Project acronym:	PRESCIENT
Project title:	Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment
Project number:	244779
Programme:	Seventh Framework Programme for research and technological development
Objective:	SiS-2009-1.1.2.1: Privacy and emerging fields of science and technology: ethical, social and legal aspects.
Contract type:	Collaborative project
Start date of project:	1 January 2010
Duration:	39 months

Deliverable 4:
Final Report — A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies

Editors:	Silvia Venier, Emilio Mordini (CSSC)
Contributors:	Michael Friedewald, Philip Schütz, Dara Hallinan (Fraunhofer ISI), David Wright, Rachel L. Finn (Trilateral Research & Consulting), Serge Gutwirth, Raphaël Gellert (VUB-LSTS), Silvia Venier, Bruno Turnheim, Emilio Mordini (CSSC)
Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due date:	30 October 2012
Submission date:	25 March 2013

Terms of use

This document was developed within the PRESCIENT project, co-funded by the European Commission within the Seventh Framework Programme (FP7), by a consortium, consisting of the following partners:

- Fraunhofer Institute for Systems and Innovation Research (co-ordinator),
- Trilateral Research & Consulting LLP,
- Centre for Science, Society and Citizenship, and
- Vrije Universiteit Brussel

Suggested citation: Venier, Silvia, Emilio Mordini, Michael Friedewald, Philip Schütz, Dara Hallinan, David Wright, Rachel L. Finn, Serge Gutwirth, Raphaël Gellert, and Bruno Turnheim, "Final Report – A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies", Deliverable 4, PRESCIENT Project, 25 March 2013. http://www.prescient-project.eu

Contents

Executive Summary

The PRESCIENT[1] project aimed at providing an extended understanding of privacy embracing different approaches and at providing policy-makers and researchers with a *tool* by means of which not only privacy and data protection risks, but also *ethical* issues related to the design, development and use of emerging technologies can be identified and addressed early on.

The PRESCIENT framework is modelled along the structure of the recently proposed Privacy Impact Assessment Frameworks (PIAs). The idea is to broaden this model to include also *ethical* issues (Privacy and Ethical Impact Assessment, P+EIA), beyond data protection and privacy aspects. The framework proposed by PRESCIENT is based on an integration of the results of research carried out throughout the project's lifecycle (that has been based on four main stages, namely *Analysis* - Stage 1, *Case Studies* - Stage 2, *Citizens* - Stage 3 and *New Framework* - Stage 4), and on current available privacy impact assessment guidelines (such as those of the UK). The main aims of this deliverable are:

- to present the results of the research carried out in the previous stages of the project that have been relevant for the development of the framework;
- to describe the process of developing the framework through the elaboration of scenarios, to fit it into the European Union legal environment, and to discuss some key philosophical and methodological challenges of conducting such exercise;
- to present PRESCIENT framework and to provide some considerations about engaging relevant stakeholders.

To this end, the deliverable is structured in three parts.

The first part (**Chapter 2, PRESCIENT Multidisciplinary approach**) discusses the findings of the previous stages 1, 2, and 3, which have been relevant to the development of the framework.

- ***Section 2.1*** focuses on the outcomes of Stage 1, *Analysis*, which explored the added value of dealing with privacy from a multi-disciplinary perspective. Four dimensions of privacy have been considered: the legal, economical, ethical and social. In addition, at this stage partners also made clear the differences between the concepts of privacy and data protection, and reflected on the (often unhelpful and misguided) use of the "balancing metaphor" between privacy and other rights. As the main outcome of Stage 1, in PRESCIENT D1[2] ***a classification of seven types of privacy*** was also provided.
- ***Section 2.2*** focuses on the outcomes of Stage 2, *Case Studies*, exploring the need to identify ethical and privacy issues in concrete examples. The five case studies included RFID (specifically in travel cards and passports), new surveillance technologies (body scanners and drones), second-generation biometrics, next generation DNA sequencing technologies, and technologies for human enhancement[3]. The ***case studies demonstrate that these new technologies impact upon multiple types of privacy and raise ethical and social issues***. In addition, the case studies show that as technologies develop and proliferate, various types of privacy which had not previously been under threat may now be compromised. Therefore, when new technologies are planned and developed, the

[1] PRESCIENT is an FP7 research project funded under the scope of the Science-in-Society theme. The acronym stands for "Privacy and Emerging Fields of Science and Technology: towards a common framework for privacy and ethical impact assessment". For more information, see also the project's website at http://www.prescient-project.eu

[2] See Gutwirth, Serge, Raphaël Gellert, Rocco Bellanova, Michael Friedewald, Philip Schütz, David Wright, Emilio Mordini, and Silvia Venier, "Legal, social, economic and ethical conceptualisations of privacy and data protection", Deliverable 1, PRESCIENT Project, 23 March 2011.

[3] See Finn, Rachel L., David Wright, Michael Friedewald, Raphaël Gellert, Serge Gutwirth, Bärbel Hüsing, Piret Kukk, Emilio Mordini, Philip Schütz, and Silvia Venier, "Privacy, data protection and ethical issues in new and emerging technologies: Five case studies", Deliverable 2, PRESCIENT Project, 27 November 2011.

developers need to consider all of the ways in which a new technology may impact upon privacy, without exclusively relying upon a check-list approach that may not capture all types of privacy.

- ***Section 2.3*** focuses on the findings of Stage 3, *Citizens*, which aimed at ***understanding whether the European citizens have sufficient knowledge on the personal data being processed and can easily access and modify this information***. Our analysis was carried out with a view on three stakeholders categories: *Data Controllers* (dealing whit the question of to what extent can European citizens have access to the personal information and are they are able to correct information and can find out how their information is being used); *Data Protection Authorities* (DPAs, exploring what role DPAs play in reconciling the rights and interests of data subjects and data controllers); and *Citizens* (considering citizens' concerns and apprehensions about new data collection technologies and regarding data storage and use). The results of this research are comprehensively discussed in PRESCIENT D3[4].

The second part of this deliverable describes the results of the activities carried out in the last stage of the project (Stage 4), and in particular of those activities that provided crucial information for the development of the framework. These activities consisted in:

- the *elaboration of a set of scenarios to explore potential ethical and privacy issues of emerging technologies*, which are presented in **Chapter 3** (**Scenarios**). Chapter 3 provides a comparative ***analysis of the ethical dilemmas as well as data protection and privacy risks*** that arise from the five different scenarios developed by partners, which aimed at informing the Privacy and Ethical Impact Assessment Framework.
- the *analysis of the evolving European Union (EU) legal framework*, which is discussed in **Chapter 4** (**Key provisions in EU data protection and privacy legislation related to privacy and ethical impact assessment**) fleshes out the different provisions relating to privacy and ethical impact assessment that can be derived from the EU legal framework. The description of the EU legal framework evidences the fact that the only references to PIAs are to be found in data protection provisions. The chapter concludes by speculating on whether it is reasonable to expect meaningful (privacy) protection from (yet another) data protection instrument.
- the *organisation of a workshop* on "New directions in ethical impact assessment of emerging technologies" (Rome, 20th and 21st September 2012) *aiming at discussing the key philosophical and methodological challenges in conducting such exercises.* **Chapter 5** (**Current Approaches to Privacy and Ethical Impact Assessment: philosophical and methodological challenges**) includes an overview on contemporary approaches to privacy and ethical impact assessment of emerging technologies and seeks to outline the main opportunities and challenges of this methodology (such as, for instance, the need to consider that technological innovation happens under uncertain and complex circumstances, and that technology ethics is a relatively young field of research).

In the third part of this document, **Chapter 6** (**PRESCIENT Privacy and Ethical Impact Assessment Framework**), the new framework is presented, and a few considerations on how to engage stakeholders are also provided. PRESCIENT partners have envisaged a P+EIA process comprising 16 principal steps (*P+EIA process*). Depending on the perceived privacy and/or ethical risks, it may not be necessary for an organisation to follow all of these steps and some may follow them in variations of the sequence set out here. If the privacy or ethical risk is regarded as relatively trivial, affecting only a few people, it may not be necessary to follow all of the steps. The P+EIA *process* should always be distinguished from a P+EIA *report*. Production of a report is only part of the process, which continues even after the assessor has finished

[4] See Friedewald, Michael, Dara Hallinan, Raphaël Gellert, Serge Gutwirth, Silvia Venier, Emilio Mordini, and David Wright, "Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data", Deliverable 3, PRESCIENT Project, 16 May 2012.

writing the report. Although the 16 steps are those recommended in the PIAF project[5], we have adapted them here to take into account any *ethical* and/or *societal* impacts raised by a project, emerging technology, new service, programme, legislation or whatever. Hence, we have produced a P+EIA, a privacy and ethical impact assessment framework.

[5] PIAF project, A Privacy Impact Assessment Framework for data protection and privacy rights. http://www.piafproject.eu/

1. Introduction

The PRESCIENT[6] project aimed at providing an extended understanding of privacy embracing different approaches and at providing policy-makers and researchers with a *tool* by means of which not only privacy and data protection risks, but also *ethical* issues related to the design, development and use of emerging technologies can be identified and addressed early on.

The PRESCIENT framework is modelled along the structure of the recently proposed Privacy Impact Assessment Frameworks (PIAs). PIAs can be defined as a

a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. A PIA is more than a tool: it is a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after the project has been deployed.[7]

Although PIAs have been around for more than a decade in a few other countries, they have only recently been introduced in Europe. The idea of PRESCIENT is to broaden this model to include also *ethical* issues (Privacy and Ethical Impact Assessment, P+EIA), beyond data protection and privacy aspects. Used in tandem with “ethical impact assessment”, PIAs could come to terms with a lack of public and stakeholder knowledge about new technologies and their ethical implications, before technologies are widely developed.

The framework proposed by PRESCIENT is based on an integration of the results of research carried out throughout the project’s lifecycle (that has been based on four main stages, namely *Analysis* - Stage 1, *Case Studies* - Stage 2, *Citizens* - Stage 3 and *New Framework* - Stage 4), and on current available privacy impact assessment guidelines (such as those of the UK).

The main aims of this deliverable are:

- to present the results of the research carried out in the previous stages of the project that have been relevant for the development of the framework;
- to describe the process of developing the framework through the elaboration of scenarios, to fit it into the European Union legal environment, and to discuss some key philosophical and methodological challenges of conducting such exercise;
- to present the PRESCIENT framework and to provide some considerations about engaging relevant stakeholders.

In line with these goals, the deliverable is structured in three parts.

The first part is devoted to the analysis of the key outcomes of the research carried out in the scope of the previous tasks of the project (Stages 1, 2, 3), which represent the basis upon which PRESCIENT framework has been developed. **Chapter 2 – PRESCIENT Multidisciplinary Approach** discusses these findings in three sections, particularly aiming at pointing out how the previous research has been relevant for the development of the framework. Section 2.1 focuses on the outcomes of Stage 1, *Analysis*, which explored the added value of dealing with privacy from a multi-disciplinary perspective. Four dimensions of privacy have been considered: the legal, economical, ethical and social. In addition, at this stage, partners also made clear the differences between the concepts of privacy and data protection, and reflected on the (often unhelpful and misguided) use of the “balancing metaphor” between privacy and other rights. As the main outcome of Stage 1, in PRESCIENT D1, a classification of **seven types of privacy** was also provided. Section 2.2 focuses on

[6] PRESCIENT is an FP7 research project funded under the scope of the Science-in-Society theme. The acronym stands for “Privacy and Emerging Fields of Science and Technology: towards a common framework for privacy and ethical impact assessment”. For more information, see also the project’s website at http://www.prescient-project.eu

[7] Wright, David, “The state of the art in privacy impact assessment”, *Computer Law & Security Review*, Vol. 28, No. 1, Feb. 2012, pp. 54-61 [p. 55].

the outcomes of Stage 2, *Case Studies*, exploring the need to identify ethical and privacy issues in concrete examples. The five case studies included RFID (specifically in travel cards and passports), new surveillance technologies (body scanners and drones), second-generation biometrics, next generation DNA sequencing technologies, and technologies for human enhancement. The case studies demonstrate that these new technologies impact upon multiple types of privacy and raise ethical and social issues. In addition, the case studies show that as technologies develop and proliferate, various types of privacy which had not previously been under threat may now be compromised. Finally, section 2.3 focuses on the findings of Stage 3, *Citizens*, which aimed at understanding whether European citizens have sufficient knowledge of the personal data being processed and can easily access and modify this information.

The second part of this deliverable deals with the preliminary research carried out in Stage 4 – *New Framework*, and in particular of those activities that provided crucial information for the development of the framework.

First, building on the findings from the case studies (as described in section 2.2 of Chapter 2), the partners were tasked with developing scenarios highlighting the privacy and ethical issues that might arise with emerging technologies and, in particular, the ethical dilemmas. **Chapter 3 – Scenarios** describes the process by which the partners created the five ethical dilemma scenarios and provides a comparative analysis of the ethical dilemmas as well as data protection and privacy risks that arise from the different scenarios. The PRESCIENT partners advocate "What-if" scenarios, such as those set out in this report, as a useful tool in identifying privacy and ethical issues arising from the development and deployment of new and emerging technologies. Scenarios are a useful tool in drawing to the attention of policy-makers and decision-makers as well as other stakeholders some of the issues that could arise in future. They are intended to provoke discussion and, with luck, debate among stakeholders will lead to consensus on how to address the issues highlighted in the scenarios – but also to be alert to other issues that might arise too. PRESCIENT scenarios were particularly aimed at informing the development of the project's Privacy and Ethical Impact Assessment Framework. In most, but not all of the scenarios, a P+EIA will be useful to address not only the privacy issues, but also the ethical issues. The qualification of "most, but not all" depends on the fact that some of the technologies and/or applications mentioned in the scenarios are already fully formed. If the use of P+EIA is introduced even earlier than the timeframe of the scenarios, i.e., when the technologies or applications are still being considered, the P+EIA instrument will have greater value because it could, theoretically, be used to influence the design or even use of particular technologies and applications.

Second, partners analysed the European Union legal environment targeting privacy and data protection impact assessment exercises. **Chapter 4 – Key provisions in EU data protection and privacy legislation related to privacy and ethical impact assessment** fleshes out the different provisions relating to privacy and ethical impact assessment that can be derived from the EU legal framework. The description of the EU legal framework evidences the fact that the only references to PIAs are to be found in data protection provisions. We have then tried to analyse this pattern by drawing from the human rights conceptual differentiation between positive and negative obligations, as developed by the European Court of Human Rights, with the right to privacy drawing predominantly on negative obligations, and the right to data protection embedded into positive obligations. Pursuant to this analysis, we have purported that PIAs represent such positive obligations, which might account for its presence within data protection instruments. This stance is confirmed to the extent that the European Commission's proposal for a general data protection regulation not only includes a provision dedicated to PIAs, but even goes so far as renaming them into data protection impact assessments (DPIAs). The chapter concludes by speculating on whether it is reasonable to expect meaningful (privacy) protection from (yet another) data protection instrument.

Third, partners decided to broaden the discussion on the key methodological and philosophical challenges in including ethical values in PIAs. A workshop was organised in Rome in September 2012 to investigate the theoretical discussion around the notions behind the development of a P+EIA with a groups of experts in ethics. **Chapter 5 – Current Approaches to Privacy and Ethical Impact Assessment: philosophical and methodological challenges** first introduces the context by discussing current efforts made at the European Union (EU) level towards the reconciliation of technological innovation and ethical values. In relation to the often perceived tension between innovation and values/rights, we argue that whether "constraints" of any kind – included those generated by ethics – are either a barrier to innovation or a support depends on a number of factors, the most important being governance. Good innovation governance interprets constraints as frameworks, which do not drive, or even prevent, innovation but only provide a structured context within which innovators are free to experiment with new and original solutions. The chapter then discusses difficulties in clearly understanding the role of ethics in the description and evaluation of emerging technologies. This is due to different sets of reasons, the most important being that technological innovation is happening under uncertain and very complex conditions. A short historical overview of the development of the field of technology ethics is then provided, trying to pointing out that this is a recent field of research, and that better informed and more proactive ethics is needed in order to having the theoretical and methodological tools to evaluate emerging technologies from a normative perspective. In the following sections of Chapter 5, an overview and a critical reflection of contemporary quantitative approaches to technological risk assessment, privacy impact assessment, and ethical assessment methodologies are also presented. Finally, the last section is concerned with summarising some philosophical and methodological challenges in conducting such exercises.

