission as part of its compliance monitoring programme of airport inspections" and that "passengers often find hand searches intrusive and upsetting to their dignity", and that "hand searching of passengers is time-consuming and labour-intensive", the document asks whether body scanners could be used as an alternative to the existing means of screening passengers. Other crucial questions posed by the consultation document concern fundamental rights ("Respect for privacy, human dignity as well as protection of personal data are the fundamental rights most often discussed in relation to body scanners. Are there any other fundamental rights that in your opinion could be affected [...] by the use of body scanners?"), whether personal data of individuals are being processed by WBI systems, eventually whether the use of Privacy Enhancing Technologies (PETs) can help facilitate compliance with data protection rules.

31. On February 2009 the *Art.29 Working Party* (Art.29 WP) and the *European Data Protection Supervisor* (EDPS) jointly answered the consultation document with an opinion on ***The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection***.[11] In the accompanying letter addressed to Mr D.Calleja Crespo, Director Air Transport at DG TREN, Mr A. Türk, Art.29 WP Chairman, expresses a "strong reservation towards body scanners as described in your questionnaire. Aviation security is a legitimate aim but the use of any devices to be introduced in addition to already existing walk through metal detectors (WTMD) and hand scanners needs to be based on sound evidence as to why they are needed and why existing measures are not sufficient [...]. The use of body scanners could only be considered as proportionate if an acceptable balance is struck between their necessity and their effectiveness on the one hand and their impact on the privacy of passengers on the other hand."[12] The opinion starts by arguing that it is not appropriate to describe "body scanners as an alternative to hand searches as an individual will still need to undergo a hand search if the scanner detects an anomalous object" Further to this argument, counter intuitively the document contends that "making body scanners voluntary undermines the reasons for needing them". Indeed "giving a choice to the individual might at first sight appear as a more balanced solution but raises serious questions as to the effective necessity and efficiency of body scanners", which can be justified only on the basis of their absolute necessity. The documents also stresses that "while assessing the necessity of body scanners, a distinction should be made between their *convenience* (gain in time) and their added value in terms of *security*

10 http://ec.europa.eu/transport/air/consultations/doc/2009_02_19_body_scanners_questionnaire.pdf

11 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009-others_en.htm

12 http://ec.europa.euijusticehome/fsj/privacyiindexen.htm

(capacity to detect concealed threat objects)", with only the latter being a valid justification for routine use of WBI technology. For the same reason, Data Protection authorities reject that certain categories of persons (e.g. minors, pregnant women, disabled persons) might be automatically exempted from body scanner. "Excluding some individuals from the screening, whatever the reason (just as giving a choice to the individual), puts into question the real necessity of the system, as any *mala fide* person could use such exemption to bypass the control". As per issues related the informational intrusiveness of WBI, the Art.29 WP and the EDPS substantially reflect the *Privacy Impact Assessment for Whole Body Imaging* published by the US Department of Homeland Security, but for considering the use of a body scanner as processing personal data (the US DHS PIA denied that body scanner images could be considered personal data, since they would not be any more linkable to an identifiable individual). The document ends by requesting the use of privacy enhancing technologies, notably the "privacy by design" approach, defined as "*the first and essential requirement in the development of body scanners*".

32. The *Information and Privacy Commissioner of Ontario*, Ms Ann Cavoukian, reached similar conclusions in her privacy impact assessment of WBI systems, published in March 2009, ***Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy***. Also Ms Cavoukian advocates "privacy algorithms" with the main goal of eliminating "*from the imagery all human features that may be considered too intrusive*"[13]. Privacy algorithms, privacy filters, obfuscation, and privacy by design delineate the integrated approach proposed by Ms Cavoukian, who ends her document by stating "Whole Body Imaging technologies that incorporate strong privacy filters – rendering bodily images to mere outlines, to front-line screeners, can deliver privacy-protective security. When combined with appropriate viewing, usage and retention policies, privacy algorithms that obscure personal details, while still allowing potentially threatening concealed objects to be revealed, will allow WBI implementations to satisfy security requirements without sacrificing (and perhaps enhancing) passenger privacy. We believe that this positive-sum paradigm can, and should be, the end goal of such airport security passenger screening technologies – security *and* privacy, not one at the expense of the other".[14]

33. In October 2009, the *Canadian Air Transport Security Authority* (CATSA) completed a **Privacy Impact Assessment in anticipation of the deployment of MM-Wave technology at selected Canadian airports**. The report concludes that "CATSA is addressing all risks with risk mitigation strategies that are in line with privacy best practices including:

- *making the mm Wave Imager screening process voluntary and anonymous;*
- *ensuring that the images are immediately and permanently deleted once the screening process is complete;*
- *ensuring that the mm Wave Imager cannot store, print or save the images.*
- *ensuring that the images reviewed during the screening process cannot be accessed by or transmitted to any other location;*

13 Keller P, Privacy Algorithm for Airport Passenger Screening Portal, Applications and Science of Computational Intelligence III (1999), Vol. 4055, pp. 476-483.

14 Ann Cavoukian, Information and Privacy Commissioner of Ontario , "Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy", March 2009.

- *ensuring that the images are exclusively reviewed by a Screening Officer located in a remote viewing room;*
- *not correlating the images in any way with the name of the passenger or any other identifying information"*[15]

34. In reply to the PIA carried out by the CATSA, the *Canadian Office of the Privacy Commissioner* (OPC) sent a ***Letter in response to the Privacy Impact Assessment (PIA) completed by the Canadian Air Transport Security Authority (CATSA)***.[16] The letter raises various interesting issues, notably about the need to introduce WBI technology: "we continue to urge CATSA to regularly scrutinize implementation of MMW screening technology and justify it against the following four-part test:

    - Is the measure demonstrably necessary to meet a specific need?
    - Is it likely to be effective in meeting that need?
    - Is the loss of privacy proportional to the need?
    - Is there a less privacy-invasive way of achieving the same end?"

    The letter concludes by recommending that "CATSA regularly review its perceived need for WBI screening against updated aviation security threat/risk assessments, as well as against enhancements or refinements to the available technology, such as improved privacy filtering software. New or alternative technologies to achieve the same screening goals in a less privacy-invasive manner should also be considered". The OPC also suggests that MM-wave technology is used "only as a secondary screening tool, and then, only as a voluntary option to a traveller undergoing a physical pat-down."

35. The issue of security threat/risk assessments is also addressed in a 2010 report prepared by the *US Government Accountability Office* (GAO) on request of the House Committee on Homeland Security, in the aftermath of the failed 25 December attack, ***Homeland Security: Better Use of Terrorist Watch list Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security.***[17] The main argument raised by the document is that to date we still lack an assessment of WBI's vulnerabilities to determine the extent to which a terrorist could to carry out an attack which could evade detection by WBI.

36. On February 1, 2010, the *UK Department for Transport* made public an **Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology** covering privacy, health and safety, data protection and equality issues. The Code requires airports to undertake scanning sensitively, having regard to the rights of passengers. The Department also announced the intention to launch a full public consultation on the requirements relating to the use of body scanners in order to finalize a Final Code of Practice by the end of 2010.[18] The Interim Codes describes WBI operating procedures and privacy requirements, which include separation between the screener (who sees the body image) and the security officer (who supervises the checkpoint), no retention

15 http://catsa.gc.ca/File/Library/59/English/PIA%20summary.pdf

16 http://www.priv.gc.ca/pia-efvp/let_20100108_e.cfm

17 GAO-10-401T , January 27, 2010, http://www.gao.gov/products/GAO-10-401T

18 http://www.dft.gov.uk/press/speechesstatements/statements/adonis20100201

of the image, possibility for the person selected for scanning to request that the screen reader is of the same sex as the person. The code also explicitly affirms that "Passengers must not be selected on the basis of personal characteristics (i.e. on a basis that may constitute discrimination such as gender, age, race or ethnic origin)". [19]

37. On June 2010, the European Commission finally issued a policy document on the Use of Security Scanners at EU airports in response to European Parliament Resolution No (2008)0521.[20] After stating that "*Common EU standards for Security Scanners can ensure an equal level of protection of fundamental rights and health (...) Only a EU approach would legally guarantee uniform application of security rules and standards throughout all EU airports. This is essential to ensure both the highest level of aviation security as well as the best possible protection of EU citizens' fundamental rights and health*", the Communication concludes: "*The Commission will decide on the next steps to take, including whether or not to propose an EU legal framework on the use of Security Scanners at EU airports and the conditions to be included in such a framework to ensure full respect of fundamental rights and to address health concerns. This will be done, in the light of the outcome of the discussion with the European Parliament and the Council. As any legislative proposal would have to be accompanied by an impact assessment, the Commission would immediately start working on such an impact assessment to address the issues raised in this Report*", that is to say that a final decision is still postponed, although the general principle that the issue is relevant to the EU has been now definitely affirmed.