In the third part of this document, **Chapter 6 – PRESCIENT Privacy and Ethical Impact Assessment Framework,** the new framework is presented, and a few considerations on how to engage stakeholders are also provided. PRESCIENT partners have envisaged a P+EIA process comprising 16 principal steps (*P+EIA process*). Depending on the perceived privacy and/or ethical risks, it may not be necessary for an organisation to follow all of these steps and some may follow them in variations of the sequence set out here. If the privacy or ethical risk is regarded as relatively trivial, affecting only a few people, it may not be necessary to follow all of the steps. The P+EIA *process* should always be distinguished from a P+EIA *report*. Production of a report is only part of the process, which continues even after the assessor has finished writing the report. Although the 16 steps are those recommended in the PIAF project[8], we have adapted them here to take into account any *ethical* and/or *societal* impacts raised by a project, emerging technology, new service, programme, legislation or whatever. Hence, we have produced a P+EIA, a privacy and ethical impact assessment framework.

[8] PIAF project, A Privacy Impact Assessment Framework for data protection and privacy rights. http://www.piafproject.eu/

2. Privacy and ethical impacts of emerging technologies: PRESCIENT's multidisciplinary approach

This chapter describes the approach that has been followed in the scope of PRESCIENT and summarizes the key findings of research conducted in previous stages of the project which have been relevant for the development of the new framework. Previous stages of the project whose findings are briefly described in the following sections are:

- *Stage 1 – Analysis*: focusing on the multi-disciplinary approach followed in PRESCIENT to analyse the concepts of privacy and data protection from different perspectives (economical, philosophical/ethical, sociological, legal). The key findings of the research conducted in this first stage is summarised in section 2.1 below;
- *Stage 2 – Case Studies*: focusing on the comparative analysis of the main privacy, data protection and ethical issues in five case studies (RFID, New Technologies of Surveillance, Second-generation Biometrics, next generation DNA sequencing technologies, Technologies for Human Enhancement). The key outcomes of the research conducted in this second stage is summarised in section 2.2 below;
- *Stage 3 – Citizens*: focusing on the analysis of citizens' concerns and knowledge about personal data processing. The key findings of the research conducted in this third stage is summarised in section 2.3 below.

2.1 The multidisciplinary approach to the concepts of privacy and data protection

Raphael Gellert and Serge Gutwirth (Vrije Universiteit Brussels)

In the first phase of the PRESCIENT project, which resulted in PRESCIENT Deliverable D1 on *Legal, social economic, ethical conceptualisations of privacy and data protection*[9], the consortium aimed at making three main points.

The first point was to insist on the disciplinary construction of concepts of privacy and data protection. In other words, we have tried to show that – contrary to the opinion according to which there would be an essence of privacy and data protection that each discipline would try to reach as closely as possible, and which would entail that there is a unified trans-disciplinary meaning of these concepts – each discipline constructs its own understanding of the notion, which differs from one to another.

The second point was to make the difference between privacy and data protection, which -we contend- is crucial.

The third point concerns the notion of balancing between privacy and other rights, and the use of the "balancing metaphor", which the consortium contends is unhelpful and misguided.

2.1.1 Defining different disciplines

The first endeavour of PRESCIENT was to advance a specific understanding of interdisciplinarity: privacy and data protection have a disciplinary constructed character. Each discipline will construct its own notion of privacy and data protection, which may at times overlap.

Therefore, one key feature of the first deliverable D.1 was to map these differences, which we will come back to *infra* (2.1.2 and 2.1.3). However, we also insisted upon the fact that too often, an interdisciplinary approach is taken for granted, thereby assuming that it is self-evident to know what the different disciplines at stake are. We took a counter-intuitive stance by claiming that we do not know in advance how to define these disciplines and that a first welcomed step is thus to epistemologically ground the deliverable.

[9] Gutwirth et al., PRESCIENT Deliverable 1, 2011.

The *legal concepts* of privacy and data protection must be derived from the classical sources of law that bind the legal practice when it states the law through adjudication. Hence, a description of the legal construction of privacy and data protection must draw from an analysis of the pertinent case law, as it develops within the pertinent legislative framework, drawing inspiration from the interpretative and systematising work of legal scholars – the "legal authorities" or the "legal doctrine".

The *social dimension* of privacy means that privacy is important to both the individual and to society. Society can be interpreted simply as the collectivity of people living in a country or, even more broadly, living in the EU. A society is more than that, however. A society is composed of people who have some affiliation with each other, notably through some shared political, social, economic, cultural or other structures, including communications networks and virtual societies, such as the Information Society, promoted by the European Commission. A society will generally support certain shared values, such as those written into the European Charter of Fundamental Rights or the Lisbon Treaty. European society shares values such as dignity, autonomy, privacy, data protection and European solidarity.

When we speak about the social dimension of privacy, we imply an interest in understanding the value of privacy to both the individual and society. We signal an interest in understanding the value of privacy in particular societal contexts, of understanding its value in relation to other social values, such as security, free markets and private enterprise. The social dimension of privacy is concerned with issues such as the free flow of information across national borders, the personalisation of services, the ubiquity of surveillance cameras, national ID card schemes, identity theft, loss of personal data, etc.

The third discipline considered was ethics, a branch of philosophy that rationally assesses questions about morality, about issues that can be classified as good (or right) and bad (or wrong). Ethics is a philosophical enquiry about concepts involved in practical reasoning, *viz.* concepts which regard the way in which human beings choose among possible different courses of action.

The modern idea of privacy does not belong primarily to ethics. It is a term originated by social and political theory to describe what is not public business, notably, which is not business of the law and the government (whatever kind of government it is). The notion of privacy becomes an *ethical term* when it is framed in terms of right, say, the (a) right to privacy, or when it is framed in terms of good, say, (b) privacy as a value or as an (c) instrument to achieve other values (e.g., being free, flourishing, achieving some virtues, affirming his own dignity, etc). This opens three main issues, say, 1) the foundation of the notion of privacy as an ethical concept; 2) the ethical and political implications of privacy claims; and 3) ethical problems raised by emerging technologies vis-à-vis the notion of privacy, and what actions should be undertaken. Privacy is an ethically multifaceted concept, being equally a good to be achieved (both a value per se and an instrument which allows us to achieve other values) and a right. Whether privacy is conceptualized as a good or as a right, or as both, its value need to be justified; one should provide reasons which explain why privacy deserves to be achieved or/and to be protected.

Finally, the background for understanding privacy and data protection from an *economic viewpoint* is the concept of "information economics", which is a branch of (neoclassical) microeconomic theory studying how information affects economic decision-making. In our context, information economics mainly deals with two issues: information asymmetry and information goods.

2.1.2 Privacy and data protection

In this sub-section, we will show how the four disciplines differentiate between privacy and data protection, and what contrast and similarities (if any) can be evidenced.

Law distinguishes between privacy and data protection. Law understands the legal right to privacy as protecting the intimacy as well as the autonomy and self-determination of citizens, whereas data protection is seen as a legal tool that regulates the processing of personal data. Ultimately, both rights are considered as instrumental tools in order to protect the political private sphere, which hallows the autonomy and self-determination of the individual. Whereas the legal right to privacy, as an *opacity tool,* determines which actions from the government (or private parties) are deemed to be lawful in relation to citizens' autonomy, the legal right to data protection, as a *transparency tool*, surrounds such practices with transparency and autonomy safeguards.

The *social approach* to privacy often does not make the distinction between privacy and data protection. It seems to include issues that other disciplines (e.g., law, ethics) would frame in terms of data protection within privacy matters. Indeed, as a matter of fact, it appears to conceptualise privacy mainly in terms of informational control (current social practices of governments or corporations consist in the processing of huge amounts of information), and hence in terms of intimacy. However, more emancipatory dimensions are not totally absent from the social discourse (i.e., dignity, autonomy, individuality, and liberty). Interestingly, the social dimension approaches privacy both as a right (enshrined in legal tools), and as a value for society.

Economics resort to quantification in order to operate properly, and there is no exception for privacy, which is quantified as personal data. However, the notion of personal data used within this framework is broader than the legal notion of personal data.

The data protection directive only covers so-called *biographical* data, i.e., data that relate to an identified or identifiable natural person. The economical approach instead refers to personal data not only when *biographical* data are concerned, but also when any information belonging to an individual (but which doesn't necessarily lead to his/her identification) is concerned. On the other hand, another important development of economics in relation to privacy has been the further quantification of the latter, resulting with the commodification of private information and its use as currency in commercial transactions.

As explained in the previous section, *ethics* is mobilized with a view to assess (or judge from a moral viewpoint) a course of action, undertaken by an autonomous agent. In our case, ethics thus relates to actions involving the privacy of individuals. Hence, ethics often appears to be a procedural tool that provides guidelines in order to assess a selected course of action,[10] but whose scope is not about giving a substantial definition of a notion[11]. In other words, it can only assess actions relating to a pre-existing concept. Consequently, the scope of ethics lies more in trying to value the notion of privacy, rather than trying to substantiate it. Therefore, and in order to grasp this concept, ethics, as a branch of philosophy, naturally turns towards this discipline. Beyond the different taxonomies that exist, such a philosophical approach mainly associates privacy with the concepts of autonomy and intimacy. Equally, as far as data protection is concerned, ethics concern moral justifications and modalities regarding the processing of such data. Indeed, ethics envisage data protection independently from privacy, because it raises other types of issues that are independent from the ones raised by privacy related actions. The concept of data protection however, is defined according to the relevant legal instruments (as opposed to privacy, which is defined from a philosophical viewpoint).

In the above paragraphs, we described the generic disciplinary constructions of privacy and data protection. In the following lines, we will try to reflect on the contrasts and similarities of these approaches.

From a formal viewpoint, not all the disciplines give the same weight to privacy and data protection. Whereas law and ethics clearly distinguish between privacy and data protection, the same does not hold true for the social and economic approach. In a social context, data protection is subsumed to informational accounts of privacy. From an economic viewpoint, the quantification of privacy entails that it can only be thought of in terms of data, and hence, in terms of data protection.

Several contrasts and similarities can be put forward in terms of substance (i.e., what is actually meant by referring to notions of privacy and/or data protection).

[10] In terms of good or bad, i.e. morally.

[11] This is the case for normative or applied ethics. It should be noted that another branch of ethics, meta-ethics, is engaged with discussing the foundations of moral concepts (e.g. in this case, the foundations of privacy as a moral concept).

It appears that the different disciplines all seem to refer privacy in terms of either *autonomy* or *intimacy*: Privacy as intimacy and autonomy from a legal perspective; privacy as (mainly, but not only) information control from a social view-point; privacy as autonomy and intimacy from an ethical perspective; and privacy as informational control in economics.

In this sense, there is a strong similarity between the four approaches. But this similarity can be taken one step further if one thinks about the concepts of autonomy and intimacy. Ultimately, intimacy can be thought of as a form of autonomy, centred, however, around the individual. Autonomy should indeed include the possibility for one's self-development both before and away from the eyes of others. Autonomy, in the end includes the faculty to shy away from others. Such an ultimate analysis is also worth from an economical viewpoint since economically valid operations entail balanced operations in power terms, which in turn entails that a degree of autonomy be entitled to the different concerned market actors. In other words, the four disciplines at hand ultimately conceptualise privacy in terms of autonomy of the individual.

What conclusions can we draw from this? First, all four disciplines provide accounts of privacy in terms of autonomy, a notion entangled in the concepts of *self-determination* and *liberty*. So it is quite interesting to see that all of the disciplines frame privacy as entangled with liberty. Yet, and second, the switch from privacy to autonomy does not necessarily mean that the four perspectives construct the notion of autonomy in the same manner. For instance, economic autonomy might not be the same as social autonomy. However, mapping the different substantiations of privacy as autonomy would go beyond the limits of this Deliverable.

Finally, as far as data protection is concerned, there is an important convergence between law and ethics as the latter uses the legal construction of data protection. It is to be noted that in the framework of the democratic constitutional state, the aim of data protection is also to safeguard the political private sphere (though from the outset). Economics frame data protection as an equivalent to informational privacy *sensu lato*.

2.1.3 Balancing

This section will tackle the issue of balancing, that is, the manner in which each discipline makes room for privacy and other rights/values.[12]

Since privacy is not an absolute value, it must leave room for other rights and values to be upheld. Classically, and especially since the 9/11 events, privacy has been put at (great) jeopardy by the need for more security. Rather than engaging into a critical discussion on the notion and meaning of "security", the consortium has strived to provide insights on how to balance the rights of privacy and (for instance) security in a manner compatible with the architecture of the democratic constitutional state, which may precisely entail discarding the "balancing metaphor".

The notion of balancing, of making trade-offs, suggests a zero-sum game where an increase in security, for example, automatically means a reduction in privacy. It suggests that upholding one right weakens *per se* the other; that it is not possible to implement one right without infringing upon the other.

In the PRESCIENT D.1, we have pursued a critique of such a linear manner of dealing with two rights that seem, *prima facie*, in opposition. It excludes the possibility that both interests can be fostered and protected together. Such a proportionality test is doomed to weigh one interest *against* the other, and makes impossible the search of a *composition* or *reconciliation* whereby the different interests at stake are all preserved in an optimal way (which is respectful of the foundational principles of the democratic constitutional state).

[12] We use the expression "right/value" because depending on the discipline, privacy and/or data protection can be framed as a right or as a value.

Instead, we have argued for a shift from the weak proportionality tests that embody the notion of balancing to *strong(er) proportionality tests* that embody what we have coined as composition or reconciliation.

Such tests include the possibility of deciding that the restrictive measures at stake are unacceptable because they harm the essence of a fundamental right or of the constitutional order, even if it can be shown that the measures at stake are actually effective in upholding another legitimate interest. In the work of the European Court of Human Rights (ECtHR), this exercise is known as the "*necessary in a democratic state*", which is a component of the broader proportionality test. The issue at stake, then, is not a "balancing" between two values, but an answer to the questions "How much erosion of a fundamental right is compatible with the democratic constitutional state in which fundamental rights are a constitutive element?", or, "In which society do we want to live?". This entails that another aspect of a stronger proportionality test consists of an obligation to explore if there are alternative measures that allow for the realisation of the legitimate interest in a way that does not affect the fundamental rights in the same way as the proposed measure. In other words, one must try to find a way to protect and enforce both values without loss of the fundamental rights at play.

In the wake of our critical approach concerning the balancing of privacy with other values, we evidenced two additional elements.

First, we underlined a –deleterious in our opinion- trend at work in the case law of the ECtHR. Often, when the Court needs to balance privacy with other rights, it will avoid engaging in a proper balancing (be it a weak one, let alone a strong one). According to Art. 8.2 ECHR[13], an interference with privacy must meet three conditions in order to be lawful. It must be foreseen by law, respond to one of the legitimate aims listed in art. 8.2,[14] be proportionate to the aim pursued/be necessary in a democratic society. However, it appears that especially in issues concerning security and privacy, the Court acknowledges the legitimacy of the fight and the need to take effective measures against crime and terrorism, and thus applies a weak version of the proportionality test or simply avoids it.

Instead it focuses on the first condition of legality and stretches it from strict legality (i.e., the existence of a legal provision justifying the interference) to a broader notion of legality that includes conditions of accessibility of the law, of foreseeability of the measures, of accountability, and of transparency.

When it finds that one of the legality conditions is not fulfilled, it will declare the interference unlawful.[15] With this strategy, the Court carefully avoids to make the substantial, normative and prohibitive choices that are inherent to a balancing exercise. In this, it can be said that the Court favours a transparency approach that has more to do with data protection at the expense of the opacity approach that characterises privacy.

Finally, it is to be noted that data protection can also feature a balancing exercise. However, contrary to privacy the point is not to determine whether an interference (in this case epitomised by a data processing) is compatible with data protection, since data protection *by default* authorises the processing of data. Therefore, the balancing operation still concerns the conditions of legality of a processing, except that this processing is not seen any more as an interference with the right. Therefore, the balancing takes place *within* data protection and has more to do with the conditions of legality of the processing as provided for by the legislation.[16]

[13] European Convention of Human Rights, ECHR

[14] 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".

[15] It is only in the situation where all the legality conditions are fulfilled that the Court will perform a test of proportionality, though a weak one, cf. *supra*, p. 9.

[16] These conditions mainly draw from Art. 6 and 7 from the EU data protection directive, and thus concern both what counts as a legitimate processing aim, and the quality and purpose of such processing.

2.2 A comparative analysis of the main privacy, data protection and ethical issues in five case studies

David Wright (Trilateral Research & Consulting)

New and emerging technologies often raise privacy and ethical issues. In the scope of the second phase of the project's lifecycle (*Stage 2 – Case Studies*), the PRESCIENT consortium undertook several case studies of new technologies to consider the privacy and ethical issues they raised. The new technologies were considered in PRESCIENT Deliverable D2 Privacy, Data Protection and Ethical Issues in new and emerging technologies. Our five case studies[17] included RFID (specifically in travel cards and passports), new surveillance technologies (body scanners and drones), second-generation biometrics, next generation DNA sequencing technologies, and technologies for human enhancement. The following pages summarise our findings with regard to the privacy and ethical issues raised by these new technologies.

We need to emphasise here that many new technologies yield many benefits, many positive impacts. The benefits of these new technologies are not the focus of our discussion here. Hence, we recognise the risk that the reader may get a skewed view of the risks posed by these new technologies from the pages follow. Such is not our intention. Indeed, to enjoy the benefits of these new technologies, steps should be taken to address the issues and overcome the risks. This is exactly the function of a privacy and ethical impact assessment. Thus, with this caution, we invite the reader to consider the privacy and ethical issues and risks we have identified in the following pages (and there may be still others not discussed here – we don't pretend to be comprehensive).

2.2.1 Seven types of privacy

The concept of privacy was comprehensively outlined in the first deliverable of this project, where we described the legal, social, economic and ethical dimensions of privacy and data protection. As described in that document, we rely upon Clarke's four different categories of privacy – privacy of the person, privacy of personal data, privacy of personal behaviour and privacy of personal communication[18] – which we have re-worked into privacy of the person, privacy of data and image, privacy of behaviour and action and privacy of personal communication. We have further expanded these four re-worked types of privacy to also include privacy of thought and feeling, privacy of location and space and privacy of association, including group privacy in order to take account of developments in technology since Clarke identified his four types. Although these *seven types of privacy* may have some overlaps, they are discussed individually because they provide a number of different lenses through which to view the effects of case study technologies. In the following sections, we review these seven types of privacy and match them to information from the case studies.

Privacy of the person

Privacy of the person encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private. Privacy of the person is thought to be conducive to individual feelings of freedom and helps to support a healthy, well-adjusted democratic society. Four of the five case studies we examine, including (1) body scanners, (2) behavioural, physiological and soft biometrics as well as multimodal biometric systems, (3) second-generation DNA sequencing and (4) brain computer interfaces as well as neuro-enhancing pharmaceuticals all carry the potential to negatively impact upon the privacy of the person.

[17] Finn et al., PRESCIENT Deliverable 2, 2011.

[18] Clarke, Roger, "What's 'Privacy'?", *Australian Law Reform Commission Workshop*, 28 July 2006.

Body scanners impact the privacy of the person through the images of an individual's naked body, the subsequent revealing of medical information and the improper viewing of such images. Body characteristics such as size and shape of genitals or medical conditions are difficult to keep private when body imaging scanners are used, particularly without PETs such as automated imaging. These scanners may also reveal information about body functions such as colostomy bags or implants.

In relation to second-generation biometrics, bodily privacy could be impacted by the systematic collection of information that could be used for classification purposes such as behaviour, emotion or psychological state. Because of this potential for classification, the *categorisation* of individuals could become a more sensitive issue than *identification* in terms of biometrics, as second-generation biometrics may enable subjects to be characterised via biometric profiling or be used to provide a link to an existing non-biometric profile. Second-generation biometrics also involve the collection of intimate information, which carries the potential to reveal sensitive personal data, including medical data, gender, age and/or ethnicity.

Second-generation DNA sequencing also impacts on the privacy of the person through the collection of intimate information that can serve as the basis for discrimination and defamation or selection in societies – sex and sexual orientation, societally defined "race", physical and mental health, (absence of specific) talents and gifts, predisposition to aberrant behaviour, aptitude or sustainability for athleticism or employment and eligibility for health, disease or disability. This information could increase the potential for genetic discrimination by government, insurers, employers, schools, banks, and others. Furthermore, genetic data could also potentially identify a person, despite the assumption that it can be rendered anonymous. If these identities were unfolded, individuals could become vulnerable to the consequences of genetic testing ranging from un-insurability, un-employability or other discrimination or misuse. These consequences could affect the individual as well as their family members, due to the heritability of genetic information. In terms of ethics, genetic information in the form of biomarkers is increasingly used to stratify the population into subgroups. Presence or absence of such biomarkers could be used to group a person into a corresponding subgroup, irrespective of the validity of such a correlation.

Human-enhancing technologies may violate privacy of the person, both through brain-computer interfaces and neuro-enhancing pharmaceuticals. For example, someone's bodily privacy could be violated by invasive BCI technology such as deep brain stimulation (used for urgent medical purposes, e.g., treating epilepsy or Parkinson's disease), which could potentially seriously alter one's behaviour and personality. Although neuro-enhancers do not qualify as a technology capable of processing personal data, they can potentially enable the prescribing doctor to exercise control over the recipient, affecting his/her bodily privacy.

Privacy of thoughts and feelings

Our case studies also reveal that new and emerging technologies carry the potential to impact on individuals' privacy of thoughts and feelings. People have a right not to share their thoughts or feelings or to have those thoughts or feeling revealed. Individuals should have the right to think whatever they like. Such creative freedom benefits society because it relates to the balance of power between the state and the individual.[19]

Behavioural biometrics can impact privacy of thoughts and feelings through the collection of intimate information that can be used to detect suspicious behaviour or predict malintent. This introduces a concern that human feelings become technically defined and represented and that automated decisions over and about individuals may be made based upon this information. Furthermore, information from brain computer

[19] Goold, Benjamin J., "Surveillance and the political value of privacy", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009, pp. 3-6.

interfaces may be able to recognise and identify patterns that shed light on certain thoughts and feelings of the carrier.

Privacy of location and space

According to a conception of privacy of location and space, individuals have the right to go wherever they wish (within reason, the prime minister's residence or a nuclear power plant would generally be off-limits), without being tracked or monitored. This conception of privacy also includes a right to solitude and a right to privacy in spaces such as the home, the car or the office. Such a conception of privacy has social value. When citizens are free to go wherever they wish without fear of identification, monitoring or tracking, they experience a sense of living in a democracy and experiencing freedom. However, our case studies reveal that technologies such as RFID-enabled travel cards and passports, UASs, embedded biometric systems and behavioural biometrics and second-generation DNA sequencing can negatively impact privacy of location and space.

The movements of individuals with RFID-enabled travel cards and e-passports can be monitored. While this information could be useful for the individual concerned in terms of billing or payment disputes, it may also harm individuals whose location information is revealed to third parties such as police or divorce lawyers. Furthermore, such associations can be spurious in situations where individuals have swapped cards, or when cards have been lost, stolen or cloned.

UAS devices can also track people or infringe upon their conception of personal space. These surveillance devices can capture images of a person or a vehicle in public space, thereby revealing their location or their movements through public space if more than one image is captured. This information can be used to place individuals in particular places at particular times. UASs can also reveal information about private spaces such as back yards or, when flying low, can even transmit images of activities captured within homes, offices or other apparently private spaces. The fact that this surveillance can be covert makes the capture of this information particularly problematic.

Second-generation biometrics such as embedded systems and behavioural biometrics may negatively impact privacy of location and space. Sensing and identifying individuals at a distance can result in covert data capture without the data subject's consent. Here, biometrics can be used in tandem with other surveillance systems, such as CCTV, static cameras or mobile phones with location detection capabilities, to pinpoint or track an individual's location.

Whole genome DNA sequencing can also negatively impact on privacy of location and space. This is primarily centred on concerns over the potential for detecting someone's location by comparing the DNA sample found at specific location and people's DNA profiles. This can be grounds for making associations between persons and their location, especially within forensics. It also introduces a possibility for making spurious associations between individuals and particular locations as a result of secondary transfers as this technology becomes more and more sensitive.

Privacy of data and image

We expand Clarke's category of privacy of personal data to include the capture of images as these have become considered a type of personal data by the European Union as part of the Data Protection Directive. This privacy of data and image includes concerns about making sure that individuals' data is not automatically available to other individuals and organisations and that they can "exercise a substantial degree of control over that data and its use".[20] Such control over personal data builds self-confidence and enables individuals to feel empowered. This can be negatively impacted by RFID-enabled travel documents, new

[20] Clarke, op. cit., 2006.

surveillance technologies, second-generation biometrics, whole genome DNA sequencing and BCIs. Like privacy of thought and feelings, this type of privacy has social value in that it addresses the balance of power between the state and the person.

RFID-enabled travel documents represent a potential threat to privacy of data and image, in authorised and unauthorised readings of RFID chips as well as threats associated with the security of back-end systems and the personal information stored on databases.

Body scanners and UASs also pose threats to the privacy of data and image. The body scanners case study identified threats regarding the potential for unauthorised or improper viewing, transmitting or storing the naked images of an individual and the effects of this. The UAS case study discussed the fact that UAS surveillance generates images of individuals, sometimes covertly, which leaves individuals no opportunity to avoid such surveillance or access the data held about them.

Behavioural biometrics and the use of biometrics at a distance both pose a threat to personal data or image. Systems that use behavioural biometrics can present a risk of loss of control by data subjects over their personal data. They may not realise that such systems are operating and this could infringe upon their rights to access data that is held about them and to have that data corrected. The use of biometrics at a distance also introduces issues around consent and transparency, where individuals may not realise systems are in operation.

Whole DNA sequencing technologies may also infringe upon the privacy of a person's data or image. The storage of genomic data without adequate consent in biobanks and databases could be compromised. Furthermore, an individual's phenotypic features (e.g., hair colour, sex, ethnic group, body height) can be derived from genomic data and used for the generation of a rough image of this person. As such, both their personal "data" and their image could be gleaned from gaps in consent and gaps in data protection.

Finally, brain-computer interfaces, as a human enhancement technology, represent a potential threat to personal data in that BCIs involve the digitalisation, collection, (temporary) storage and processing of information about brain activity. This data is highly sensitive, because it contains unique personal information whose prospective worth, especially in terms of its marketing value for the advertisement industry (cf. neuro-marketing), might increase immensely.

Privacy of behaviour and action

We also re-work Clarke's notion of privacy of personal behaviour to privacy of behaviour and action. This concept includes sensitive issues such as sexual preferences and habits, political activities and religious practices. However, the notion of privacy of personal behaviour concerns activities that happen in public space, as well as private space. Clarke makes a distinction between casual observation of behaviour by a few nearby people in a public space with the systematic recording and storage of information about those activities.[21] People have a right to behave as they please (within certain limits, e.g., for example, disrupting the Queen's garden party is off-limits) without having their actions monitored or controlled by others. This benefits individuals in that they are free to do what they like without interference from others which contributes to "the development and exercise of autonomy and freedom in thought and action".[22]

Privacy of behaviour and action can be negatively impacted by RFID-enabled travel documents, in that people's behaviours and travel activities can be reconstructed or inferred from information generated as a result of their use of these technologies. Travel routes, frequent destinations and mode of transport can be gleaned from information available on both e-passport databases and travel card databases. Furthermore, aggregated information can provide details that enable their routines to be inferred.

[21] Clarke, op. cit., 2006.

[22] Nissenbaum, Helen, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford Law Books, Stanford CA, 2010, p. 82.

New surveillance technologies such as body imaging scanners and unmanned aircraft systems can also negatively impact privacy of behaviour and action. Images generated from body scanners could reveal information about behaviour such as augmentation surgeries or medical related practices. With surveillance-oriented UASs, everyone is monitored regardless of whether their activities warrant suspicion. Furthermore, the potential to use surveillance covertly means that individuals cannot adjust their behaviour to account for surveillance, unless individuals assume they are being surveilled at all times and attempt to adjust their behaviour accordingly.

Behavioural biometrics potentially impact privacy of behaviour and action primarily through processes of automation. Human behaviour can be monitored, captured, stored and analysed in order to enable systems to become knowledgeable about people. Subsequently, measurements of changes in behaviour and definitions of "abnormal" behaviour become automated. This could lead to monitoring and recording of infrequent behaviours that are not suspicious or criminally deviant. Behavioural biometrics may also impact privacy of behaviour and action by revealing sensitive information about a person's psychological state, which can be used for behaviour prediction.

The advent of whole genome DNA sequencing carries the potential to negatively impact privacy of behaviour and action. As techniques become more sensitive, characteristics in human behaviour may be linked with specific genes and gene sequences. Furthermore, second-generation DNA sequencing might reveal sensitive information on the person's predisposition to certain psychological states and might be used for assessing the predisposition to impaired mental health and aberrant behaviour.

Human enhancement technologies potentially impact upon privacy of behaviour an action in two ways. First, drawing on BCI technology, behavioural neuroscience allows the location of parts of the brain that are supposed to be responsible for certain kinds of behaviour, attitudes and actions. That way, not only would the anticipation of buying behaviour be possible, but also individuals could lose their ability to consent to preventive strategies, such as crime prevention. Second, neuro-enhancers are closely linked to the risk of losing control over one's will and actions. That is why especially prescribed "enhancing" drugs such as Ritalin or modafinil pose a threat of external control (heteronomy) over the individual's behaviour.

Privacy of personal communication

Privacy of personal communications represents the sixth type of privacy which we identify. This type of privacy is shared with Clarke, and includes the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail messages. People have a right to keep their communications with others private and free from outside monitoring. This benefits individuals because they do not feel inhibited about what they say or feel constantly "on guard" that their communications could be intercepted. Society benefits from this aspect of privacy because it enables and encourages a free discussion of a wide range of views and options, and enables growth in the communications sector. This aspect of privacy can be negatively affected by behavioural biometrics and brain-computer interfaces.

Second-generation biometrics, specifically behavioural biometrics, can negatively impact individuals' privacy of personal communications. Speech recognition technologies can be utilised to analyse and disclose the content of communication, and these can be linked with automated systems to ensure that communications by certain individuals, or communications about certain topics, can be monitored or recorded.

This aspect of privacy may also be impacted by brain-computer interfaces, whereby the interception or monitoring of data streams between the BCI user and the machine could be possible.

Privacy of association, including group privacy

Privacy of association, including group privacy, is concerned with people's right to associate with whomever they wish, without being monitored. This has long been recognised as desirable (necessary) for a democratic society as it fosters freedom of speech, including political speech, freedom of worship and other forms of association. Society benefits from this aspect of privacy in that a wide variety of interest groups will be fostered, which may help to ensure that marginalised voices, some of whom will press for more political or economic change, are heard. However, UAS surveillance may impact upon privacy of association through its ability to monitor individuals and crowds, sometimes covertly. Unmanned aircraft systems can also generate information about groups or individuals with whom they associate. If UAS visual surveillance was combined with biometrics such as facial recognition technology, individual group membership and affiliation could be discovered.

Behavioural biometrics may negatively impact privacy of association. Behavioural biometrics introduces concerns over the potential for the automated creation of categories and allocation of individuals to such categories, which raises the potential for individual or group profiling and/or discrimination.

Second-generation, whole genome sequencing potentially impacts upon privacy of association in negative ways. An individual's presence at a particular location could be detected through linking a person's DNA profile with DNA found at that location. Individuals could be categorised into particular groups based on information gleaned from their DNA sequence. DNA sequencing and profiling makes it possible to monitor groups and individuals and generate sensitive information about the groups or individuals with whom they associate.

Synthesising types of privacy

These case studies and the aspects of privacy they may potentially infringe upon are summarised in the table below.