38. Further the Commission's Communication both the European Parliament Committee on the Environment, Public Health and Food Safety (ENVI)[21] and the Committee on Civil Liberties, Justice and Home Affairs (LIBE),[22] issued specific opinions to be incorporated by the Committee on Transport and Tourism, in its motion for a resolution. The ENVI's opinion "*suggests, as the most appropriate solution as far as health is concerned, technology based on passive millimetre wave imaging systems, which do not emit any radiation*". In its turn, the LIBE's opinion emphasis that every person "*should have the right to refuse a body scan, without the obligation to give any explanation, and the right to request a standard security check, with full respect for the rights and dignity of that person*".

39. In early February 2011 also European Economic and Social Committee (EESC) replied to the Commission's Communication by issuing an opinion. [23] The EESC shows strong

19 UK Dept. for Transport, Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology (Body Scanners) in an Aviation Security Environment, http://www.dft.gov.uk/pgr/security/aviation/airport/

20 COM(2010) 311 final, Brussels, 15.6.2010

21 Committee on the Environment, Public Health and Food Safety, DRAFT OPINION on air safety, with particular reference to body scanners, 9 November 2010

22 Committee on Civil Liberties, Justice and Home Affairs, DRAFT OPINION on aviation security with a special focus on security scanners, 14 February 2011

23 European Economic and Social Committee, TEN/429, Opinion on the Use of Security Scanners at EU airports, Brussels, 16 February 2011

reservations on the EC Communication on the basis of "*the potential adoption and implementation of a future regulation which could place considerable burdens on private individuals, affecting the exercise of their fundamental rights*". Furthermore the EESC affirms that "*the communication does not appear to comply fully with the three criteria of necessity, proportionality and legality*" and "*All in all, there are serious doubts, not as to the legality, but rather the legitimacy of the communication*". In addition the EESC opinion "*calls on the Commission to provide conclusive studies on the potential implications of such devices for the health of passengers and of staff submitted to frequent checks in the course of their work; in the event of any doubt, it would be preferable to use other types of instruments*". Also the EESC wishes to "*remind the Commission that the Communication makes no mention of the effective legal remedy that should be guaranteed to the weaker party, i.e. the passenger*"

40. However in February 2011 the EP Committee on Transport and Tourism (TRAN),[24] say, the Parliamentary Committee responsible for the subject matter, produced a draft resolution quite positive concerning body scanner technology. The Committee calls on "*the Commission to propose adding security scanners to the list of authorised screening methods, together with appropriate rules for their use, as set out in this resolution* " and although they suggest that "*the use of security scanners must be based on common rules that not only lay down detection performance but also impose the necessary safeguards to protect the health and fundamental rights of passengers and workers*". The TRAN's resolution is expected to be discussed by the European Parliament in late June 2011.

24 Committee on Transport and Tourism, DRAFT REPORT on aviation security, with a special focus on security scanners, 23 February 2011

CHAPTER 4: Ethical discussion

Bodily Integrity

41. The human body - its legal and moral status, its value, its meanings, and the way in which technologies modify it - lies at the heart of the body scanner debate. The notion of "body" is much more metaphysical than people usually think. What is the body? Say, what is the body "alone", without "its" mind? The body isolated is just a corpse.[1] Indeed what we call "human body" is a sophisticated metaphysical concept[2], which results from the binary opposition of mind / body rooted in Platonic dualism, late Greek philosophy, Christian theology, and Cartesianism. The idea of body is a simulation and a partial model, which splits in two the polysemic and ambiguous nature of the human subject. In other words, the concept of body is *a way of seeing* actual human beings. Biomedical practices separate mind and body, and keep the body as a medium of disease. A similar operation is carried out by current security practices, which tend to dissolve the subject into risk categories. The overseer's gaze observes and explores the human body as a source of risks, as a potential threat. The human body under surveillance becomes "an assemblage comprised of myriad component parts and processes which are broken down for purposes of observation".[3] Such a "securitized" body is mirrored by the suicide terrorist's body being turned into a weapon: both the securitized and the terrorist's bodies are highly symbolic constructions, whose meanings go well beyond their mere physical reality. The human body is a symbolic field and should be studied as such.[4]

KEY MESSAGE TO POLICY MAKERS

Practices which concern the body are unavoidably invested with cultural values, and in their turn produce new values. WBI impact assessment should consider the symbolic dimension, which is often more relevant to policy setting than conventional technology assessment.

42. Bodily issues associated to the adoption of body scanners at airport checkpoints, include various kinds of violation of body integrity. The word integrity literally means "the quality or state of being complete or undivided". Physical and mental integrity thus refers to the

1 "The corpse is, if you will, a dream about the body which, as we have said, imagines the body as dismembered in two ways. On one hand, this dream is a way of imagining the body as isolated or cut off from its natural context or situation. On the other hand, this dream is a way of imagining the body as fragmented within itself, as a specimen" Romanyshyn R, (1989) *Technology as Symptom and Dream*. New York: Routledge, p.119

2 The terms psyche and soma were already present in Homer, but with a different meaning: soma indicated the corpse, the dead body, while psyche was the vital breath. Even the biblical tradition ignored concepts like soul, body, spirit. *Nefesh*, then translated psyche, expressed the fragility of the human being, his desire, his incompleteness. *Basar* was not the body, but the weakness of the man who denies God. A man is flesh enlivened by God, away from God he becomes futility and impotence.

3 Haggerty KD, Ericson RV (2000), The Surveillance Assemblage, British Journal of Sociology, 51, 4, 605–622

4 Slattery DP, (1994), Of corpses and kings: Antigone and the body politic, *Lit: Literature Interpretation Theory*, 5, 2: 155 – 167

inviolability of a person's body and mind, say, it refers to the right against being touched (in physical and metaphorical senses) without consent. Historically, the notion of body integrity comes from the legal conception of *Habeas Corpus* (Latin: you shall have the body), originally the legal action through which a person can seek protection against an unlawful detention. The *Habeas Corpus* affirms the right not to be imprisoned arbitrarily and to not have the body violated in any other way (e.g., physical inspection, torture, abusive treatments, and so on). "The violation of the right to physical and psychological integrity of persons is a category of violation that has several gradations and embraces treatment ranging from torture to other types of humiliation or cruel, inhuman or degrading treatment with varying degrees of physical and psychological effects caused by endogenous and exogenous factors which must be proven in each specific case".[5] Body integrity is threatened by physical pain, injuries, sexual assaults, rape, physical inspections, and the like. Mental integrity is violated any time when emotional and cognitive processes are brutally invaded, abused and/or disrupted.

Dignity and Physical Privacy

43. We all have an interest in protecting our physical or mental integrity. This is clearly expressed by the ***Universal Declaration of Human Rights*** (art.3) which states that everyone has a right to the inviolability of his or her person, and by the ***Convention on Human Rights and Biomedicine***[6] (art.1), which states that "Parties to this Convention shall protect the dignity and identity of all human beings and guarantee everyone, without discrimination, respect for their integrity and other rights and fundamental freedoms with regard to the application of biology and medicine". The principle of body integrity does not concern only violations of the body resulting in suffering or in adverse health conditions, but it also deals with intrusions without harmful effects. This leads to an additional issue, which is particularly relevant to the body scanner debate. Does a bodily or psychological intrusion constitute a violation of integrity only if it is perceived as such? Or, on the contrary, are there objective criteria to establish when a violation infringes the right to integrity? Indeed the principle of the "inviolability of the body" includes two cognate, but different,[7] concepts: 1) the view "that the body is a

5 Inter-American Court of Human Rights, *Loayza Tamayo Case*, Judgment of Sept. 17, 1997 (Ser. C) No. 33, para. 57, http://www1.umn.edu/humanrts/iachr/C/42-ing.html

6 The concept of body integrity has important applications in the biomedical sphere, where inter alia it requires that invasive actions cannot be lifted without the informed consent of the patient.