Types of privacy	RFID-enabled travel documents	New surveillance technologies	Second-generation DNA sequencing	Second-generation biometrics	Human enhancement technologies
Privacy of person		✓	✓	✓	✓
Privacy of thought and feelings				✓	✓
Privacy of location and space	✓	✓	✓	✓	
Privacy of data and image	✓	✓	✓	✓	✓
Privacy of behaviour and action	✓	✓	✓	✓	✓
Privacy of communication				✓	✓
Privacy of association, including group privacy		✓	✓	✓	

Table 9.1: Types of privacy potentially impacted by case study technologies

From the information presented in this chapter and in the table above, we draw various conclusions. First, privacy and data protection are not synonymous. While data protection can be equated with one type of privacy (informational privacy), the concept of privacy is broader than simply data protection. For example, body scanners raise concerns beyond data protection. The introduction of protections from unauthorised viewing of the images, encryption and automated imaging software that used CCTV or generic images of a person did not assuage all of the privacy-related issues around their use. Instead, issues about the generation of naked images, revealing medical conditions and providing alternatives to body scanning whilst protecting the right to travel also emerged as significant issues. Therefore, issues around privacy of the person and privacy around behaviour and action, as well as other ethical concerns had to be considered and adequately addressed before the EC would support their use in EU airports. Any legal or regulatory instrument or set of instruments needs to move beyond data protection impact assessments, which are often only compliance checks, to consider all of the privacy aspects, ethical issues and social concerns that we identify in this document, as well as any others that are emerging or specific to that technology.

Different technologies potentially negatively impact upon different types of privacy. Consolidating the case study information illustrates that privacy of data and image and privacy of behaviour and action are threatened by most if not all new and emerging surveillance technologies. In contrast, privacy of thought and feelings and privacy of communication are potentially impacted by second-generation biometrics and human enhancement technology only. As technologies develop and proliferate, various types of privacy which had not previously been under threat may now be compromised. Therefore, when new technologies are planned and developed, the developers need to consider all of the ways in which a new technology may impact upon privacy, without relying upon a check-list approach that may not capture all types of privacy.

2.2.2 Considering ethical and social issues

In addition to privacy issues, new technologies also raise ethical[23] and social issues such as human dignity, equality and the rule of law, discrimination, consent, self-determination and protection from harm.

Human dignity

We find that all five of our case studies potentially infringe upon human dignity. In relation to RFID-enabled travel documents, the case study argued that the continuous collection of data from individuals without their knowledge could impact human dignity. The body scanners case study argued that the imperative to undergo body scans that reveal naked images of passengers and/or medical conditions particularly impacts upon human dignity. Further implications for human dignity include the danger that the use of UASs could foster a "Playstation mentality" among operators as they do not see at first-hand the consequences of their actions on the ground. Thus, individuals operating UAS systems as well as those targeted by UAS systems could become de-humanised. Individuals can also become de-humanised by the "informatization of the body"[24], whereby the digitalisation of physical and behavioural attributes could affect our representations of ourselves. In relation to second-generation DNA sequencing human dignity in health care could be impacted if principles of anonymisation mean that individuals are not informed about new information regarding their disease risk profiles. Also in the DNA case study, requiring people arrested for certain crimes to give DNA samples, and by proxy, requiring family members of those individuals to reveal DNA information negatively affects human dignity as well as autonomy. Finally, the human enhancement

[23] For an analysis of the philosophical and methodological challenges inherent in the exercise of determining what constitute an "ethical issue", as well as of assessing how new technologies "impact" over these issues, refer to chapter 5 of the present deliverable on "Contemporary approaches to privacy and ethical impact assessment".

[24] van der Ploeg, Irma, The Machine Readable Body: Essays on biometrics and the Informatization of the body, Shaker, Germany, 2005.

case study argued that individuals have a right to self-determination as part of human dignity, which means that their informed consent to use BCIs, despite the privacy concerns, should be respected.

Equality

The RFID, body scanners, second generation DNA sequencing and second-generation biometrics case studies all raised issues surrounding intentional or un-intentional discrimination against particular population groups. In terms of RFID, this included the potential for power differentials between those operating RFID travel card systems and those who carry the cards. As a result, data processers can categorise individuals into particular profiles and this could result in a denial of service. The body scanners case study also identified the potential for religious discrimination, where religious Jewish and Muslim women who placed a premium on personal modesty were being discriminated against by compulsory body scanning policies. Information from the second-generation biometric case study also identified discriminatory effects in relation to older people, children, those with certain medical conditions or disabilities and/or those of particular racial backgrounds for whom it is known that biometrics are less accurate. This could result in these groups being less able to access state services as biometrics become more widely deployed. Finally, in relation to the DNA case study, individuals may be discriminated against as DNA information becomes increasingly able to reveal information about social or (eventually possibly) psychological characteristics such as race or personality characteristics that could result in discrimination. Furthermore, family members of those who are arrested may become discriminated against as a result of information about them that is revealed by their family member's DNA.

Consent

With regard to the rule of law, our case studies also identified potential ethical or social impacts. The RFID case studies identified the potential for identity theft, where some RFID systems did not secure personal data enough to protect individuals from harm. The consequences of identity theft could include an individual being denied a job or the ability to get bank credit, which could significantly affect their life chances. The body scanners case study argued that these devices interfered with an individual's right to travel and their religious freedom in some contexts where body scanning was a requirement to fly with no alternative, for example, a pat down search. Stakeholders quoted in the UAS case study commented that these devices represented a generalised threat to freedom and civil liberties. However, both the UAS and second-generation biometrics case studies argued that the deployment of these devices "at a distance" negatively impacted upon people's ability to consent to the collection and processing of their data as required by the EU Data Protection Directive. Consent is also impacted in the second-generation DNA sequencing case study by Internet and direct-to-consumer testing, particularly with regard to paternity testing, which can be done covertly and without the consent of the other parent. The DNA case study also recognised that second-generation sequencing may not adequately address the data protection principle of anonymity if individuals can be re-identified from sophisticated DNA sequencing techniques.

2.2.3 Conclusions from the five case studies analysis

The case studies demonstrate that these new technologies impact upon multiple types of privacy and raise ethical and social issues. In addition to data protection issues surrounding consent and data minimisation, other types of privacy issues emerge. For example, body scanners raise bodily privacy issues, while BCIs or second-generation biometrics raise issues around the privacy of thoughts and feelings. Also, data protection principles such as anonymisation may actually raise ethical problems, such as when individuals' DNA reveals a propensity to develop certain diseases. Individuals should be free to meet, communicate and interact with any individuals or organisations that they wish without being subject to monitoring by surveillance technologies. Individuals should also be free to move about in public space or travel across borders without submitting their bodies to automated surveillance by new and emerging technologies.

The proposed Data Protection Regulation, released by the EC on 25 Jan 2012, includes a provision for the mandatory undertaking of data protection impact assessments (DPIAs) when processing operations present risks to data subjects. Article 33 of the proposed Regulation cites several examples of risks, some of which have been discussed in this paper (genetic or biometric data).

The introduction of mandatory PIAs would enable organisations to account for the complexity of new technologies, their increasing capabilities, their applications, the sectors in which they are deployed and their impacts on a range of data protection, privacy and ethical issues. Using PIAs, privacy, data protection and ethical considerations would be built in to the whole process of technology development and deployment. As Wright argues, a mandatory PIA would "complement data protection legislation and help to increase awareness of the exigencies and obligations imposed by such legislation [and encourage] high levels of accountability and transparency[, which] are vital to the way organizations handle and share personal information".[25]

However, some have criticised PIAs for their focus on privacy to the detriment of other considerations such as ethical or social issues. Raab and Wright argue that this can be rectified by a pluralistic approach that captures the various ethical, social and other "meanings and associations within privacy's conceptual family".[26] Mechanisms such as pluralistic privacy impact assessments would encourage organisations to consider a variety of privacy, data protection, ethical and social risks and how these can be adequately addressed, rather than simply complying with a checklist of data protection principles. Furthermore, privacy impact assessments that are regularly updated enable organisations to anticipate further changes in technology capabilities or applications. Legal regulation should also include adequate redress mechanisms and meaningful sanctions for organisations or bodies which do not comply with relevant data protection principles and codes of conduct. These legal mechanisms should be harmonised across the EU to ensure that all organisations adhere to similarly high standards of privacy, data, ethical and social protections.

2.3 The analysis of citizens' concerns and knowledge about personal data processing

Dara Hallinan and Michael Friedewald (Fraunhofer ISI)

The third phase of PRESCIENT focused on citizen perceptions, concerns and knowledge.[27] Our analysis was carried out with a view on three stakeholders categories:

1. Data Controllers: In this analysis we took a data controllers' perspective on the data subjects' right to be informed (article 10 and article 11 of Directive 95/46/EC), and the right of access to data (as enshrined in article 12 of the data protection Directive). This part dealt whit the question of to what extent can European citizens have access to the personal information and are they are able to correct information and can find out how their information is being used.
2. Data Protection Authorities (DPAs): This part explored what role DPAs play in reconciling the rights and interests of data subjects and data controllers.

[25] Wright, David, "Should Privacy Impact Assessments be mandatory?", *Communications of the ACM*, Vol. 54, No. 8, August 2011, pp. 121-131, [p. 128].

[26] Raab, Charles and David Wright, "Surveillance: Extending the Limits of Privacy Impact Assessment", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

[27] The outcomes of this research are presented in Friedewald et al., PRESCIENT Deliverable 3, 2012.

3. Citizens: The analysis of citizen perceptions was split into two parts. The first considered citizens' concerns and apprehensions about new data collection technologies. The second considered citizens' knowledge and concerns regarding data storage and use.

The results of this research are comprehensively discussed in PRESCIENT D3 on "Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data"[28]. In the following lines, we present a brief overview of the main outcomes.

2.3.1 Implementation of data subjects' rights at selected data controllers

First, we examined the websites of some of the most important data controllers, and assessed the extent to which the information disclosed in the privacy notices is in line with the requirements of the Data Protection Directive articles 10 and 11. Some consistent trends emerged from this analysis. There are persistent misconceptions as to the meaning of personal data, as several data controllers take a very narrow view and consider as personal data only the information that users have voluntarily disclosed. In general data controllers are quite elusive as to the duration and purpose(s) of the processing. Many shortcomings have been also observed as to the information provided concerning the right of access to data. These several shortcomings can be understood and analysed in the light of the substantial requirements concerning the information provided that are to be found in the CNIL's (the French DPA's) letter to Google.[29] Furthermore, issues of applicable law to the data controllers might (at least) partly account for some of the shortcomings observed. Finally, it is worthwhile observing that many data controllers have adopted multi-layered privacy notices in the wake of the Art 29 WP's opinion 10/2004.[30] Yet, such a simplification of the explanatory framework should not be undertaken at the expense of the quality of the information provided.

We then aimed at determining how data subjects can concretely exercise their right of access (if at all) from the perspective of data controllers, that is, how do data controllers experience users' demands of access to their personal data. To this end, we contacted data controllers and asked them a list of questions concerning the data subject's right to access, such as how many requests they have actually received or if there are differences between Member States in regard to as how the right of access to information is exercised by the European citizens. We made a selection of five important data controllers, and we finally chose Google, Facebook, Microsoft, Amazon and Wikimedia. This exercise proved to be more difficult than anticipated. In the first instance it proved extremely difficult to reach, be it through phone, e-mail, or regular physical mail, a responsible person who had competences to address such requests. Second, even in cases where we managed to find the responsible person, either no information was available; either the data controllers were not in a position to gather evidence in order to answer our questions.

2.3.2 DPA activities supporting citizens' rights

The activity on DPAs has been carried out in two main phases. The first step was the analysis of the websites of the Data Protection Authorities of the 27 Member States and the European Data Protection Supervisor as well as the Art. 29 Working Party (DPAs websites inspections). The second step was to prepare a questionnaire and to send it to all Data Protection Authorities in Europe in order to collect more information on their activities (interviews). The purpose of the questionnaire was to gather contributions from DPAs in Europe on citizens' attitudes towards data protection, to assess to what extent EU citizens contact European DPAs and how these institutions are reacting to and supporting these claims. This touched both the question of how individual data subjects or groups of data subjects are asserting their rights as well

[28] Ibid.

[29] http://www.cnil.fr/fileadmin/documents/en/20121016-letter_google-article_29-FINAL.pdf

[30] Article 29 Data Protection Working Party, "Opinion 10/2004 on More Harmonised Information Provisions", Working Paper 11987/04/EN, WP 100, Brussels, 2004.

as on the more general question of whether supervisory authorities are willing and capable to enforce the law. We sent the questionnaire to all Data Protection Authorities in Europe, as well as to the European Data Protection Supervisor. Out of 27 Member States and one EU institution (EDPS), 19 authorities replied to the questionnaire.

We found that for most of the European DPAs the support of citizens' in the enforcement of their rights is just one among many tasks and that they are confronted with the problem of limited resources to carry out these tasks. The study, however, showed that the DPAs are noticing an increase in the number and type of complaints received. Citizens usually address the DPA to pose questions on their rights in a specific case, to request assistance to access, rectify or delete information, and to report violation of data protection rules. There is an increasing trend towards complaints related to data processing in online services, video surveillance in public spaces, surveillance at work, as well as data processing in the public health and financial sectors. The reaction time of DPA varies between days for simple inquiries to several months for more complex complaints that require an inspection. Delays may also occur also when the DPA has to wait for information on data processing from a public institution, a private company, or the DPA of another country.

2.3.3 Citizens' knowledge and concerns

Finally we have analysed a wide range of European (and some international) public opinion surveys on European citizens' concerns about new technologies and regarding data storage and use. However, the quantity of applicable surveys was limited, their focus was often narrow and their results were difficult to extrapolate into more elaborated explanations of opinion and behaviour. Accordingly, sources employing other methodologies, such as ethnographic studies and focus groups, supplemented the use of surveys. The task was split into two parts, the first considering citizens' concerns and apprehensions about new technologies and their applications, the second considering citizens knowledge and concerns regarding data storage and use.

Citizens' concerns and apprehensions arise from a wider process of opinion formation in which a number of factors play a role. In order to comprehend and categorise not only fears, but also the driving forces behind these fears, the logic of their manifestation and their relation to other aspects of public opinion on data collection and processing technologies, a holistic view of the processes and factors involved in public perception of new technologies must be taken before considering fears related to technologies specifically.

Perception of a technology is shaped by a number of factors. Firstly, demographic factors, such as the individual's nationality, are significant, as are personal factors, such as the individual's broader social tendencies and stance on issues related to a technology and its use. Secondly, as the complexity of much new technology often leaves a knowledge discrepancy, second hand sources, such as the media, play a significant role in opinion formation. Thirdly, each technology conjures up images based on its presented operation, provoking greater or lesser reactions of unease (physically invasive technologies, for example, tend to provoke comparatively greater unease). Fourthly, each technology is referenced to preceding technologies, with opinion being shaped around common points of reference. Finally, the sphere of use (economic, social, etc.) will define the factors and mode of acceptance.

One significant aspect of public opinion is the lack of solid understanding of many new technologies and the infrastructures in which they operate. First, the presentation of the media of such technologies is not always neutral or focussed on the specifics of operation of the technology. Second, technological understanding is not always within reach of the general public. Finally, the environment of data flows in which the eventual privacy risks manifest, is largely invisible to the individual – the consequences of each technology are not necessarily easily comprehensible, or even directly relatable to that technology.

It was clear that there is an awareness of the potential and usefulness/necessity of data collection in certain situations. However data collection technologies are greeted with a certain uneasiness. This is partly due to the lack of technological understanding, but also due to the perception that the spread of technologies may be threatening to fundamental social principles. There is uncertainty about the legitimacy, reasoning and targeting behind much data collection technologies and the context of their deployment. Unease also arises due to the complexity of related social issues, making tracing a path of causation between social debates and technological deployment difficult (what is the exact problem and how exactly will technology provide a solution?) Finally, the lack of clarity as to 'the who, the why, the how and to what end' of the data controllers is seen as a significant concern, demonstrating a lack of transparency and providing the basis for function creep or the misuse of the technology or collected data.

The second part then focussed on citizens' awareness concerning data collection and use. The consideration as to whether the public knows what data is stored, why and for what period requires a deeper analysis than simply a consideration of awareness of collected data types and their locations. The purpose of a consideration of citizens' knowledge of data collection, storage and use is to better understand citizens' perceptions of the connections and purposes behind the development of the data environment and their place within, and interaction with, this environment. The section begins with a brief comment on the diversity of the European public and the difficulties this creates in trying to analyse 'public' opinion. It then takes as its starting point public awareness and knowledge of the current data protection framework as the template for the regulation of data collection and flows and as the key framework safeguarding citizens' rights in the data environment. The section then considers public perception of the data environment in reality, considering public perception of the actors and networks which make up the data environment. The section then attempts to add depth to the causes and logic of public engagement with the data environment, considering why the public behave as they do when engaging with this environment. Finally, public perception of the effectiveness of the regulatory framework against the current reality of data processing is considered.

It is striking that the public allocates data protection and privacy significant importance. Whilst there is significant variation across Europe, it also seems that the majority of Europeans are familiar with the framework's key rights and principles (such as the right of access). However, knowledge levels drop considerably concerning the more abstract or complicated aspects of protection (for example the status or content of 'sensitive data'). Surprisingly, considering awareness of the general principles of data protection, there was relatively low awareness of DPAs and their functions (although this also varied greatly across member states). Comprehension of the significance of data protection within a wider legal order was conspicuously lacking. Although people are aware of the existence of the right to data protection, they are not immediately aware of why it has manifested in its current form and at first thought seemed to be relatively unaware of its social function. It is however, interesting to note that in longer discussions of issues related to data protection, participants began to voice opinions more resonant with a comprehension of the social function of the right.

In the consideration of the data environment in reality, surveys tended to demarcate state actors and private organisations as key actors. It is interesting to note that 'individuals' were not seen as key actors. The public allocated trust in different actors with considerable nuance. Generally speaking, state actors were more trusted than private actors, whilst the level of trust also varied according to which state or private sector was considered. However, despite this nuance in trust allocation, there is little conception as to the model of interaction between organisations or as to the flow of data between organisations. Whilst the public generally disapproved of data transfer between government and private organisations, it seemed that the public lacked a picture of data flows after first instances of collection. Perhaps, as a consequence of this, there was contradiction and split opinion in the consideration of more abstract questions – for example, when considering how the allocation of responsibility for the safe handling of data should be divided. It seemed that the public were particularly concerned about ID fraud, but also demonstrated concern and annoyance at the commercial collection and use of data. Although there were more abstract fears relating to the combination of data sources and/or databases, and further issues related to assemblages of data in terms of their social basis, these were at best only loosely defined and generally emerged only after more lengthy discussion.

Despite the fact that 63% state that disclosing personal information is a big issue for them, individuals seem to accept the need to divulge increasing amounts of data. This seems to be based on the deterministic viewpoint that disclosure is 'simply part of modern life'. On the one hand, there is the perceived obligation, legally and practically, to release ever more information. On the other hand, the public recognise short and long term benefits from disclosure – in the form of exchanges for rewards and participation in data environments.

It is evident that stated privacy preferences and actual behaviour differ significantly (the privacy paradox). Acquisti and Grossklags consider the possibility that "Privacy in theory may mean many different things in practice" and consequently that "the parameters affecting the decision process of the individual are perceived differently at the forecasting (survey) and operative (behaviour) phases". They isolate a series of potential limiting factors to the individual decision to balance a transaction with a potential information security impact. The decision-making model may be unbalanced by limited information, bounded rationality issues, self-control problems and other behavioural distortions. The behaviour of the public in releasing data, despite abstract awareness of the dangers may be explained by considering the difficulty the public has in perceiving the data environment. It is clear that the public comprehend neither the supporting technological infrastructure nor the data flows and networks that make up the data environment. Thus, whilst not unaware of dangers and the existence of structures through which data processing and protection operate, there is a lack of understanding as to how and why they operate. The lack of understanding of the data environment mentioned above would certainly account for impacts on each of these potential limiting factors and thus significantly reduces the ability of the individual to "rationally" balance each specific action. Consequently, awareness of issues and danger related to data releases (and the importance of privacy and data protection) may not translate into cautions corresponding action in concrete situations.

The above makes clear that the public suffers from a certain knowledge shortfall in understanding the framework and the environment it is designed to regulate. The aggregated uncertainty this creates can make it difficult to isolate specific expectations as to how and to what extent protection is expected from law generally and the data protection framework in particular. However, certain features of opinion are clear. Most importantly, a majority of the public feels they have lost control over their data and believes that the current protection frameworks cannot cope with the demands placed on them. Whilst the public seems not to disapprove of data protection *principles*, it does not perceive protection in reality to be of the same quality.

We find that it is in the enforcement and application of regulation in the data environment in which problems are perceived to lie. That the public see a problem in enforcement is demonstrated by the desire for relatively harsh measures for organisations which breach norms, whilst the uncertainty of application against a complicated current environment is demonstrated in the discrepancy and uncertainty in defining terms for even relatively basic concepts, such as responsibility allocation.

3. Scenarios

Scenario guru Peter Schwartz defines scenarios as "a tool for ordering one's perceptions about alternative future environments in which one's decisions might be played out… Concretely, they resemble a set of stories". He also said "scenarios can help people make better decisions – usually difficult decisions – they hey would otherwise miss or deny."[31]

This chapter describes the process of creating *ethical dilemma scenarios* involving new and emerging technologies. It is based on the premise that the development and deployment of new and emerging technologies often give rise to privacy issues and ethical dilemmas. By ethical dilemmas, we mean situations involving ethical principles and issues where the choice of what might be the right decision, the right course of action, is not immediately clear and hence requires a privacy and ethical impact assessment in which stakeholders are engaged in order to help policy-makers and/or industry project managers to arrive at an optimal choice.

3.1 Introduction

David Wright (Trilateral Research & Consulting)

One of the aims of the PRESCIENT project is to provide an early identification of privacy and ethical issues arising from emerging technologies and their relevance for European Commission (EC) policy.

Following an analysis of privacy and data protection as conceptualised from an ethical, socio-economic and legal perspective (Stage 1), the PRESCIENT partners prepared a set of case studies wherein they identified the privacy, data protection and ethical issues arising from five different emerging technologies and their applications (Stage 2). The technologies and applications included RFID-embedded travel cards and passports, unmanned aerial systems ("drones")[32] and body scanners, biometrics, DNA sequencing and human enhancement.

Building on the findings from the case studies, the partners were tasked with developing scenarios highlighting the privacy and ethical issues that might arise with emerging technologies and, in particular, the ethical dilemmas. The last major task in the project was to develop a privacy and ethical impact assessment framework by means of which such privacy issues and ethical could be addressed (Stage 4), which is presented in Chapter 6.

This chapter describes the process by which the partners created the ethical dilemma scenarios. We think the process by which we created these scenarios and the privacy and ethical impact assessment methodology we developed to find solutions has wide applicability to other technologies and is a useful way to consider the privacy and ethical issues that might arise from the deployment of new technologies *in advance* so that policy-makers and technology companies can avoid or mitigate the risks and, especially, damage to citizen-consumer trust and confidence and to their companies' reputation.

Furthermore, the development of "What if" scenarios, like those set out in the pages that follow, could inform or be factored into a privacy and ethical impact assessment as a way of stimulating stakeholder interest in the process and consideration of possible risks.

[31] Both quotes come from Schwartz, Peter, *The Art of the Long View*, John Wiley & Sons, Chichester, 1998 (first published 1991), p. 4.

[32] Finn, Rachel L., and David Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review*, Vol. 28, No. 2, Apr. 2012, pp. 184-194.

Specify the objectives of the scenarios

Technology scenarios can serve many different purposes. They may be used as warnings for policy-makers and industry decision-makers about the privacy and ethical issues that may arise with the development of new technologies. They may be developed to describe the kind of future we want and to prompt us to consider what steps we need to take to arrive at that future ("backcasting"). They may be "what-if" scenarios, i.e., what would we do if a future as described by the scenario arrives. They may serve as a way of engaging stakeholders to think about the future.

Thus, those developing scenarios should be clear about how they intend to use the scenarios, and they should specify what they want the scenarios to achieve.

In our case, we wanted to develop scenarios that posed ethical dilemmas which do not present easy policy choices (each alternative is equally problematic) for which there is a need for privacy and ethical impact assessments. Thus, we would describe our scenarios as "What if" scenarios – in other words, if policy-makers and/or other stakeholders were to face a future such as that described in the scenario, how would they respond? What would they do to address the privacy and ethical issues raised in the scenario?

Identify the types of the scenarios

There are many different types of scenarios.

Scenarios may generally be normative or exploratory. Scenarios frequently are tools used in foresight studies.

They may be "sunny" or "dark", the first describing a positive future, one that we want, while the second describes a future we do not want.

Some scenarios may be narratives, i.e., they tell a story, while other scenarios may be descriptive, they describe a future.

Scenarios sometimes are structured as sensitivity analyses, coming as a set of three, with one scenario describing the "status quo", i.e., a future with no surprises, a worst case scenario and a best case scenario.

Scenarios can also be structured orthogonally, with a set of four scenarios, each occupying a different space in a quadrant where, for example, the horizontal axis is the degree of impact and the vertical axis is the degree of uncertainty.

Point of view is a factor to be considered too. Some scenarios could be set out as forecasts, i.e., from the perspective of someone today gazing into the future and offering his or her prediction of what might unfold. Or they could be told from the point of view of a witness in, say, 10 years from now, by someone who is like a reporter, engaged in reportage, describing the future as a lived event.

They could be short vignettes of a paragraph or two, or they could be relatively long and detailed.

The PRESCIENT partners discussed different approaches, types of scenarios and methodologies for constructing scenarios. Taking into account the aforementioned case studies and, in particular, the privacy and ethical issues that were identified in the case studies, the partners agreed that we wanted to create short "what-if" scenarios situated about 10 years in the future. The objective of the scenarios was to tell some short stories based on the emergence of new technologies so that they could "provoke" policy-makers and decision-makers to consider what they might do if the scenario materialised into reality and so that they could "provoke" consideration of an ethical and privacy impact assessment as a tool to address the dilemmas posed in the scenarios.

Identify the technologies and applications

As we were developing technology scenarios, identifying relevant technologies was, of course, of crucial importance, but it is a difficult, perhaps hopeless challenge: How is it possible to predict what technologies will exist a decade hence? While it may not be possible to predict specific technologies, it may not be quite so difficult to predict the capabilities, proliferation and impacts of those technologies.

In our case, we focussed on several technologies or types of technologies. For example, we focused on human enhancement technologies. We didn't predict specific human enhancement technologies; it was sufficient to assume that there would be a variety of technologies available 10 years from now that would enable cognitive, physical and sensory enhancement and still others that would enable humans to resist pain and live longer. We assumed there would be some diffusion of these technologies, e.g., to military personnel and to rich people, but not to everyone. And with regard to impacts, we assumed that such technologies would create a two-tier society, i.e., between those who had been enhanced and those who had not been. We also assumed that one impact would be conflict between the enhanced and the unenhanced.

The PRESCIENT partners considered various technologies around which we could write our scenarios. After some discussion, we agreed to build scenarios involving the following:

- Biometrics and, in particular, facial recognition. We assumed that the reliability of facial recognition would continue to improve to the point in a decade from now where reliability would be in the order of 90 per cent.
- Dragonfly drones. We assumed drones about the size of dragonflies would be widely available at low cost. We assumed that they would be capable of carrying different payloads and, in particular, video surveillance.
- Data analytics ("big data") – We assumed continuing progress in data mining, data aggregation and predictive analytics would give political campaign staff the same capabilities as commercial vendors to target individual citizens, to know how they react to certain stimuli and messages and, thereby, to strongly "influence", if not actually control their voting intentions.
- Human enhancement – As discussed briefly above, we assumed that the military in particular would want to "enhance" its troops by giving them different types of implants that would enable cognitive, physical and sensory enhancement as well as enable them to withstand pain and other stresses and, for good measure, to live longer.
- Near field communications (NFC) – We assumed that with the Internet of Things or ambient intelligence, all products would bear RFID or "smart dust" (networking sensors and actuators in a mesh configuration) and with smart phones, people's behaviour, attitudes, location, activities, etc., would constantly be tracked and assimilated to the point where privacy becomes a historical curiosity.

Identify the key ethical issues that are going to emerge

Having identified the technologies, the partners then identified and discussed a range of different ethical issues that these technologies could provoke. We created a spreadsheet with several different columns, the first of which listed the technologies. The second column listed various applications of those technologies. The next few columns were headed by various ethical *values* such as equity and fairness, discrimination and social sorting, trust, privacy and consent. Those were followed by another set of columns headed by various *issues*, including freedom to opt out, the ability of government to regulate big companies, accountability, information and power asymmetries, manipulation, function creep and chilling effect.

The partners then attempted to fill in the various cells to give some examples of the intersection of technologies, applications, values and issues. Thus, for example, with regard to biometric technologies, such as facial recognition, used in security applications, under the values of inclusion and equity as a counter to discrimination and social sorting, we stated that "Some individuals could be prevented from accessing goods and services because of failures in biometric systems and/or mis-identifications. Some are also more likely to be monitored and tracked because of racial characteristics, age, ability, etc." And in the issue column headed by "Information asymmetries", we stated that "Covert systems would mean that security institutions have more information about an individual than either the person realises or than the person has about the organisation operating the system."

Filling in the cells helped to frame the scenarios. Also, as our scenarios would be relatively brief scenarios of two or three pages, the partners agreed to focus on only three ethical issues in each scenario, a primary ethical issue and two "secondary" ethical issues. We also agreed that we should focus on different ethical issues in each scenario.

Scenarios in four quadrants

Having identified the technologies, applications, values and ethical issues which could feature in the scenarios, the partners had several brainstorming sessions to discuss and agree the story line of each scenario. The partners also agreed that we should construct scenarios of different types that could be situated in four different quadrants in an orthogonal relationship to each other as follows.

Four types of scenarios:

1. *Dark scenario* – Corporations & governments manipulate & control citizen-consumers to the point where citizens no longer care about privacy or the related ethical issues.	2. *Popular push-back* – Citizens are repelled by and repel government and corporate attempts to manipulate and control their behaviour and, as a result, governments are forced to introduce privacy- and ethical- friendly policies
3. *Sunny scenario* – Corporations and governments are concerned about the welfare and well-being of citizen-consumers.	4. *Unintended consequences* – The democratisation of surveillance makes it harder to catch the bad guys

One can see a relation between the four quadrants as follows. The dark scenario (Quadrant 1) prompts push-back from the citizenry (Quadrant 2), which in turn makes corporations and governments much more sensitive to the concerns of citizens (Quadrant 3), which gives rise to unintended consequences (Quadrant 4). In the following sections the five scenarios are presented.

3.2 Privacy is dead. So what (yawn)?

Raphael Gellert (Vrije Universiteit Brussels)

Type of scenario: Dark scenario (Quadrant 1)

Corporations and governments manipulate and control citizen-consumers to the point where citizens no longer care about privacy or the related ethical issues. This dark scenario[33] describes a future wherein there is a proliferation of near field communications (NFC) for mobile payments.

[33] About "dark scenarios" see Punie, Yves, Ioannis Maghiros, and Sabine Delaitre, "Dark Scenarios as a constructive tool for future-oriented technology analysis: Safeguards in a world of ambient Intelligence", in *Proceedings of the Second International Seville Seminar on Future-Oriented Technology Analysis: Impact of FTA Approaches on Policy and Decision-Making*, Seville, 28-29 September 2006.

The scenario

10 September 2022, this is an ordinary Saturday in the life of Katherine. After a hard working week as a manager in a bank, she intends to make good use of her weekend to do some shopping, before going out with her friends to a new dance club that recently opened downtown.

In order to get to the shopping district, she uses public transportation. She steps in the newly renovated tram n° 7. She does not need to bother whether she still holds a valid transportation ticket: her smartphone is equipped with near field communication (NFC) technology. It automatically proceeds to the payment as soon as she passes close enough to a reader. Once the transaction is completed, she immediately receives an advertising message from a screen in the tram, suggesting a few special offers for different types of tickets (yearly, monthly, etc.) of particular interest to her.

Since NFC technology was first introduced as a means for mobile payment (as a matter of fact, it started in public transportation systems) some 10 years ago, tremendous progress has been achieved especially in terms of database interoperability. This has been made possible through initiatives in the field of e-government. In order to better administer its citizens, the government has proceeded to the centralisation of databases pertaining to the different services it offers to its citizens. There is thus a massive aggregation of data, namely from her bank account, her health record, her ID card, her data from the population register, her marital status, her social entitlements file (she is categorised as being part of the active population), as well as DNA and biometric information. All of this information is stored in the NFC chip in her smartphone, and is accessible to the reader, which enables offers especially targeted to her.

Out of the need to make savings, the government has gradually sub-contracted to private companies almost all of the public services it provides, as well as the associated operations (in this case, the data collection, aggregation, mining and the ensuing profiling). Because private companies run these services they have access to these massive sets of data, which they use, *inter alia*, for targeted advertisement such as the one to which Katherine has just been subjected. As she finds the offer interesting and subscribes to it, she arrives at her stop and steps out of the tram.