7 Actually, together with Giorgio Agamben, one could argue that these two concepts are anything but the two sides of the same coin, being the notion of sacred body only the other side of the notion of body as a property. In his analysis of the *habeas corpus*, Agamben argues that "the root of modern democracy's secret biopolitical calling lies here: he who will appear later as the bearer of rights and, according to a curious oxymoron, as the new sovereign subject (*subiectus superaneus*, in other words, what is below and, at the same time, most elevated) can only be constituted as such through the repetition of the sovereign exception and the isolation of *corpus*, bare life, in himself. If it is true that law needs a body in order to be in force, and if one can speak, in this sense, of "law's desire to have a body," democracy responds to this desire by compelling law to assume the care of this body. This ambiguous (or polar) character of democracy appears even more clearly in the *habeas corpus* if one considers the fact that the same legal procedure that was originally intended to assure the presence of the accused at the trial and, therefore, to keep the accused from avoiding judgment, turns -- in its new and definitive form -- into grounds for the sheriff to detain and exhibit the body of the accused. *Corpus is a two-faced being, the bearer both of subjection to sovereign power and of individual liberties" (Agamben G, 1988,* Homo Sacer: Sovereign Power and Bare Life. Stanford UP, Stanford, CA. P 124-125)

'sacredness' in the biological order"[8]; and 2) the view of the body as personal property, whose borders cannot be trespassed without the owner's consent. There are then two diverse perspectives about body integrity, the former contends that the right to be free from bodily (and mental) intrusion is inherently part of the notion of human dignity[9], the latter maintains that bodily integrity is the right of "every human being ... to determine what shall be done with his own body"[10] and to protect his physical privacy. While the dignitarian approach usually contends that body integrity is – at least in part – an objective concept, the privacy approach emphasises the subjective aspect of body integrity, which always implies the notion of consent (or lack of) to the intrusion.

44. The tension between dignitarian and privacy interpretations of body integrity is well illustrated by the Dutch Constitution (art.11) which states "everyone has a right to untouchability of his body, except for restrictions provided by or valid because of the law". Then, according to Dutch criminal law (art.56), arrested people can be "examined on body and clothes" but only if the examination limits itself to the surface of the body (including natural orifices), while "cutting or pulling hair, drawing blood and obtaining sperm, and taking x-rays are not warranted".[11] The law then prohibits the use of any instrument which can penetrate the body surface, conceptualised as a moral and legal border not to be trespassed. It is evident that here there is a tension related to the word "untouchability", which could refer either to the dignity, the sacredness, of the whole body, or to the notion of 'body' as a private property, which is touchable only to the extent that its owner consents.[12]

45. A dignitarian interpretation of the notion of body integrity is endorsed by the *Charter of Fundamental Rights of the European Union*, which has an article (art.3), specifically focusing on the *Right to the integrity of the person*, in the first Chapter devoted to Dignity:

    1. Everyone has the right to respect for his or her physical and mental integrity.
    2. In the fields of medicine and biology, the following must be respected in particular: the free and informed consent of the person concerned, according to the procedures laid down by law [...]

    The context in which art.3 is collocated points out that "the dignity principle should be regarded as a tool to identify the cases in which the body should be absolutely *inviolable*" [13] and that consequently "the principle of inviolability of the body and physical

8 Murray TH, (1987), On the Human Body as Property: the Meaning of Embodiment, Markets, and The Need of Strangers, *Journal of Law Reform* 20, 4:1055-1089

9 See for instance, Maschke KJ, (2003), Proxy Research Consent and the Decisionally Impaired: Science, the Common Good, and Bodily Integrity, *Journal of Disability Policy Studies* 13, 4

10 Schloendorff v. Society of New York Hospital, 1914, quoted by Maschke KJ, (2003).

11 Ten Have HA, Welie JW, (1998) Ownership of the Human Body Philosophical Considerations, Springer, p.102

12 The notion of sacredness implies etymologically that something is untouchable because it belongs to the god. The two notions of dignity and privacy eventually differ only in defining who is the owner of the body, whether the god or the man.

13 European Group on Ethics in Science and New Technologies (EGE), Op. N° 20, Ethical aspects of ICT implants in the human body, Adopted on 16/03/2005

and psychological integrity set out in Article 3 of the Charter of Fundamental Rights rules out any activity that may jeopardise integrity in whole or in part - even with the data subject's consent."[14] The respect for body integrity demands that body inviolability is considered – at least in part – a non-negotiable principle. Body integrity is violated any time that an undue and unsolicited intrusion "penetrates" the individual's personal sphere, independently from whether such an intrusion is tactile, visual, acoustic, psychological, etc. or whether it produces injuries.

46. In the US bodily integrity is protected by the Fourth Amendment of the Constitution, which protects physical privacy:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

In order to be reasonable a search should meet people's rational expectations about their right to privacy.[15] Intrusive searches demand specific reasons, might need a warrant, and cannot be a routine procedure. In 2008 the New York State Court of Appeals (New York State's highest court) discussed the case of Azim Hall, a drug dealer who was stripped and searched by the police and was found to have a string hanging from his anus. The police pulled the string and found a baggie of cocaine inside his rectum. Azim Hall complained that his Fourth Amendment right was violated. The Court ruled that

> There are three distinct and increasingly intrusive types of bodily examinations undertaken by law enforcement after certain arrests and it is critical to differentiate between these categories of searches. A "strip search" requires the arrestee to disrobe so that a police officer can visually inspect the person's body. The second type of examination — a "visual body cavity inspection" — occurs when a police officer looks at the arrestee's anal or genital cavities, usually by asking the arrestee to bend over; however, the officer does not touch the arrestee's body cavity. In contrast, a "manual body cavity search" includes some degree of touching or probing of a body cavity that causes a physical intrusion beyond the body's surface [...] Summarizing the relevant constitutional precedent, it is clear that a strip search must be founded on a reasonable suspicion that the arrestee is concealing evidence underneath clothing and the search must be conducted in a reasonable manner. To advance to the next level required for a visual cavity inspection, the police must have a specific, articulable factual basis supporting a reasonable suspicion to believe the arrestee secreted evidence inside a body cavity and the visual inspection must be conducted reasonably. If an object is visually detected or other information provides probable cause that an object is hidden inside the arrestee's body, Schmerber dictates that a warrant be obtained before conducting a body cavity search unless an emergency situation exists.[16]

14 Ibid.

15 Katz v. United States, 389 U.S. 347, 351 (1967)

16 People v. Azim Hall, 2008 NY Slip Op 2676 (2008)

Then according to *People v. Azim Hall* it would be difficult to justify a body scanner examination on a routine-basis without "*a reasonable suspicion*" that the person is "*concealing evidence underneath clothing*". On the other hand, a specific warrant is not necessary, given that WBI cannot inspect body cavities.

47. There is an apparent a tension between the **EU Charter** and the **US Constitution** perspectives on body scanners. In the European perspective the potential offence of WBI to body integrity does not seem to depend chiefly on the way in which the subject perceives the intrusion, nor on whether personal data are properly handled. In other words the offence to human dignity can be hardly mitigated by only respecting rules of decency and by adopting privacy and modesty filters. The potential offence is related to the fact that the human body is not respected, because it is exposed as though it were a commodity. As Murphy and Wilds argue, the body scanner "reduces the traveler's body to the same legal status as a piece of luggage on a conveyor belt."[17] This casts doubts about whether routine search though WBI might ever be consistent with respect for EU fundamental rights, notably art.3, unless the technology would not show the body at all, but merely the objects the person is holding.

48. Also in the light of the **US Constitution**, it would be difficult to justify routine air traveler screening through body scanners. As Klitou[18] argues "under the current conditions, whereby the employment of a privacy algorithm or the deletion of the images is not mechanically ensured and other safeguards are not legally binding, the use of back-scatter body scanners is disproportionate and constitutes an unjustified violation of privacy in a democratic society [...]the law, as it stands now, is unable to adequately uphold the integrity of the Fourth Amendment or protect the right to privacy." It is notable, however, that, according to this perspective, effective and legally binding privacy algorithms could protect the right to privacy and then make WBI systems consistent with the Fourth Amendment.

49. Finally, an ethical framework which would include both dignitarian and privacy perspectives, could be based on the notion of body as a "gift"[19]. The body is never completely "ours", for the very reason that it has a symbolic dimension, say, each body is "embodied" in a given human community. We "receive" ourselves as a gift from the human community and we are in debt with our fellow human beings. In fact, persons are not simply co-extensive with their bodies: people are made up also by their human relations, by the social networks to which they belong across space and time. "We are bound together by our often needy bodies (and by our other, non physiological needs) into a community of needs. In this community-really multiple communities, sometimes overlapping, some like ripples extending wider and wider around a core we can recognize the needs of others through our shared embodiment".[20] Our shared embodiment is also the source of our fragility, and the moral justification for cooperation when safety and collective security are at stake. This would be the case of WBI for aviation security, provided that its effectiveness and proportionality are convincingly demonstrated.