Thanks to new shopping applications, she confidently knows where to go. Like many of her friends, she uses a personal online shopping application whereby she books items. Now she simply needs to go in the shop and try out the clothes she has favoured. As soon as she enters the first shop, her smartphone is read at a distance by RFID readers, which thus have access to the list of items she has pre-selected. They precisely indicate to her in which part of the store they are located. Because all her personal information is centralised in her smartphone and because, sadly, she has not made any effort to protect it (she has neither anonymised, nor encrypted her data, partly because she does not regard her personal privacy as very important and partly because of the effort needed to take what she thinks are unnecessary precautions), the store's RFID readers have full access to it, including the list of items that have previously been bought in this store as well as in competing shops.

In addition to the clothes she had previously intended to buy, she waivers in front of another item. Thanks to her smartphone's locational capacities, the shop's numerous RFID readers are able to determine that she has been spending some time in front of these items. She is thus immediately offered a 20 per cent discount on these items if she buys them in addition to the ones already planned – which she does.

At the store exit, she receives a new advertisement: given the clothes she has just bought, she is invited to try a new lipstick and nail polish in a nearby perfumery that has a partnership with this clothes shop. The idea is tempting. Yet, once she gets there, she realises these products do not correspond to her tastes... Taking stock of her dislike, the perfumery's advertisement screens come up with suggestions that might suit her better, which is indeed the case.

At this point, her smartphone alarm reminds her that she is just in time to go back home, to change and to meet with her friends.

Once safely arrived back home, she changes into her new clothes for the party to which she is going this evening and, as she does so, she switches on the television. She falls right into the middle of a heated debate between an industry expert and a privacy activist. The latter argues that new technologies such as mobile payments through NFC technology and the ensuing personalised advertising present many dangers for citizens' privacy, data protection and other fundamental rights. Among these threats, he enumerates the following issues of particular importance. He first points out the particularly steep intrusiveness of this technology, not least because its (supposedly) optimum functioning relies upon the processing of huge quantities of personal data (Katherine does not regard this as very sensitive data) and equally important data mining and profiling operations. Such operations would have been considered as important privacy and data protection violations a decade ago. The quantity and quality of data disclosed are characteristic of a privacy violation. Consent, which epitomises the notion of control over one's own data, is completely absent in such setting (be it in its opt-in or opt-out version). Other principles such as data minimisation, data quality and purpose specification are mindlessly violated.

In the wake of these privacy and data protection violations, the privacy advocate also points out the pernicious bargain taking place: People are disclosing their personal information in order for this system to work. But, he asks, is it really worth it? Are the advantages brought by the quasi-automation of our environment really worth disclosing so much of our information? And aren't there other associated dangers? The privacy activist points out the dangers for personal autonomy: is there still some room for individual free choice since we are only presented with advertising that supposedly matches us best? And what if these predictions are wrong (as was the case with the lipstick) or what if we want to discover new choices? Personalised advertising, he argues, is a typical case of power inequality where citizens are at the mercy of opaque systems, the functioning of which they cannot grasp. Such power inequality can and does result in discriminatory practices such as raising health-insurance premiums for people who might be at risk based upon profiling information or proposing choices to people based upon their ethnicity or their (estimated) income and social status. People might even be refused access to certain stores depending upon these criteria. He criticises the collusion between government and private businesses in the aggregation and processing of vast amounts of data from hundreds of different sources. Just as it provides businesses with data that make pervasive advertisement possible, it also fosters surveillance by the government, which tracks all behaviours it deems to be suspect or at least socially undesirable, thereby threatening the general presumption of innocence, a cornerstone of the constitutional democratic state. He castigates pervasive function creep.

He concludes his intervention by arguing that these practices literally amount to making citizens naked in the eyes of industry and the government.

Puzzled by the fact that someone might oppose the very technologies that helped her achieve such a successful shopping day ("So much fuss about trivialities," she thinks), Katherine switches off the TV as she leaves in her new attire, her thoughts already focusing on the fun she is about to have.

Ethical dilemma

This scenario highlights the ethical dilemma raised by the conveniences offered by new technologies and the sacrifices made in privacy. It also raises other ethical issues relating to the freedom to opt out and function creep, whereby many applications and technologies serve purposes not originally specified upon their first introduction.

3.3 The presidential candidate, her campaign manager and data analytics

Rachel Finn (Trilateral Research & Consulting)

Type of scenario: Dark scenario (Quadrant 1)

This is a dark scenario because campaign managers use advanced technologies to manipulate the electorate while voters are largely unaware of how they are being manipulated at an individual with messages tailored to each of them.

The scenario

Ellie sits at her desk with an elbow on her desk and her hand supporting the weight of her head as she reads the latest poll figures. She is trailing behind her rival presidential candidate by seven percentage points with no visible way to close the gap since funds have been running out.

Peter, her campaign manager, enters the room with a grim look on his face. “Have you seen the latest figures?” he asks.

Her frown is all the response he needs.

“We have to do something,” he says. “Have you thought anymore about my suggestion?”

“Yes: I think all those personalised data analytics are creepy. Plus, what those ‘sentiment managers’ are describing sounds suspiciously like manipulation. Is there room in a democracy for these kinds of manipulation?”

Peter stares at her, exasperated. “We’re mobilising democracy, not undermining it! Personalised advertising software helps us to identify the characteristics of people who are already supporting you, those who aren’t and those who are undecided. It uses publicly available information from the voters’ register, social networking sites and other databases to work out their age, race, gender and other, softer characteristics. These could be family size, recreational interests, health and where they stand on specific political issues. We track them as they move from one website to another, so that we have a better understanding of their interests and so that we can target personalised adverts that address their interests. Once we’ve identified the undecided individuals, we can use our new understanding of their personal characteristics to make a more personal appeal to them – to show them how your policies will bring benefits to them, and others like them.

“Most people don’t vote because they don’t know enough about the candidates, and because they’re not motivated enough to find out what each candidate’s polices mean for them,” he continued. “We would be encouraging people to vote and to make an informed choice.”

Ellie responds, “Yes, but don’t people have a right to be dis-engaged? Should we tracking them, putting them under automated surveillance, building profiles of them so that we can target them with adverts, with the policies that we think will appeal to them? Isn’t there a risk that we could be telling two different voters two completely different things?”

“You can’t be so naïve, Ellie. You think the anti-immigration lobby is not using the exact same techniques in favour of your opponent? Why do you think his numbers have been going up? Besides, people *do* consent to receive these targeted adverts. When people use social networking sites, they are told their personal information may be used for other purposes.”

“And the sentiment managers?” Ellie asks.

“All they do is identify what works. That is what focus groups and polls have been doing for years. They run an ad and use sentiment analysis and decision science to identify which aspects of the ad capture people’s visual attention, what aspects raise their blood pressure and to what aspects they respond favourably. You’ve seen the briefing. The only difference between these techniques and focus groups and polls is that they eliminate the self-reporting aspect. People cannot always accurately explain what they like about an advertisement. How many times have you heard someone say, 'I dunno, I just liked it'? These techniques can tell *us* more about how voters respond to particular ads and we can use this information to convince other people that you're the right person for the job."

He continued, "Plus, with information like this, we can tailor the advertisements to connect with what is most relevant to different groups. So, for example, we can highlight your child tax credit policies for voters with young families, and pensions for older voters. Each voter gets his or her own personalised message and feels like you're talking about the issues that matter to them."

Ellie shakes her head. "But, if we know that mention of crime control alongside an image of a working class youth will dilate a voter's pupils and raise their blood pressure, doesn't it become manipulation if we use that information to pique their interest? I mean, we're influencing their body's physical response."

"If you knock on a voter's door, and you hear three deadbolts unlock when he opens the door, are you telling me you're *not* going to mention crime control when you do your pitch?" Peter answers. "You're becoming in danger of falling behind the times if you ignore the new tools that are at your disposal. Other candidates are using these methods, and it's streamlining their campaigns and making them more effective and efficient. You cannot compete against the conservatives without using personalised campaign messages. Not only have they got more campaign money than we have, they're using it more efficiently than we are."

"Well, you're ignoring another problem," Ellie retorts, "There is no way that I can use personalised data analytics after being so critical of them as the Commerce Minister. The Conservatives will jump down my throat and accuse me of being hypocritical."

"I haven't forgotten," says Peter. "But remember that the Central Trade Union has already offered to run the analytics and ads for us, in lieu of a contribution. All we have to do is use our software to feed them the information. They'll identify the potential supporters and start the mobilisation strategy. All you need to do is nod your head. No one will criticise you for recording issue-specific advertisements," he promised. "They're standard practice."

Ethical dilemma

The scenario highlights the ethical dilemma raised by the use of data mining and data analytics to pinpoint individual voters and to play on their prejudices, fears, apprehensions, behaviour, proclivities in order to get them to vote for the candidate who, at the same time, fears that her image as a "clean" candidate could be undermined by the use of such technologies. The scenario also raises other ethical issues, notably social sorting, manipulation and function creep.

3.4 The bionic soldier

Philip Schütz (Fraunhofer ISI)

Type of scenario: Popular push-back (Quadrant 2)

This scenario depicts the tension between "enhanced" military troops and the non-enhanced (the rest of us). This is a "popular push-back" scenario (as we have termed it) because the scenario highlights some popular pushback against a two-tiered society of enhanced citizens and "ordinary" non-enhanced citizens.

The scenario

He loves, no, actually he *owes* the military. For more than 30 years, he has served the army, working his way up from the lowest military rank as a private to the post of a full general. Carl is a widely known and respected figure in his country. Politicians and governmental officials regularly seek his advice, and he considers it his duty to give his considered opinion on these issues.

However, at the moment, he doesn't know what to do. Two weeks ago, the chairmen of the country's two largest political parties approached Carl. They asked for his opinion on draft legislation aiming to reregulate the prescription and usage of pharmaceutical and technical human enhancement. Carl was aware of the fact that nowadays a so-called *performance enhancing kit* is given to everyone accepted for army recruit training. He remembered that even when he had joined the British army in 2001, shortly after the September 11 terrorist attacks, and had been sent to Iraq, drugs such as Ritalin or modafinil had been regularly subject to off-label usage by soldiers in order to increase the ability to stay awake and to withstand the emotional pressure.

But today, in 2025, the enhancing kit involves much more. There is, of course, the by now famous miracle drug called *NH*, i.e., a neuro enhancer, developed and exclusively produced for the military. Normally, military personnel start with small doses, but once one's body and mind get used to it, the soldier can take more. NH not only increases one's focus and alertness ability immensely, the taking of the drug also results in calming the person, making nervousness, high blood pressure and hyperventilation a thing of the past. So, in fact, he regularly takes NH, when, for example, preparing an important speech all night long or being nervous shortly before the actual speech. Although he would never admit that in public, he knows that NH is also used to exercise more control over the soldiers. It is not clear yet how addictive NH really is, however, the drug makes one increasingly numb towards any emotions whatsoever. That way the military becomes your one and only family.

Alongside NH, there is also the recently introduced *wonder chip*, which is implanted into a soldier's temple. This chip is not only a unique identifier and tracking device – saving your life when kidnapped in operation areas – but also provides an interface that wirelessly connects the carrier's visual nerve with the matrix, an exclusive and well-protected military communication net. Specifically designed homepages from the military make information and knowledge ubiquitously accessible. However, the navigation through the matrix is mind-controlled and, thus, needs to be learned and constantly improved in numerous training sessions. He has noticed that soldiers are increasingly relying on that visual piece of information they get from the matrix, which allows the content provider to have an unusual amount of influence on them.

Above all, these two elements of the enhancing kit are now subject to the new regulatory initiative in which he was approached by parliament to give his opinion. And all of this would not be so damn difficult if he did not have his best friend William. They knew each other since childhood, and it was soon clear that William was one of the brightest individuals he would ever get to know. William went into science and research and became a professor at a renowned university. Although his friend had always stayed out of any political activities, he knew that began to change approximately four years ago when William spotted a group of his students, apparently taking NH in order to improve their test performances. William knew that it was really difficult to legally acquire NH without the army's approval, but when he researched the family background of these students he realised immediately that high-ranking army officials had given NH to their children. Even worse, he also found out that one of the older students who had already served the army must have had this new wonder chip implant, making him an exceptional student as well as an extremely difficult know-it-all to handle.

William knew that he could not go public with the call for banning that kind of enhancement, which was already too important and prevalent within the military. It was only afterwards that William realised how he had to go public. After publishing an article about unfair conditions for non-enhanced students on the UK's most famous blog, William became a widely known political figure. His claim to open up the market for enhancement products, such as NH as well as the wonder chip, and let civil society take part in the advantages of such developments found many supporters across Europe.

The main reason Carl was against any legal changes with regard to the exclusiveness of human enhancement products for the military had always been the national security argument. What would happen if terrorists or hostile nations could profit from these developments if they were available on the open market? Nor was Carl convinced by the social equity argument William always put forward. These human enhancements were the first steps towards creating cyborgs: didn't people see that? On the other hand, he knew people in the British defence industry who would warmly welcome a new mass market for their products.

The arguments for and against human enhancement seemed to be equally balanced. He recognised that polarisation in society between the enhanced and not-enhanced had dangerous ethical consequences. Society required some convincing resolution of the debate.

Ethical dilemma

This scenario highlights the ethical dilemma that arises when society has two types of individuals, those who have been enhanced and those who haven't been. It raises other ethical issues, notably equity, fairness and power asymmetries.

3.5 Facial give-away

Silvia Venier and Emilio Mordini (Centre for Science, Society and Citizenship)

Type of scenario: Sunny scenario (Quadrant 3)

This is a sunny scenario in the sense that governments and companies recognise that they must do the right thing by citizen-consumers and they decide to take the initiative in engaging other stakeholders to find the right way forward in the use of this technology and how long images and videos ought to be stored, who should have access to such data, etc. The scenario makes clear there is a need for a privacy and ethical impact assessment. A privacy impact assessment alone is not sufficient. Ethical issues such as consent and trust must also be considered.

The scenario

Laura is 45 years old. Her life is busy and fulfilled. She works as an accountant for a large company in the centre of her city, where she also lives with her husband and their two sons. A few weeks ago, her 73-year-old mother Louisa was diagnosed with second stage Alzheimer's disease (AD). AD is a degenerative form of dementia, a progressive neurological condition characterised by the build-up of proteins in the brain that gradually damage and eventually destroy the nerve cells, making it progressively more difficult to remember, reason and use language. In the ageing society of 2025, AD is a growing concern. The disease currently affects approximately 15 per cent of the population aged 65 years and older, and almost 60 per cent of the population aged 85 and older. It has recently been estimated that the population affected by AD will increase three times in the next 30 years.

Today, Laura has taken a day off work to accompany her mother to the clinic. At the end of the visit, the doctor tells her mother: "I would like to propose something to you, Louisa. A new device has recently been developed which helps AD patients deal with their short-term memory problems." A mini-camera and face recognition software are embedded in the patient's glasses and connected to a Bluetooth-enabled wristwatch. "When the glasses recognise a face," continues the doctor, "this watch vibrates and displays the person's name on it. This can help you to remember the name of the person you are looking at. What about having a try?"

Louisa seems a bit confused by the explanation, but her daughter encourages her to try the device. After all, with their large family, the device could really help Louisa with the names of all of the relatives and other people with whom she interacts. For Laura, the biggest concern is that her mother's mind might start taking things too easy, might stop making the effort to try to remember. On the other hand, a great advantage is that the device could improve her mother's general quality of life, since in social interaction, she will probably feel less awkward and frustrated at being unable to recall a person's name.

While Louisa's favourite nurse, Linda, explains how the new glasses and watch should be used, the doctor turns to Laura. "I would like to propose something to you as well," he says, and informs her about the recent development of a screening test that detects early-onset AD. "As you know, one of the difficulties in AD treatment in the past was that there was no early and definitive test for Alzheimer's. A diagnosis could take years. But evidence accumulated during the past decade suggests the possibility of early diagnoses using an advanced brain-imaging scanner and the combination of genetic and other biometric data. With the test, we are able to make a positive clinical diagnosis of probable Alzheimer's, with approximately 90 per cent accuracy, as long as 30 years before onset. Would you be interested in such a test?"