---

17 Murphy MC, Wilds MR (2001). X-rated x-ray invades privacy rights. *Criminal Justice Policy Review, 12*(4), 333–343.

18 Klitou D, (2008), Backscatter body scanners – A strip search by other means, *Computer Law & Security Report* 24, 316 – 325

19 Murray T, Gifts of the Body and the Needs of strangers, *Hastings Center Report*, April 1987, 30-38

20 Murray T, (1987), ibid.

KEY MESSAGE TO POLICY MAKERS

In order to make WBI technology consistent with respect for human dignity, integrity and physical privacy WBI should not show the "naked" body but merely the objects the person is holding. This general tenet implies two converging strategies. First the officer viewing the image should not see the scanned person. The use of modesty filters is also advisable. Second, WBI systems should be selected according to their capacity to detect prohibited items without providing anatomic and medical details. In any case the adoption of WBI technology for routine screening is ethically tenable only if its effectiveness and proportionality are convincingly demonstrated.

Physical Integrity

50. Direct effects on the body of current WBI technologies are very limited[21] and the health impact of all existing WBI is negligible. Apart from x-ray transmission systems, no WBI, including x-ray backscatter, is expected to have any relevant health impact on people. To be sure, pacemakers and implantable cardioverter-defibrillators (ICDs) may be susceptible to electromagnetic interference from a number of devices (e.g., cellular telephones, electronic surveillance systems, metal detectors). People with such medical implants should also avoid electromagnetic pulse generating body scanners (but they could be examined through passive systems).

51. In the case of backscatter technology, however, the body is going to absorb a very low dose of ionizing radiation, which is likely to produce negligible effects on human cells. Although the dose absorbed is below the threshold of health risks and could be considered as a component of the background radiation in which we all live, there is no rationale to expose anyone to an additional source of ionizing radiations, as low as they are, when the same results could be achieved by using non-ionizing electromagnetic waves. Given that there is no evidence that x-ray backscatters are more reliable and accurate than MM-wave scanners, it is difficult to understand why backscatter technology is still considered as a potential candidate for people screening at airport check-points. On the contrary there are two parallel arguments that suggest excluding backscatters from potential screening technologies would be wise: 1) In the absence of any other benefit, one should give privilege to the least physically intrusive technology, and there is no doubt that MM-wave devices have less effects on the human body than x-ray backscatters; 2) In the absence of any other benefit, one should promote the most acceptable technology, and people are likely to prefer to undergo non-ionizing radiations rather than ionizing radiations.

52. X-ray transmission systems have never been proposed for routinely screening in airports. Yet, sooner or later, it is likely that the possibility to use them for selected checks will be raised. Advances in miniaturisation are making it easier for terrorists to hide small bombs into body cavities, or implant them surgically. These bombs, powerful enough to cause a plane to crash, will not be detected by metal detectors and body scanners. Such a body bomb method was tested for the first time in August 2009, when

21 In the EU health and safety of electrical equipment is governed by the Low Voltage Directive 2006/95/EC, and by the Council Recommendation 1999/519/EC. Millimeter wave technology is instead covered by the Directive 1999/5/EC on radio and telecommunication equipment.

the Saudi anti-terrorism chief, Prince Mohammed bin Nayef, survived a terrorist attack carried out by a 23-year-old Al Qaeda militant who got through several security checks with military grade plastic explosive in his rectum. The bomb was probably triggered by a signal from a mobile phone text message. Most analysts think that this kind of attack is going to increase and consequently will have a very relevant impact on screening tactics and techniques for years to come.[22] To date only X-ray transmission systems could detect explosives hidden inside the body, although very low radiation systems are available.[23]

KEY MESSAGE TO POLICY MAKERS

Assuming all other conditions equal, there is no reason to adopt X-ray backscatters, which expose the subject to an additional – although negligible – source of ionizing radiations. Other WBI technologies should be preferred for standard use. The use of X-ray transmission systems for selected checks (i.e., explosives hidden inside the body) should be avoided and alternative technologies using non-ionizing radiations should be investigated.

Mental Integrity

53. On Jan 11, 2010 German activists from the Pirate Party organised for a "fleshmob" in the Berlin-Tegel airport. Naked protesters marked their bodies with a number of messages such as, "Something to hide?" and "Be a good citizen — drop your pants."[24] Body scanner images might show intimate body parts, like breasts and genitalia, as well as intimate personal and medical details and many scholars and privacy advocates have argued that WBI should be considered a "virtual strip search"[25]. Menstrual pads, incontinence pads, diapers and suchlike, are all detectable and WBI can also easily detect under-the-skin implants, such as breast and penile implants and a vast array of cosmetic surgeries. Colostomy inserts, various kinds of prosthesis, electronic body implants, and body piercings can also all be revealed by all WBI systems. Although in real life the quality of images is far from those advertised in producers' web sites and leaflets, it is difficult to deny that the end result of WBI, without any modesty filter, "is similar to that of strip searches and far more intrusive than patdowns"[26].

22 http://www.dailymail.co.uk/news/worldnews/article-1218562/Bombers-hide-devices-inside-bodies-Travellers-Europe-face-body-X-rays.html

23 There are also *Body Orifice Screening Systems*, which are designed for security inspection of body cavities. The Body Orifice screening system are non intrusive and eliminates the liability and safety issues associated with manual searches. The systems use a low ionising radiations (http://www.adani.by/en/products/security-x-ray/personnel)

24 German 'Fleshmob' Protests Airport Scanners; Wired, Jan 12, 2010 http://www.wired.com/threatlevel/2010/01/german-leshmob/#ixzz0cVWE4UJX

25 American Civil Liberties Union (ACLU) Backgrounder on Body scanners and "Virtual Strip Searches", available at http://www.aclu.org/privacy/35540res20080606.html

26 Klitou D, (2008), ibid.

54. Imposed "virtual" nakedness is an important threat to bodily and psychological integrity. Nakedness is more than nudity. While *nudity* is the simple state of absence of clothing, *nakedness* is a mental state, which implies being stripped of decency, to lack an element of protection. *Nakedness* involves objectification, the process of symbolically turning a person into an object to be appraised. As Rabbi Bradley Shavit Artson argues "In the Garden, Adam and Eve were nude and complete. Outcast, and with a consciousness of having sinned, they became naked."[27] While *nudity* is an objective, empirical, condition, *nakedness* is a highly symbolic experience, which is culturally determined. In most cultures, physical exposure is a form of pornography, which "would de-sacralize matter, deprive matter of spirit"[28]. *Nakedness* has also to do with power: those who see are usually more powerful than those who are seen. In *Foucauldian* terms the exercise of power involves regulation through visibility.

55. What turns nudity into nakedness is degradation.[29] Degradation means devaluation, dehumanization. Degradation always implies a certain degree of self-degradation, as pointed out by Primo Levi in *The Drowned and the Saved* (1986). Levi shows how physical degradation tends to produce the complicity of the victim, and eventually it destroys the sense of worth and self-esteem, and generates humiliation. Humiliation is the last step in this path through threats to mental integrity. "To be humiliated means to have your personal boundaries violated and your personal space invaded [...] Although the feelings of humiliation are intensely personal, the process itself is located in the relationship between the persons."[30]

56. Worries about the risk that WBI might become an humiliating experience have been raised in particular for women, children, incapacitated persons, and specific ethnic and religious groups. Most PIAs recommend that individuals could opt for being examined by an operator of the same gender or, even, that the procedure routinely provides two machines, one for women, and one for men. The Canadian Privacy Commissioner asked that incapacitated persons might be exempted from WBI examination, on the basis of their incapacity to provide a free and informed consent. One should also take into account that some persons wouldn't even be able to enter the body scanner, e.g. mothers with baby carriages and people in a wheelchair. In the UK the civil rights group *Action on Rights for Children* questioned whether the scanners could breach the Protection of Children Act 1978, under which it is illegal to create an indecent image or a "pseudo-image" of a child.[31] Trevor Phillips, head of the *Equality and Human Rights Commission* (EHRC), a UK non-departmental Government body, also warned "that using profiling techniques to single out Muslims, Asians and black people for scanning at airports

27 Rabbi Bradley Shavit Artson, *Shabbat Parashat Yitro, 22 Shevat 5764 - The Naked & The Nude* - http://judaism.ajula.edu/Content/ContentUnit.asp?CID=912&u=4556&t=0

28 Griffin S, (1978) *Woman and Nature: The Roaring Inside Her.* New York: Harper

29 Shapiro DL, (2004), The Nature of Humiliation Paper presented at the 2005 Workshop on Humiliation and Violent Conflict, Columbia University, New York, December 15-16, 2005.

30 Klein DC (2005) The Humiliation Dynamic: Looking to the Past and Future, Paper presented at the 2005 Workshop on Humiliation and Violent Conflict, Columbia University, New York, December 15-16, 2005.

31 Body scanners threaten children's rights, The Guardian, Jan 4, 2010 http://www.guardian.co.uk/commentisfree/libertycentral/2010/jan/04/airport-body-scanners

could breach race and religious discrimination laws introduced by the government."[32] Some Islamic groups[33] have questioned whether body scanners are "particularly offensive to Muslim women, who may choose to dress modestly, as well as being targeted for profiling on the basis of their race, religion or appear". [34] Indeed Islam guides that, for both men and women, clothing must be as loose as not to outline the shape of the body, this rule is apparently contradicted by body scanners. A Fatwa issued on February 9th by the *Fiqh Council of North America* emphasized that "a general and public use of such scanners is against the teaching of Islam, natural law and all religions and cultures that stand for decency and modesty"[35]. The Fatwa recommends to Muslim to avail the pat down search over the "nude body scanners". Also the *Rabbinical Center of Europe* (RCE) complained that WBI in European airports might compromise Jewish women's modesty, and recommended that "men are scanned by men, and women by women, akin to body frisk." [36] In June 2009, *Agudath Israel,* which represents traditional American Orthodox communities, sent a letter to the US Senate subcommittee dealing with the body scanner dossier, promoting an amendment that limited the use of the full-body scanners to situations in which passengers had already failed a metal detector test, provided that those passengers be also offered the option of a pat-down search. In this letter *Agudath Israel* judged WBI "offensive, and far short of acceptable norms of modesty (*tzniut*) under the laws and practices of Judaism and many faith communities". [37]

KEY MESSAGE TO POLICY MAKERS

All forms of modesty deserve to be fully respected– no matter how far they are from the western ethos. Some people could perceive WBI screening as an humiliating experience. Their objections should be always be taken into account. No one should be ever be obliged to undergo to any security measure that he feels humiliating and degrading. In particular no one should be offered the option to accept such a measure in exchange for a benefit. This would make it still more humiliating.

32 Airport full-body scanners 'break laws on privacy', The Sunday Times January 17, 2010, http://www.timesonline.co.uk/tol/news/politics/article6990990.ece

33 EU divided on use of airport body scanners, http://www.msnbc.msn.com/id/34747772

34 Airport Body Scanners Only Offensive to Muslim Women?, *Muslimah Media Watch,* http://muslimahmediawatch.org/2010/01/naked-ambition-plans-for-airport-body-scanners-only-offensive-to-muslim-women/

35 http://www.fiqhcouncil.org. See also http://theklaxon.com/council-issues-fatwa-on-full-body-scanners-at-airports-complicates-u-s-security/4989

36 http://www.ynet.co.il/english/articles/0,7340,L-3831622,00.html

37 How Modern Airport Security May Run Afoul of Jewish Law, The Jewish Daily Forward http://www.forward.com/articles/123364/

CHAPTER 5: Privacy issues

57. Emerging WBI technologies promise to be more and more privacy invasive. Today, there is no clear cut distinction between MM-wave and T-ray technology, which are a continuum along the electromagnetic spectrum. All frequencies in this region can be used both to create an image of an object or to gather information on its chemical makeup. As energy moves from the shorter infrared to the longer microwave region of the electromagnetic band, it becomes able to do different things. As frequencies increase, the radiation acquires spectroscopic capacities (e.g., it can be used to identify different kinds of chemicals and materials). Also it penetrates the human body surface through half a centimeter, becoming able to distinguish normal skin tissue from tumours, and some superficial breast cancers; T-radiation can also get an image of the dental arcade, which could be used for personal identification.

58. Technologies rapidly evolves: screening systems in the near future probably will be based on "a fusion of multiple technologies, on the ability to detect multiple threats simultaneously, and most important, on the ability to perform the screening on people not as a dedicated function, but while people are engaged in other activities, such as standing in line for passport control, waiting at the ticket counter or walking from one area of a facility to another"[1]. Emerging WBI systems include "covert systems capable of scanning a vehicle traveling at five to 30 mph [...] smart programs may be written to recognize shapes, optimize machine settings for selected purposes, or identify certain materials, [...] Present technology may also assume different forms. For example, systems may be disguised within decorative portals for the covert screening of individuals passing through the portals. Smaller transmission systems may be produced for the sole purpose of imaging stomach contents in order to search people suspected of having swallowed contraband".[2] It also thinkable that future WBI could become part of wider systems for hostile intention detection, which is one of the main trends in aviation security.[3]

59. Once WBI systems are legally justified and their use is standard in airports, there is the menace that nothing might prevent the slippery slope towards the adoption of more advanced, and privacy intrusive, systems, and the introduction of WBI for more mundane applications, like in sporting stadiums, public malls, schools, etc. In brief, WBI technology risks to become a building block of the wider apparatus called (by Monahan and Wall[4]) *somatic surveillance* in which "bodies are not only informatized but controlled in various ways".

---

1 Homeland Security Market Research, *People Screening Facing a Challenging, Transition Period*, http://www.homelandsecurityresearch.net/2009/03/17/people-screening-facing-a-challenging-transition-period)

2 NCRP (2004)

3 See in the US http://www.dhs.gov/files/programs/gc_1218480185439.shtm#12, and in the EU http://cordis.europa.eu/fp7/security/fp7-project-leaflets_en.html

4 Monahan T, Wall T, (2007), Somatic Surveillance: Corporeal Control through Information Networks, *Surveillance & Society*, 1, 4(3): 154-173

KEY MESSAGE TO POLICY MAKERS

Emerging WBI technologies should be addressed as soon as possible. In this field technology evolves very rapidly and once the use of WBI systems becomes standard in airports, there is a concrete risk that more advanced and privacy intrusive systems are would further then be introduced, and that they are could also be used for more mundane applications.

Privacy Enhancing Technologies

60. Vis-à-vis such a worrying scenario, there is however a consensus among PIA documents that a proper use of privacy enhancing technologies (PET) can minimize privacy invasion and make WBI systems ethically tenable. The so called "second generation" WBI systems which have been adopted e.g., in The Netherlands and in Italy, feature only a kind of generic, impersonal, graphics[5]. The point is whether these protections are, and will be, actually implemented. For instance *Privacy International* "is sceptical about the privacy safeguards that the US Transportation Safety Administration (TSA) is touting. The TSA say that the technology is capable of obscuring faces, but this claimed protection is just a software fix that can be undone as easily as it is applied [...] The TSA also say it will not retain the images. That protection would certainly be a vital step for such a potentially invasive system, but given the irresistible pull that images created by this system will create on some employees (for example when a celebrity or someone with an unusual or *freakish* body goes through the system), our attitude is one of *trust but verify*".[6]

61. Two recent cases could support such a skeptical approach. In 2009 the American Electronic Privacy Information Center (EPIC) provided a document to CNN in which the US TSA asked the seller that the body scanners have the ability to store and send images when in test mode. The document also showed that the scanners have 10 variable privacy settings.[7] On February 9, 2010, the movie star Shahrukh Khan revealed on the BBC's Jonathan Ross[8] show that he passed through a body scanner and later had the image of his naked body printed out and circulated by Heathrow security staff. His claims have resonance because of his latest film, *My Name is Khan*, which is about racial profiling of Muslims at airports. A BAA spokeswoman said the claims were "completely factually incorrect". She stressed WBI images could not be stored or distributed in any form and said there would be no investigation into his claims because they "simply could not be true".[9]

5 See e.g., http://detecterfp7.blogspot.com/2010/01/focus-on-full-body-scanners.html and http://www.spiegel.de/fotostrecke/fotostrecke-50292-4.html

6 Statement on proposed deployments of body scanners in airports, www.privacyinternational.org

7 http://www.cnn.com/2010/TRAVEL /01/11/ body.scanners/index.html

8 http://www.bbc.co.uk/programmes/b00qn04k

9 http://www.telegraph.co.uk/news/newstopics/bollywood/7203872/Airport-denies-body-scanner-photo-claim-by-Bollywood-star-Shahrukh-Khan.html

KEY MESSAGE TO POLICY MAKERS

Privacy Enhancing Technologies (PETs) can alleviate privacy concern only if PETs cannot be "switched-off". The "privacy-by-design" approach is the right approach. In addition, given the highly sensitive policy area, it would be advisable to introduce an independent and legally binding control that PETs are properly implemented. In terms of communication with the public, it is paramount that any privacy complaint – although unrealistic – is seriously considered and overtly discussed.

Does WBI generate personal data?