Due to the lower prices of screening devices, primary care doctors and specialists are no longer reticent in suggesting this procedure to patients. Moreover, their hospitals receive funds for the use of this device from the government (which is increasingly interested in the early detection of AD). Patients are assured that their data will remain confidential. The government recently adopted a law obliging service providers to protect patient anonymity and to destroy personal data immediately after the test. Laura's hospital subcontracts the AD screening to a service provider who protects the anonymity of AD test results (stored in temporary databases) through the use of biometrics.

Laura agrees to take the test. A few weeks later, she receives terrible news: her results confirm the onset of AD. This is a deep shock. Her life will never be the same again. She starts thinking about the changes for her family. The children of AD patients can suffer physically and emotionally as their parents are no longer able to look after themselves. "I will lose awareness of my surroundings and become dependent on others," she thinks. She is also concerned that she will be unable to continue in her profession. AD patients are often forced into early retirement and may not have access to the full range of benefits available to those who retire at the minimum age set by the government. For this reason, she decides to take out special medical and life insurance coverage to protect her family and herself.

A few days after the insurance request is sent, however, she receives a letter: "We regret to inform you that your application for the selected health insurance coverage plan has been rejected." There being no apparent reason for this, Laura wonders whether a link can be established between the AD screening service and the insurance company. She decides to contact an investigative journalist, Nigel. Nigel discovers that the insurance company recently bought a new device able to extract biometric templates from the so-called "accidentally built virtual face databases" and to create specific databases according to previously selected criteria. A database of people living in the area was created. "But the big news," Nigel says, looking at Laura while slowly sipping his tea, "is that an employee of the AD screening service provider was selling anonymous test results to the insurance company, who were able to match the biometric identifiers found in the test results with the previously established database."

The "big scoop" concerning health insurance discrimination is immediately published in the local and national press, and causes widespread indignation among the public. Concerns are raised over the potential for biometrics to be used as a key to link sensitive personal information from different sources. The news also alerts the government, who assure the electorate that immediate action will be taken to curb this form of discrimination. In particular, the National Health Agency decides to launch a stakeholder consultation on ensuring responsible identity management and the protection of anonymity in healthcare sector services.

Ethical dilemma

The scenario highlights the ethical dilemma wherein governments and the private sector like the great increase in security brought about by reliable facial recognition technologies, but, acting responsibly, see the damage it causes to privacy, which is a cornerstone of democracy. The scenario focuses on the trade-off between privacy and security, also explores issues related to consent and trust.

3.6 Dragonfly drones

Rachel Finn (Trilateral Research & Consulting)

Type of scenario: Democratisation of surveillance (Quadrant 4)

This is a democratisation of surveillance scenario because it depicts the ready availability of low-cost surveillance technology to all citizens. The downside of such ready availability is that it makes it harder for the police to catch evil-doers.

The scenario

Police superintendent Max Eggleton gets into a taxi cab on his way to an interview with a journalist from the *Daily Post*. He asks to be taken to Journal Square and sits back in his seat to clear his mind in preparation for the interview. As he looks out the window, he surveys the innumerable tiny dots – dragonfly drones – hovering above people's heads on the street, outside windows and flying overhead and sighs to himself. In fact, it is precisely these dragonfly drones that are the subject of his interview with the journalist. He feels a mix of helplessness and frustration as his taxi cab travels through the downtown streets.

During the cab ride, Eggleton recalls how the 2015 relaxation of the Federal Aviation Authority (FAA) and European Aviation Safety Agency (EASA) rules surrounding the use of unmanned aircraft systems resulted in an explosion in the numbers of these small aircraft in the skies. Journalists and the Highways Agency began using drones to monitor traffic flows and generate alerts about accidents and other incidents, private security firms started using them to monitor buildings and sites they are contracted to guard, schools acquired drones to ensure students stay in the grounds during the day and the police began using them to assist in surveillance, evidence gathering and incident response. In addition to these corporate or official uses, the proliferation of do-it-yourself drones has also resulted in ordinary citizens having access to affordable dragonfly drones in large numbers.

Ordinary citizens are primarily using drones harmlessly to monitor and record their lives and activities, to which Eggleton does not object. He has seen wedding photographers using drones not much bigger than a dragonfly to record videos since they can get closer to the couple and produce pictures from almost any angle without disrupting the ceremony. Sports professionals use small drones to record their movements and play in order to produce individualised recordings to help them optimise their moves. Young people play with their personal drones for life-logging, as an accompaniment to social media to record their daily lives in case an incident worthy of being uploaded to their pages should occur. However, Eggleton knows that other citizens are using these drones for more sinister means. Neighbours have begun using this technology to covertly monitor one another's activities, including infidelity, anti-social behaviour and activities that generate terrorism-related suspicion. Furthermore, some criminals and anti-government activists have begun using dragonfly drones to monitor police locations and activities. It is precisely these counter-surveillance activities that have been thwarting the police force's ability to collect evidence against suspects or carry out effective raids. As Eggleton's taxi pulls up in Journal Square, he wonders how he is going to "sell" the need for better regulation of dragonfly drones to the *Daily Post* journalist who will likely be sympathetic to industry's resistance to further regulation.

Eggleton meets the journalist in the bar of a hotel just off Journal Square. The two greet one another, choose a table and order coffees from the waiter. Once the coffees arrive and each has added their cream and sugar, the journalist leans forward in her chair. "Superintendent Eggleton, I understand you have a lot of experience using dragonfly drones as part of your police work. Why then are you calling for better regulation of these devices?"

Eggleton considers for a moment and answers, "Technology that is not commonly available to the general public has often been available to the police, so long as specific oversight mechanisms have been in place. When police use drones, and particularly when they use these so-called dragonfly drones that can be deployed covertly, we must ensure that citizens' civil liberties, including their privacy, is taken into full consideration. However, citizens who use these drones do not have to pass such rigorous oversight requirements, with the effect that many citizens are infringing upon one another's privacy and civil rights through covert surveillance and on one another's civil liberties through protecting criminal networks."

The journalist queries, "How have drones been protecting criminal networks?"

Eggleton responds, "Drones are currently being used to monitor the spaces in which crimes are being conducted, the properties in which criminals are conducting business and the homes in which they live. Dragonfly drones have the ability to identify objects or people in the surrounding area. They can identify the drones the police are using to collect evidence or protect police officers and they can detect the presence of police officers in the vicinity. They make it much more difficult for the police to catch criminals in the act, because they are aware that police officers are approaching, and they can flee once they are aware that police raids are about to occur. Previously, police could assemble for a raid a few streets away from the target and move in once they were fully prepared. Now, with dragonfly drones, police do not even realise that they themselves are being monitored and the target has slipped away before the police raid the premises."

He continues, "The use of dragonfly drones by citizens has another consequence: Criminals are using drones to monitor police activities, procedures and habits. Thus, they have more information about the police than the police do about them. This information asymmetry also assists criminals in avoiding detection or arrest. For example, first response officers almost always arrive in teams of two officers per car. Criminals can judge whether to fight or flee by using intelligence gathered from drones to assess the number of cars, and thus the number of police officers, responding to their activities. In contrast, the police often have no idea how many individuals they will encounter once they arrive at the scene."

"That's all well and good," says the journalist. "However, industry lobbyists point out that it is individuals who are committing these offences, not the drones themselves. And, in fact, many consumers are using drones for recreational activities responsibly. They also point out that any restrictions on the development and use of drones could stifle innovation and harm the economic competitiveness of the region. How would you respond to their position?"

Again, Eggleton considers for a moment and then responds, "The police are not anti-innovation or anti-recreation. We simply wish to continue protecting citizens by responding effectively to police call-outs and catching criminals. Some sort of oversight is necessary to ensure that those who purchase drones for recreational purposes are aware of how their activities may infringe upon privacy and other civil liberties, and to keep drones out of the hands of those who may be seeking to use them for criminal purposes. Currently, the police are accountable to government authorities, and ultimately citizens themselves, in how we deploy and use drones. Citizen users are not accountable to anyone."

At this, the journalist smiled and said, "Thank you for your time, Superintendent and I apologise that our conversation has to be so brief. I have just one final question. How should policy-makers respond to your call today to regulate the use of dragonfly drones by citizens?"

Eggleton returned her smile and said, “Well, I’d like to see them banned for everyone except the police.”

“That’s not going to happen,” said the journalist. She too uses the dragonfly drones and there is absolutely no way she is going to stop.

“But,” Eggleton continued, “the technology is becoming so widely used that it would be like trying to regulate mobile phones. We know that. Still, I think we need to have some kind of assessment of the impacts of this technology, some wide discussion or consultation with everyone who has an interest. I don’t have a solution to propose, and I’m not pushing one, except that I believe we need a discussion of the impacts these dragonfly drones are having on our society.”

Ethical dilemma

The proliferation of dragonfly drones creates an ethical dilemma for policy-makers and the police. Such technology in the hands of evil-doers thwarts the efforts of the police to catch evil-doers, because the latter can use dragonfly drones to surveil the police, to see where they are. While policy-makers want to regulate such technologies, they are facing enormous pressure from manufacturers and vendors who tell them to get off the back of the free market, to stop over-regulating the market. The scenario also raises other ethical issues, notably accountability, because people who have their own drones are not accountable to any authority for their use. Ironically, such technology overcomes an information or power asymmetry that the police and security services have typically had over ordinary citizens, but as a consequence, overcoming such an information and power asymmetry has made it much harder for the police to do their jobs, to catch evil-doers.

3.7 An analysis of five ethical dilemma scenarios

David Wright (Trilateral Research & Consulting)

The most obvious factor in the five scenarios is (or should be!) that each presents an ethical dilemma which has been summarised at the end of each scenario. There are various methodologies for constructing and deconstructing scenarios. Only four are mentioned here, and the last three are related and, we believe, the most relevant.

Bjork-Schwartz methodology

Staffan Björk set out the major steps in creating orthogonal scenarios (or futures), like those that we have created, as follows:

- identify a focal issue and determine the time frame;
- identify key factors;
- search for the unknown driving forces behind the key factors;
- organise forces in scale of importance and uncertainty;
- pick important and uncertain forces and create a scenario matrix or a few scenarios by combining forces;
- evaluate the focal question in each scenario;
- identify indicators that tell in which direction the environment is heading.[34]

[34] See Björk, Staffan, “Designing Mobile Ad Hoc Collaborative Applications: Scenario experiences with Smart-Its”, Position paper at the Mobile Ad Hoc Collaboration Workshop at CHI 2002, p. 2. Bjork’s list of key points appears to have been adapted from Schwartz, Peter, *The Art of the Long View*, John Wiley, Chichester, 1998, pp. 241-247.

SWAMI's deconstruction methodology

However, the scenarios can be analysed (or deconstructed) according to several criteria. The SWAMI methodology is helpful here. The SWAMI consortium[35] devised a methodology, an analytical structure for both constructing and deconstructing scenarios, not only the SWAMI scenarios, but many other technology-oriented scenarios. The analytical structure comprises the following elements or activities.[36]

Framing the scenario

This first step summarises the scenario in question and explains its context—who are the main actors in the scenario, what happens to them or what do they do, how far into the future is the scenario set, where does it take place and in what domain (home, office, on the move, shopping, etc.). It identifies the type of scenario (trend, normative, explorative) and key assumptions (e.g., intelligent technologies will be embedded everywhere in rich countries, but not in poor countries).

Identifying the technologies and/or devices

Next, the most important AmI technologies and/or devices used and/or implied in the scenarios are identified.

Identifying the applications

The analysis then considers the applications that emerge in each scenario and that are supported by the technologies mentioned in the previous step.

The drivers

At this step, the analysis identifies the key drivers that impel the scenario or, more particularly, the development and use of the applications. Drivers are typically socio-economic, political or environmental forces or personal motivations (e.g., greed).[37]

Issues

Next, the major issues raised by the scenarios are identified and explicated. In the SWAMI scenarios, the issues of concern, as mentioned above, are privacy, identity, trust, security and inclusiveness (or its opposite, the digital divide). A discussion of the issues considers the threats and vulnerabilities exposed by the scenario as well as their impacts and legal implications.

Conclusions

The final step is a reality check of the scenario itself (how likely is it? are the technologies plausible?) and a consideration of what should be done to address the issues it raises. One might conclude, as the

[35] Three of the four PRESCIENT partners were also partners in the SWAMI project.

[36] This concise description of the SWAMI methodology has been extracted from Wright, David, "Alternative futures: AmI scenarios and Minority Report", *Futures*, Vol.40, No.5, June 2008, pp. 473–488 [pp.481-482]. For a more in-depth description, see Wright, David, Serge Gutwirth, Michael Friedewald et al. (eds.), *Safeguards in a World of Ambient Intelligence*, Springer, Dordrecht, 2008.

[37] Schwartz, op. cit., p. 101, says "The process of building scenarios starts with he same thing that the priests did – looking for driving forces, the forces that influence the outcome of events… Driving forces are the elements that move the plot of a scenario." He says driving forces could be social, technological, economic, political or environmental. He goes on to say (p. 108) that after identifying and exploring the driving forces, one must uncover he "predetermined elements" and the "critical uncertainties". "Predetermined elements do not depend on any particular chain of events. If it seems certain, no matter which scenario comes to pass, then it is a predetermined element." (p. 110).

SWAMI partners did, that a range of socio-economic, technological and legal safeguards are needed in order to minimise the risks posed by the threats and vulnerabilities highlighted by the scenario.

ENISA scenario analysis

The European Network and Information Security Agency (ENISA) built on the SWAMI methodology[38] and took it further to analyse threats, vulnerabilities, risks and controls posed by the development of new technologies.

ENISA and its expert groups on emerging and future risks (EFR) analysed scenarios in order to identify and extract all the elements needed in order to proceed with its risk assessment and management. The elements to be identified are:

- *Assets (tangible and intangible)* – What assets are mentioned or implicit in the scenario?
- *Vulnerabilities* – What vulnerabilities are apparent or can be perceived in those assets?
- *Existing controls* – What controls appear to be in place or could or should be put in place to safeguard the assets, especially in terms of their vulnerabilities?
- *Threats* – What threats are referenced in the scenario or are implicit or can be imagined?
- *Impact* – If the assets are attacked or compromised in some way, what would be the impacts?
- *Acceptable risk level* – Given the probability of a risk and its potential consequences, what is regarded as an acceptable level of risk?
- *Assumptions* – What assumptions have been made or seem apparent in the scenario analysis, e.g., in terms of the vulnerabilities, threats, impacts and risk acceptability?

PRESCIENT scenario analysis

For the purpose of analysing the PRESCIENT scenarios, we can adapt the above methodologies and, in particular, identify for each scenario:

- The framing of the scenario
- The technologies
- The applications
- The drivers
- The privacy risks
- The ethical issues
- The controls
- The conclusions

As a test of this approach to deconstructing ethical dilemma scenarios, we apply the methodology to the first scenario ["Privacy is dead. So what (yawn)"].

Framing the scenario

The scenario is set 10 years into the future. It concerns a young woman, Katherine, a bank manager, who likes to party and go dancing with her friends. She uses the latest technologies as a matter of routine.

[38] See, for example, the credit given to the SWAMI methodology in ENISA, *'Being diabetic in 2011': Identifying emerging and future risks in remote health monitoring and treatment*, European Network and Information Security Agency, Heraklion, 2009, p. 26.

The technologies

The scenario refers to several technologies, notably Katherine's smartphone equipped with near field communications (NFC). It also refers to others such as data aggregation, data mining, profiling, targeted advertising, RFID, biometrics (including DNA), location determination, and even an old technology (television).

The applications

She can use the smartphone for multiple functions, including paying for her transport, some of which she initiates and some of which are initiated by others who sense her presence (she is targeted with adverts). The scenario refers to what is today called "big data", i.e., the aggregation of massive databases for e-government and other purposes. Katherine likes the new shopping applications which make use of her personal data. Most of the technologies mentioned in the scenario are used for surveillance and targeted marketing applications. "Smart" technologies seem to be embedded and ubiquitous in Katherine's world.

The drivers

The development of the new technologies and applications referenced in the scenario seem impelled by organisations wanting to target individual consumers, to maximise the efficiency of their marketing and advertising budgets. Efficiency also drives the government who gradually sub-contracts all public services to the private sector, despite the risk of companies repurposing personal data. Katherine makes use of the new technologies and applications because they offer a high degree of convenience. She seems to be relatively "tech-savvy", although totally unconcerned about her personal privacy. Like so many people today, she seems afflicted by the disease of consumerism. The need to protect privacy is still a driver 10 years in the future as demonstrated by the fact that a privacy advocate gets some air time on televisions and argues his case forcibly, even if it falls on deaf ears in Katherine's case.