62. The US TSA claims that the adoption of privacy enhancing technologies could irrevocably unlink WBI images from recognisable individuals. This would prevent labelling WBI images 'personal data', and considering WBI procedures data processing, "*TSA has developed operating processes for the WBI, used for pilot operations, that do not collect, store, or distribute any personally identifiable information.*"[10] This view is rejected by most EU privacy authorities, notably by the Art.29 WP and the European Data Protection Supervisor on the basis that "*a link is established between the data provided by the body scanner and the individual who is being screened. Based on the information provided by the body scanner, an evaluation of the threat will be conducted which will result in an impact on the individual (release or additional check). It has therefore to be considered as a processing of personal data.*"[11]

63. Whether WBI devices are or are not generating and handling personal data is not a trivial particular, because it has important legal implications. According to known WBI operating procedures, and according to available information about privacy-built-in protections, in most systems body scanner images 1) are not retained, and 2) the WBI operator is located in a remote viewing room, and is not allowed to either see the scanned subject, nor to keep, or transmit outside, any image. Transportation authorities usually argue that these protections should prevent linking WBI images to any person. Yet this does not completely solve the problem.

64. First of all, personal details generated by WBI are not linked to a person, if that person is released, but if she is retained and further investigated, data may be linked. Given that in most trials (and notably in Dutch trials at Amsterdam airport) there have been a high number of false positives - say, people who set off the system alarm and required further examination, without concealing any prohibited item under their clothes - it is hardly tenable that WBI systems are not going to generate personal data. All false positive people are indeed "linked" to their body scanner images and - although images will not be eventually stored in the system, nor in any other medium - sensible bodily information becomes potentially linkable to an identified person.

65. It is often misunderstood that the mere fact that images are not retained does not imply that WBI systems are not generating data. At the very least they are generating aggregated data about themselves and their effectiveness in detecting concealed objects.

10 US DHS, Privacy Impact Assessment for TSA Whole Body Imaging October 17, 2008

11 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009-others_en.htm

Thus, although images are not retained, they are generating aggregated data about peoples' bodily modifications (e.g., number of people with body piercings, or with under-skin implants). All these details cannot be considered personal data provided that they are not linked to any specific person. Yet there is moment in which there is such a link, although temporary and volatile: when the person is "in" the scanner and the image is in the process of being generated. In that moment data is in the system and is aligned to an identifiable person (the actual person who is in progress to be scanned). This is indeed the most delicate moment of the whole process. If the system is hacked, this is the moment in which one could either produce fake images or steal images from the system. Likewise, this is the moment in which the system can be (mis)used.

66. The issues of function creep and system misuse have hardly been addressed, yet there is a theoretical possibility that WBI systems can be (mis)used for different purposes rather than for detecting concealed objects. WBI systems can be used for people profiling and for personal identfiication. Imagine, for instance, that checkpoint operators have been alerted that a person, who is a likely terrorist, is known for having a breast implant. Operators might be instructed to single out all people with a breast implant and submit them to an extra screening. WBI systems could also be used to identify persons. In the previous example, it would be enough that operators are instructed that the suspected terrorist, beyond the breast implant, *has* a Nigerian passport, *and* is aged less than thirty, *and* spent a month in London in the last year (all these elements could be deduced from the Passenger Name Record, PNR, file). By crossing these clues with the information about the breast implant, WBI can easily allow the identification of the alleged terrorist when she passes through the body scanner. As we mentioned, WBI devices could also be misused for hostile intention detection. Microwave dielectrometer portals are already able (at least according to the producer) to monitor and detect increased heart rates and perspiration levels of people[12] and chances are that next WBI generations could do even more.

KEY MESSAGE TO POLICY MAKERS

Although images are not retained, WBI systems are generating data. Reaching an international consensus about whether these data are personal and to what extent they are sensitive is certainly important. Yet it is still more important to find a consensus about 1) what data are actually generated; 2) how they should be protected. WBI systems could be hacked and there is a common interest from both security agencies and privacy advocates to improve body scanner security and to build more and more secure systems.

12 http://www.global-security-solutions.com/PeoplePortal.htm

CHAPTER 6: Governance

67. In the EU, security screening at airports is "supervised" by the Union, although they remain under member state jurisdictions. According to Regulation (EC) 300/2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, the European Parliament and of the Council "should lay down the basic principles of what has to be done in order to safeguard civil aviation against acts of unlawful interference without going into the technical and procedural details of how they are to be implemented." National legislations are then responsible for detailed regulations. However in most countries, there is not yet a proper legal framework for the use of body scanners. Air Transportation agencies self-regulations are not binding and could be changed at any moment (and without any obligation to inform citizens) at the discretion of each national agency. Modesty filters, privacy algorithms, built-in restrictions that prevent printing, transmitting and circulating WBI images are not legally mandated in any EU country. There are no agreed international standards concerning WBI and no WBI technology is certified. [1]

KEY MESSAGE TO POLICY MAKERS

If we want to implement trusted body scanners, we should define a legal framework and describe attributes, capabilities, characteristics and qualities which allow users to verify whether the systems are trustworthy. This should be substantiated in appropriate standards and certification procedures. If WBI has to be implemented, European standards and certifications must be developed as soon as possible.

Regular Review

68. A regular review of the rationale which justifies the use of WBI technologies is advisable, also as per Regulation (EC) No 300/2008, which states that "Member States should also be allowed, on the basis of a risk assessment, to apply more stringent measures than those laid down in this Regulation". This implies a regular review of the proportionality between body scanner screening and airport security needs (i.e., the actual risk for passengers). Yet it is questionable whether a public and reliable risk assessment of the proportionality principle[2] is ever possible in a sensitive field such as aviation security.

1 The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Guide 2:2004 defines a standard as "*a document, established by consensus that provides rules, guidelines or characteristics for activities or their results*." Standards play a role in everyday life by establishing the size, configuration, or protocol of a product, process, or system. Standards also define terms so that there is no misunderstanding among those using the standards. They enable development of integrated, scalable, system solutions.

2 Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

KEY MESSAGE TO POLICY MAKERS

Reviews of WBI technologies and the rationale which justifies their use, notably as far as the proportionality principle is concerned, must be carried out on regular basis. Citizens input during the system application phase should also be part of the total review system. Although specific contents of these reviews could be partly restricted, review results should always be public.

WBI operating procedures

69. Control of people who enter the airport sterile area[3] is the primary task of airport checkpoints. A secondary task is to ensure that people who have been cleared remain cleared before boarding their aircraft. Primary screening methods are those used for controlling all people who want to enter the sterile area. Secondary methods are those used only for some selected groups in addition to primary screening. The issue of whether WBI should be a primary or as secondary screening method is extremely political and ethically sensitive. If WBI is intended as a primary method, it means that we create an intermediate level, between pat-down and strip search, which becomes routine. In other words we "upgrade" the level of intrusiveness of standard security checks. Reading governmental documents, official and unofficial statements, reports and parliamentary hearings, it is unclear what the actual plans are. Yet two points are probably out of discussion, 1) for now WBI is not going to substitute hand search, as it is demonstrated by all operating protocols, which advise further hand search if any anomaly is detected during WBI screening; 2) WBI is not going to make WTMD totally obsolete, given that WBI cannot detect objects hidden in body cavities, which could be instead sensed by metal detectors (if they are made by metal). It is then difficult to escape the impression that in the short term, WBI is destined to become an additional screening tool rather than a substitute for current procedures. This also casts doubts about whether WBI is going to expedite checkpoint procedures. Considering that people have to be offered to opt between WBI and physical search, and some of those who opted for WBI will still undergo a physical search after WBI screening, it is arguable that large scale application of WBI will ever speed up security checks.

70. There is a substantial consensus that establishing rules for body scanner operating procedures is a crucial component of their deployment. Unfortunately these details are not going to become public because of security reasons. "The impact of passenger risk uncertainty can be mitigated by designing sufficient flexibility into security operations, in terms of what procedures are used to screen varying passenger risk profiles. The pursuit of this objective requires a measure of intelligence into how passenger risk is assigned."[4] Regulation (EC) No 300/2008 states "As a general rule, the Commission should publish measures that have a direct impact on passengers. Implementing acts

3 The "sterile area" refers to portions of an airport that provides passengers access to boarding aircraft and to which the access is controlled. People who enter sterile area include passengers, flight crew members, and airport personnel, employed by the airport, air carriers, or by companies, that conduct business in airports.

4 Nikolaev AG, Jacobson SH, Lee J, (2009) Designing for flexibility in aviation security systems *J Transp Secur* n2:1–8

setting out common measures and procedures for the implementation of the common basic standards on aviation security which contain sensitive security information, together with Commission inspection reports and the answers of the appropriate authorities should be regarded as EU classified information". Does WBI operating procedures contain sensitive security information? The UK Department for Transportation wrote that "body scanners must be operated in accordance with detailed protocols which contain the security sensitive information on the operation of the body scanner including selection criteria for those to be scanned. The details of the protocol are not published due to the security sensitive content but will comply with the requirements contained in this interim Code of Practice."[5]

71. On the other hand, WBI Standard Operating Procedures may determine the overall degree of democratic acceptability of the whole system. On 8 Dec 2009, the Washington Post revealed that the TSA inadvertently posted online its operating manual for screening passengers. The manual, which was immediately obscured by the TSA but which is still readable online,[6] reveals "technical settings used by X-ray machines and explosives detectors. It also includes pictures of credentials used by members of Congress, CIA employees and federal air marshals, and it identifies 12 countries whose passport holders are automatically subjected to added scrutiny".[7] Some of these details should be considered security sensitive (e.g., body scanner setting) , yet most of them were politically and ethically sensitive. For instance the manual listed criteria to be adopted for selecting people who should undergo to WBI screening. Passengers holding passports from, or taking flights that originated in or passed through, Cuba, Iran, Sudan and Syria, Afghanistan, Algeria, Lebanon, Libya, Iraq, Nigeria, Pakistan, Saudi Arabia, Somalia, and Yemen, have to pass through body scanners or to be physically searched. Singling out travellers from a few specified countries for enhanced screening is not a technical setting, but it is a, very arguable, political decision.

72. As pointed out by the Art.29 WP and EDPS joint reply to the EC public consultation on body scanners[8], "excluding some individuals from the screening, whatever the reason (just as giving a choice to the individual), puts into question the real necessity of the system". Moreover it is highly questionable that it could be ever ethically acceptable that certain categories of travelers (because of their nationality, their ethnicity, or religious beliefs) would have to go routinely through WBI or full physical search. This would be in contrast with Chapter III of the EU Charter, which deals with the prohibition of any discrimination (art. 21), and the respect of cultural, religious and linguistic diversity (art. 22).

73. A similar principle is also affirmed in the Commission's ***Green Paper on detection technologies in the work of law enforcement, customs and other security authorities***[9], which

5 UK Dept. for Transport, *Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology in an Aviation Security Environment*, www.dft.gov.uk/pgr/security/aviation/airport/

6 http://boardingarea.com/blogs/thewanderingaramean/2009/12/the-tsa-makes-another-stupid-move/

7 http://www.washingtonpost.com/wp-dyn/content/article/2009/12/08/AR2009120803206.html?hpid=topnews

8 The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection, http://ec.europa.euijusticehome/fsj/privacyiindexen.htm

9 COM(2006) 474 final

states that "policies relating to detection and associated technologies have to comply in full with the existing legal framework, including the EU Charter of Fundamental Rights, the European Convention on Human Rights and data protection principles and rules as laid down in Directive 95/46/EC. In this context, the Commission stresses that the design, manufacture and use of detection technologies and associated technologies, together with legislation or other measures aiming to regulate or promote them, must fully comply with Fundamental Rights as provided for in the EU Charter of Fundamental Rights and the European Convention on Human Rights"[10]

KEY MESSAGE TO POLICY MAKERS

Selective screening procedures are hardly consistent with fundamental rights and should be avoided. We welcome the EDPS and Art.29 WP suggestion that the body scanner screening should be universal, say, no specific subgroup of travellers should be targeted or exempted on the basis of considerations about nationality, race, ethnicity, religion, gender, and age. Yet we understand that specific security conditions could oblige to the selection of specific categories of people for body scanner screening. Such a procedure should be always be convincingly justified and should be temporary.

74. Identifying individuals who should undergo to WBI also raises serious questions in relation to civil liberties, also because of the intersection between migration management and aviation security. Selection criteria are very politically sensitive details, which allow to evaluate the consistency of WBI systems with fundamental human rights and democratic rules. As solemnly affirmed by the Berlin Declaration "In the European Union, we are turning our common ideals into reality: for us, the individual is paramount. His dignity is inviolable. His rights are inalienable [...] We will fight terrorism, organised crime and illegal immigration together. We stand up for liberties and civil rights also in the struggle against those who oppose them".[11]

The airport as a total institution

75. A quite neglected aspect of body scanners is their "symbolic" function in the whole security airport apparatus. This is not a minor issue. Airports share several features with the so-called "total institutions". This is a term used by social scientists to describe an "institution where all parts of life of individuals under the institution are subordinated to and dependent upon the authorities of the organization. Total institutions are social microcosms dictated by hegemony and clear hierarchy [...]A place of residence and work where a large number of like-situated individuals, cut off from the wider society for an appreciable period of time together, lead an enclosed, formally administered round of life"[12] In the standard sociological account total institutions include boarding schools, concentration camps, colleges, cults, prisons, mental institutions, sailing ships, boot camps, monasteries, convents, nursing homes, and orphanages.

10 Ibid.

11 Declaration on the occasion of the fiftieth anniversary of the signature of the Treaties of Rome, http://www.eu2007.de/en/About_the_EU/Constitutional_Treaty/BerlinerErklaerung.html

12 Goffman E (1961), Asylums. Essays on the social situation of mental patients and other inmates Anchor Books, Doubleday & Company, Inc., New York

76. As some scholars have noticed,[13] airports are very close to total institutions. Airports are self-contained structures, with health clinics, religious sites, entertainment, hospitality, police power, and so on. People who enter the security area are segregated (at least for the period of time in which they stay in this area). Interestingly enough stripping processes are a peculiar feature of all total institutions (be they colleges, hospitals, prisons, barracks). Personal identity equipment is removed, as well as other possessions with which the inmate may have identified himself. Such a strip is a "rite of passage", which marks the entrance into the total institution through a mortification of the person (etymologically mortification means to turn someone into a corpse). At symbolic level what happens with body scanners at airport check-points is that "people are stripped of their status as honest citizens and treated like potential criminals. This is more evident in those airports in which operators are a bit rude and the whole screening procedure is carried out in almost-military manner."[14] Body scanner "virtual strip" could progressively turn into a "symbolic strip" which figuratively deprives the person of his "global citizenship rights", in other words while we claim to protect universal rights, we run the risk to deny them with our security practices.

13 Salter MB, Adey P, (2008), *Politics at the Airport,* Minnesota UP

14 Salter MB, Adey P, (2008), ibid.

CHAPTER 7: Conclusions

77. **WE BELIEVE** that the primary aim of security is to safeguard the human person in his or her physical, mental, and social integrity. Respect for human dignity, body integrity and privacy (both physical and informational) are thus essential components of any security policy. Security measures which impair human integrity of those which should be protected are self-contradictory and eventually are also less effective. The primary purpose of WBI technology and systems is only to detect prohibited items concealed on the body. We think that WBI is legitimate as far as it fulfils its original purpose. Any different goal, like people identification or profiling, or detection of anatomic and/or medical details, is not legitimate and is not respectful of personal integrity.

78. **WE ARE CONCERNED** that body scanners could humiliate people by unravelling anatomic and/or medical details, and by hurting their feelings of modesty. We are concerned by the lack of clarity about WBI operating procedures, and by confusion and inconsistencies about primary and secondary screenings, voluntariness and compulsion. We are also concerned that body scanners can be used to discriminate against certain groups of travellers. In other words we are concerned that WBI technologies and systems can be (mis)used for wider purposes than the detection of concealed objects.

79. **WE REGARD** the European Charter of Fundamental Rights as the general framework for the introduction in the EU of new technologies for passenger screening and aviation security.

80. **WE RECOMMEND** that respect for the primacy of the human person and attention to his or her needs are the leading principles followed in the establishment of aviation security. We also recommend that the European Commission should propose a specific framework for detection, profiling, and identification technologies for aviation security. We recommend that WBI operating procedures should be subject to a public, democratic, scrutiny. Appropriate exemptions can be provided only for those parts of SOP manuals which directly deal with technically sensitive details. We finally recommend that the European Commission should encourage the use of codes of practice and ethical codes at MS level, and promote the establishment of a system of complaints and remedies at EU level.

81. **WE WELCOME** the regular use of privacy enhancing and "privacy-by-design" technologies in WBI system design. We also recommend that technologies should be selected and systems should be designed in order to make practically impossible to fulfil illegitimate purposes. We recommend that the European Commission, in conjunction with the European Data Protection Supervisor and the Art.29 Working Party, promote independent, publicly available, Privacy Impact Assessments (PIAs) prior to the adoption of any new WBI technology and system.

82. **WE URGE** the European Commission to commit to a plan of action to promote further research on ethical, legal, and social implications (ELSI) of technologies for aviation security, their likely effect on public trust and their communicational and symbolic dimensions. In particular we recommend that the European Commission and the European Parliament promote the adoption of an ethical framework for trials with new WBI technologies.

Acknowledgments

CSSC gratefully acknowledges HIDE and RISE consortia for their contribution to this document, and the following reviewers for their effective assistance in improving the quality of this report:

Kamlesh Bajaj, Data Security Council of India (INDIA)

Alessandro Caloprisco, Italian Data Protection Authority (ITALY)

Nigel Cameron, Centre for Policy on Emerging Technologies (USA)

Alastair V. Campbell, National University of Singapore (SINGAPORE)

Chi-Shing Chen, National Cheng-Chi University (TAIWAN)

Frediano Maria Di Carlo, Elsag Datamat SPA (ITALY)

Simon Dobrisek, University of Ljubljana (SLOVENIA)

Juliet Lodge, University of Leeds (UK)

Ajay Kumar, The Hong Kong Polytechnic University (HONG KONG)

Niovi Pavlidou, Aristotle University of Thessaloniki (GREECE)

Max Snijder, European Biometric Forum, (IRELAND)

Kush Wadhwa, Global Security Intelligence (USA)

David Zhang, The Hong Kong Polytechnic University (HONG KONG)

Steven W. Smith, President of Tek84 Engineering Group LLC (San Diego, CA), and developer of the first X-ray backscatter, kindly reviewed the report. A few points of disagreement with Steven have been indicated in the footnote.

A special thanks also to Prof. **Irma van der Ploeg** (Zuyd University, THE NETHERLANDS) who participated in the writing of an early version of this report.

Dr **Rene von Schomberg** (European Commission, DG Research, Ethics and Governance) was the DG RTD contact point for this report.

ANNEX II:
Note on authors and projects

Introduction

René von Schomberg is an agricultural scientist and philosopher. He holds Ph.D's from the University of Twente (NL) (Science and Technology Studies) and J.W.Goethe University in Frankfurt (Philosophy). He has been a European Union Fellow at George Mason University, USA in 2007 and has been with the European Commission since 1998. He is author/co-editor of 12 books, most recently: Implementing the Precautionary Principle, Perspectives and Prospects, co-edited with E. Fisher and J. Jones, E.Elgar Publishers, 2006 and Understanding Public Debate on Nanotechnologies. Options for Framing Public Policy, co-edited with Sarah Davies, Publication Office of the European Union, 2010

Chapter 1

Bern Carsten Stahl is Professor of Critical Research in Technology and Director of the Centre for Computing and Social Responsibility,which is one of the research groups of the Department of Informatics of the Faculty of Technology at De Montfort University, UK
He is project coordinator of
ETICA project: Website: http://www.etica-project.eu/

Chapter 2

Walter Peissl (ITA/ÖAW) is Deputy Director at the Institute for Technology Assessment (ITA), in Vienna, Austria.
Projects PRISE: http://prise.oeaw.ac.at and EUROPRISE: https://www.european-privacy-seal.eu/

Chapter 3

Stephen Rainey and Philippe Goujon are at the Computer Departement, Faculté d'Informatique, FUNDP, of the University of Namur, Belgium
Stephen Rainey and Philippe Goujon are partners to the projects
Project EGAIS: http://www.egais-project.eu/
Project ETICA: http://www.etica-project.eu/

Chapter 4

Kjetil Rommetveit is at Centre for the Study of the Sciences and the Humanities University of Bergen, and coordinator of the
Project TECHNOLIFE: http://www.technolife.no/

Chapter 5

David Wright is at Trilateral Research & Consulting, London, UK
Raphaël Gellert and Serge Gutwirth are at the Vrije Uniersiteit Brussels, Belgium
Michael Friedewald is at Fraunhofer Institute for Systems and Innovation Research, Karlsruhe, Germany
Project: PRESCIENT (Privacy and Emerging Sciences and Technologies):
http://www.prescient-project.eu/prescient/index.php

Chapter 6

Daniel Guagnin, Leon Hempel and Carla Ilten are at Center for Technology and Society at the Technical University of Berlin and coordinators of the
PATS project: http://www.pats-project.eu/

Chapter 7

Zaharya Menevidis, is at Fraunhofer-Institute for Production Systems and Design Technology IPK, in Berlin and coordinator of the ETHICAL project
Samantha Swartzman is at Imperial College London Business School, Healthcare Management Group, London, UK
Efstratios Stylianidis is at GeoImaging Ltd in Cyprus
Project ETHICAL: http://www.ethical-fp7.eu/

Chapter 8

Aharon Hauptman, Yair Sharan and Tal Soffer are at The Interdisciplinary Center for Technology Analysis and Forecasting at Tel-Aviv University. They authored the article with contributions of the PRACTIS consortium partners (www.practis.org) from which they are the coordinator

Chapter 9

Maggie Mort is at the Department of Sociology/Division of Medicine, Lancaster University UK, *Celia Roberts* Department of Sociology Lancaster University UK and *Christine Milligan* is at the Division of Health Research Lancaster University, UK . They acknowledge contributions from: Josephine Baxter, Elham Kashefi, Miquel Domenech; Blanca Callen, Daniel Lopez, Tomas Sanchez Criado, Ingunn Moser, Hilde Thygesen, Jeannette Pols and Dick Willems.
Project: EFORTT: http://www.lancs.ac.uk/efortt/index.html

ANNEX I

Emilio Mordini is at the Centre for Science, Society and Citenship (CSSC) in Rome. He is coordinator of the
Project RISE: http://www.riseproject.eu/
Project HIDE: http://www.hideproject.org/

ANNEX III: Agenda workshop in the European Parliament

WORKSHOP

Governance and Ethics of Emerging ICT and Security Technologies

18 November 2010

Europan Parliament

Rue Wiertz
Altiero Spinelli

(Meeting room A1H-1)

AGENDA

18 November (a.m.)

09:00-09:15 ***Welcome coffee***

Signature of attendance list and collection of reimbursement file

09:15-09:30 **Welcome and Introduction to workshop**

Jorgo Chatzimarkakis, MEP/STOA Panel

09:30-10:15 ***Session 1***

Interaction between ICT & Human Practices: promoting user involvement

- Kjetil Rommetveit: Technolife
- Guido van Steendam: ICT-Ethics
- Maggie Mort: EFORTT

10:15-10:30 Pēteris Zilgalvis (DG INFSO)

Responses from DG INFSO

10:30-11:00 **Round Table Debate**

11:00-11:15 ***Coffee break***

11:15-12:00 ***Session 2***

International Data Sharing: Ethical Challenges of Biometrics and medical applications

- Emilio Mordini: HIDE and RISE
- Zaharya Menevidis: ETHICAL
- James Peter Burgess: Biometric personhood

12:00-12:15 Francis Pēteris Svilans (DG JUST)
Response from DG JUSTICE (Data protection, Fundamental rights and citizenship)

12:15-12:45 **Round table Debate**

12:45-13:45 ***Lunch***

18 November (p.m.)

13:45-14:00 *Signature of attendance list and collection of reimbursement file*

14:15-15:00 ***Session 3***
Privacy as a fundamental right (EU Charter) and (privacy) assessment methodologies

- Bernd Carsten Stahl: ETICA
- Yair Sharan: PRACTIS
- Leon Hempel: PATS

15:00-15:15 Maria-Eva Engdahl (DG ENTR)
Response from DG ENTERPRISE

15:15-15:45 **Round Table Debate with MEP, Silvia Adriana Ticau**

15:45-16:00 ***Coffee break***

16:00-16:15 Prabhat Agarwal (DG INFSO)
Perspectives from DG INFSO: research and policy needs

16:15 -16:30 Round Table debate continued

16:30-17:00 **Round Table Debate on "Responsible Innovation"**

17:00-17:15 **Outlook to workshop Future Technology and Society on 19 November**
Prabhat Agarwal (DG INFSO); René von Schomberg (DG RTD)

European Commission

Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields

Luxembourg: Publications Office of the European Union

2011 – 217 pp. – 17.6 x 25.0 cm

ISBN 978-92-79-20404-3
ISSN 1018-5593
doi: 10.2777/58723

This publication, introduced and edited by René von Schomberg, consists of a series of research articles reflecting on how to proceed towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technology fields.

The authors who contributed to this publication are coordinators or participants to major FP7 projects funded under the Science in Society Programme. A total of 10 projects have inspired the authors to reflect and address various governance and ethics issues underlying the responsible development of these new technologies.

A deliberative approach to the responsible development of these technologies implies inclusive governance, based on broad stakeholder involvement, public debate and early societal intervention in research and innovation, among other, by means of ethics assessments and various technology and privacy impact assessments.

KI-NA-24835-EN-C

ISBN 978-92-79-20404-3

Publications Office