The privacy risks

The privacy risks are not something she gives any thought to. On the contrary, she doesn't see what the fuss is all about. Hence, she makes no effort to anonymise or encrypt her personal data, partly because she doesn't see the need. The privacy advocate in the televised debate points out some of the privacy risks. Intrusiveness is one, but the privacy advocate also notes privacy violations arising from the aggregation, mining and repurposing of data, from the absence of consent, data minimisation, data quality and purpose specification. Most disturbing is that these violations take place "mindlessly". The advocate points out the risk to personal autonomy – i.e., free will, free choice is compromised if consumers are being manipulated by targeted advertising. Furthermore, "the systems" that target consumers are opaque, and the implications extend beyond the individual to society as a whole – there are power asymmetries, discriminatory practices and government-industry collusion. Pervasive surveillance can be used to track suspect and socially undesirable behaviour, which threatens the general presumption of innocence, a cornerstone of the constitutional democratic state.

The ethical issues

This scenario also raises ethical issues, which are briefly highlighted at the end of the scenario. The ethical dilemma arises from the conveniences offered by new technologies and the sacrifices made in privacy. It also raises other ethical issues relating to the freedom to opt out and function creep, whereby many applications and technologies serve purposes not originally specified upon their first introduction. As noted above, the scenario makes clear that the privacy and ethical issues go well beyond those affecting just an individual, but have implications for society as a whole, indeed for democracy itself.

The controls

The scenario seems to suggest that there are few controls in place 10 years hence. Government and industry "collude" in sharing and outsourcing data to the private sector which is then relentlessly repurposed. Constitutional and legal safeguards seem to be ignored or are virtually unenforceable by virtue of the widespread violations. The only controls seem to be the warnings from privacy advocates and the media willingness to give airtime to them.

The conclusions

A privacy and ethical impact assessment (P+EIA) might or might not be helpful in the future depicted in this scenario. Once new technologies are deployed, there is little point in conducting a privacy and ethical impact assessment in the sense that such an assessment would help to identify risks and propose solutions for overcoming those risks only if it's possible to influence the design of the technology. All of the technologies referred to in the scenario are fully deployed, so a P+EIA will not be able to influence those. Technology development continues apace, however, so there could still be value in carrying out a privacy and ethical impact assessment as new technologies emerge, before they are deployed, when there is still a possibility of influencing the outcome. Even so, one wonders whether, in the dark scenario presented here, the future has already been compromised. Privacy is so rampantly violated and consumers have already been so "brain-washed" that many stakeholders may no longer see the point of an impact assessment.

Ethical issues raised in the scenarios

In this section, we briefly summarise the key ethical issues raised in the five scenarios set out above.

Scenario 1 ("Privacy is dead") sets out an ethical dilemma, especially for policy-makers, i.e., which could be summarised in these questions: Should the convenience of new technologies be allowed to compromise traditional democratic values, such as privacy? Should society accept the inevitability of function creep and the repurposing of personal data?

Scenario 2 ("The presidential candidate") sets out an ethical dilemma for a presidential candidate who is behind in the polls, who is being urged to do what other politicians are doing, i.e., to use the power of Internet tracking technologies and social sorting. She does not want to compromise her image as a "clean" candidate, and prefers not to use data analytics to prey on the prejudices, fears, apprehensions, behaviour, proclivities of voters. What should she do? (One possibility might be to "go public", to inform the electorate about how the new technologies are being used to manipulate their voting intentions.)

Scenario 3 ("The Bionic Soldier") highlights an ethical dilemma spawned by new technologies (implants) and pharmaceuticals which gives rise to a tension between the enhanced and non-enhanced. Can society justify two classes of individuals, those who have been enhanced and those who haven't been? The scenario raises other ethical issues, notably equity, fairness and power asymmetries.

Scenario 4 ("Facial give-away") highlights the ethical dilemma wherein governments and the private sector like the great increase in security brought about by reliable facial recognition and biometric technologies, but, acting responsibly, see the damage it causes to privacy, which is a cornerstone of democracy, when, for example, insurance companies gather such data and use it to discriminate against certain individuals (those with Alzheimer's or with a strong possibility of getting the disease). The scenario raises ethical issues relating to consent and trust. The government, again acting responsibly, assures the electorate that immediate action will be taken to curb this form of discrimination and the National Health Agency decides to launch a stakeholder consultation on ensuring responsible identity management and the protection of anonymity in healthcare sector services.

Scenario 5 ("Dragonfly drones") highlight an ethical dilemma for policy-makers and the police, i.e., can or should anything be done to curtail the private use of dragonfly drones, when it is apparent that it is thwarting the efforts of the police to catch evil-doers. While right-thinking policy-makers might want to regulate such technologies, they are facing pressures from manufacturers and vendors who want government to get off the back of the free market, to stop over-regulating the market. The scenario also raises other ethical issues, notably accountability, because people who have their own drones are not accountable to any authority for their use.

The way forward: privacy and ethical impact assessment

The PRESCIENT partners advocate "What-if" scenarios, such as those set out in this report, as a useful tool in identifying privacy and ethical issues arising from the development and deployment of new and emerging technologies. Scenarios, as mentioned at the beginning of this chapter, are a useful tool in drawing to the attention of policy-makers and decision-makers as well as other stakeholders some of the issues that could arise in future. They are intended to provoke discussion and, with luck, debate among stakeholders will lead to consensus on how to address the issues highlighted in the scenarios – but also to be alert to other issues that might arise too. For example, discussion of the scenarios and the ethical issues identified in the preceding section may lead to the identification of other issues that were not initially apparent or even explicit in the scenarios.

In most, but not all of the scenarios, a Privacy and Ethical Impact Assessment (P+EIA) will be useful to address not only the privacy issues, but also the ethical issues. There is a qualification here of "most, but not all", simply because some of the technologies and/or applications are already fully formed. If the use of P+EIA is introduced even earlier than the timeframe of the scenarios – i.e., when the technologies or applications are still being considered, the P+EIA instrument will have greater value because it could, theoretically, be used to influence the design or even use of particular technologies and applications.

While a P+EIA is an important instrument for uncovering privacy and ethical risks, its effectiveness depends on how well it is structured.

As is apparent from some of the above scenarios, one cannot rely on a single instrument in resisting intrusive privacy practices or discrimination. In the last scenario, on dragonfly drones, Eggleton, the police commissioner, is talking to the press. Media attention is an important instrument. Similarly, when Laura (in the "facial give away" scenario) discovers she has been refused insurance because the insurance company discovered she had incipient Alzheimer's disease, she goes to the media to draw attention to the linkage between her personal data and discrimination by the insurance company. Fortunately, the government is responsive to such inequities. In the scenario on the tension between the enhanced and non-enhanced citizens, public opinion is an important factor in combatting discriminatory practices. And, as just mentioned, a responsive government is also important.

Before presenting the PRESCIENT P+EIA framework (Chapter 6), in the following Chapters we will analyse the legal provisions on PIAs at the EU level (Chapter 4) and we will give an overview on current approaches to privacy and ethical impact assessment of emerging technologies, discussing the main philosophical and methodological challenges of such methodologies (Chapter 5).

4. Key provisions of EU data protection and privacy legislation

Raphael Gellert and Serge Gutwirth (Vrije Universiteit Brussels)

This chapter will flesh out the different provision relating to privacy and ethical impact assessment (respectively PIA and EIA) that can be derived from the EU legal framework.

We note from the outset that the EU legal framework has provisions for only PIAs; it is silent on EIAs.

In the first section of this chapter, we describe the existing legal framework. The description evidences the fact that the only references to PIAs are to be found in data protection provisions.

We then try to analyse this pattern by drawing from the human rights conceptual differentiation between positive and negative obligations, as developed by the European Court of Human Rights, with the right to privacy drawing predominantly on negative obligations, and the right to data protection embedded into positive obligations. Pursuant to this analysis, we will purport that PIAs represent such positive obligations, which might account for its presence within data protection instruments.

This stance is confirmed to the extent that the European Commission's proposal for a general data protection regulation not only includes a provision dedicated to PIAs, but even goes so far as renaming them into data protection impact assessments (DPIAs).

We conclude by speculating on whether it is reasonable to expect meaningful (privacy) protection from (yet another) data protection instrument.

4.1 The existing EU legal framework

As has been described in the first PRESCIENT Deliverable, the EU privacy and data protection legal framework is composed of several instruments and provisions. The latter stem from EU instruments, as well as from Council of Europe instruments and case-law [from the European Court of Human Rights (ECtHR)], which is also part of the EU legal order.[39]

In the same Deliverable we made the conceptual distinction between the rights to privacy and data protection.

Whereas the right to privacy is enshrined in one sole provision, Article 7 of the EU Charter for Fundamental Rights (EUCFR), which replicates Article 8 of the European Convention of Fundamental Rights (ECHR), the right to data protection is scattered among several instrument with different legal statuses.

The main instrument is Directive 95/46/EC, known as the data protection directive.[40] It contains the main principles concerning the manner in which the personal right to data protection must be protected.

Other relevant EU instruments include the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters of 27 November 2008,[41] the 2002/58/EC Directive (E-Privacy Directive), which actualises the data protection principles to face some of the new challenges raised by continuing developments in the electronic communications sector.[42]

[39] See Gutwirth et al., PRESCIENT Deliverable 1, 2011, pp. 5ff.

[40] European Parliament and the Council, Directive 95/46/EC 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. OJ L 281, 23.11.1995.

[41] Council Framework Decision 2008/877/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L350/60, 30.12.2008. This Framework Decision aimed to fill the gap left by the restricted scope of the Data Protection Directive, by providing a regulatory framework for the protection of personal data in the area of police what was called the "third pillar" before the entry into force of the Lisbon Treaty.

[42] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O. J. L 201, 31/07/2002, p. 0037 – 0047. Recital 4 mentions that the aim of the directive

This Directive has been amended by Directive 2006/24/EC known as the data retention directive,[43] and by Directive 2009/136/EC.[44] Regulation EC No. 45/2001 regulates the protection of individuals with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data.[45] This Regulation is particularly important because, inter alia, it created the European Data Protection Supervisor (EDPS), an autonomous EU institution with the powers of supervision, consultation and co-operation (Art. 41).

In addition, Art. 16 of the Treaty of Lisbon on the Functioning of the European Union (TFEU) enacted a general constitutional provision on data protection[46] and it gave the EUCFR binding force in the EU.

It is interesting to compare the institutional structure of the two rights. On the one hand, the right to privacy is constituted of one single provision with quasi-constitutional status (two including the ECHR). On the other hand, the right to data protection is composed not only of two provisions with quasi-constitutional status (Article 8 of the EUCFR and Article 16 TFEU), but also of several instruments (Directives, a Regulation, and a Council Framework Decision) with quasi-legislative status that can be seen as implementations of such quasi-constitutionally enshrined right.

The former observation is not without consequences for our argument. Since the legal instruments enshrining the right to privacy solely contain provision concerning the content of this right (and the conditions under to which to derogate therefrom), it literally entails that there are no provisions concerning privacy impact assessments.

Therefore, if there are any provisions concerning privacy impact assessments, the former suggests that they should/would be found in data protection legislation.

Is this the case?

There are no legal bases for PIA in the existing framework. However, it can be argued that some provisions contain what has been coined as forerunners of PIA –since they also focus on anticipative measures to be taken in the view of potential risks associated with future processing operations, namely prior checking and prior consultation.[47]

Art. 20 of the data protection directive establishes prior checking,[48] and Art. 28 empowers the national data protection authorities (DPAs) with prior consultation functions.[49]

is to translate “the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector”.

[43] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal L 105, 13/04/2006,* p. 0054 – 0063.

[44] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws Text with EEA relevance, *Official Journal L 337 , 18/12/2009,* p. 0011 – 0036.

[45] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1, 12.01.2001.

[46] “Everyone has the right to the protection of their personal data” (art.16[1] TFEU).

[47] See, PIAF, D.1., A Privacy Impact Assessment Framework for data protection and privacy rights, especially p. 200, and p. 202. On prior checking and prior consultation as PIA forerunners, see also Luiz Costa, “Privacy and the precautionary principle”, *Computer Law & Security Review*, Vol. 28, No. 1, 2012, pp. 14–24.

[48] Art. 20 provides that: “1. 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.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

Regulation 45/2001, regulating processing of personal data by EU institutions and bodies, equally endows the EDPS with similar powers in terms of checking,[50] and consultation.[51]

Similarly, the Council Framework Decision 2008/977/JHA provides for prior consultation.[52]

In addition to these binding instruments, provisions related to PIA can be found in non-binding (i.e., soft law) EU instruments, and in particular in the European Commission's (EC) Recommendations.[53] In 2009, the EC issued a Recommendation laying down the legal basis for a RFID PIA Framework.[54]

This PIA Framework in the field of RFID has the status of a Guidance Document as has been produced by the Art.29 WP. In conformity with the provisions of the EC Recommendation, the latter has endorsed the document after a multi-stakeholders consultation and drafting process.[55] Following the Commission's Recommendation, the industry and other relevant stakeholders prepared the RFID PIA framework. On 31 March 2010, they submitted it for endorsement to the Art. 29 Working Party. On 13 July 2010 the Working Party rejected it.[56] The revised Framework was submitted on 12 January 2011. On 11 February 2011 the Working Party finally endorsed the RFID PIA framework.[57]

In addition to this privacy-specific impact assessment framework, one should also briefly mention the more general regulatory impact assessment (RIA) framework.[58]

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards."

[49] Art. 28 provides that: "(…) 2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

"– effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions."

[50] Art. 27 of the Regulation provides that: "Processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes shall be subject to prior checking by the European Data Protection Supervisor."

[51] Art. 28 of the Regulation provides that: "1. The Community institutions and bodies shall inform the European Data Protection Supervisor when drawing up administrative measures relating to the processing of personal data involving a Community institution or body alone or jointly with others.

2. When it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission shall consult the European Data Protection Supervisor."

[52] Art. 23 provides that: "Member States shall ensure that the competent national supervisory authorities are consulted prior to the processing of personal data which will form part of a new filing system to be created where:

(a) special categories of data referred to in Article 6 are to be processed; or

(b) the type of processing, in particular using new technologies, mechanism or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the privacy, of the data subject."

[53] According to Art. 288 TFEU, a Recommendation is a non-binding instrument. This entails that the addressee of the Recommendation is called on, but not placed under any legal obligation to abide by it.

[54] European Commission, Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C(2009) 3200 final..

[55] According to Art. 4 of this Recommendation, "Member States should ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments. This framework should be submitted for endorsement to the Article 29 Data Protection Working Party within 12 months from the publication of this Recommendation in the Official Journal of the European Union."

[56] Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 175.

[57] Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180.

[58] On the legal status and binding force of impact assessments, see PIAF, D.1., op. cit., p. 203; and Meuwese, A., *Impact Assessment in EU Lawmaking*, Ph.D. Thesis, Uni. Leiden, 2008, pp. 102-104.

RIAs are part of the Better Regulation Action Plan.[59] In short, they aim at improving the quality of the legislative work of the EU institutions (by anticipating their potential negative impacts and shortcomings).[60]

Among the three major steps that need to be taken in order to conduct an impact assessment,[61] the first one deals with the identification of economic, social and environmental impacts. Social impacts include impacts concerning "*Individuals, private and family life, personal data"*.[62]

4.1.1 Impact assessment provisions to be found in data protection instruments

There is something that looks to some extent like a contradiction in terms when one analyses the former section[63]: the only provisions relating to privacy impact assessments are not to be found within privacy instruments, but instead in data protection tools.

In the following lines, we will attempt first to provide some explanations that might be of help, especially in view of the EC Proposal for a Data Protection Regulation (cf. *infra*, 5.3.3).

4.1.1.1 Negative and positive human rights obligation as a heuristic for (potential) explanation(s)

In the first PRESCIENT Deliverable, we have tried to render the conceptual difference between privacy and data protection by resorting to the concepts of *opacity* and *transparency*.

Accordingly privacy is an *opacity* tool, that is, a prohibitive and normative tool that determines whether an interference with individual autonomy is acceptable or not.[64] If such interference is deemed unlawful then the state must restrain from interfering with the right. The fact that the State should refrain from interfering with the right to privacy pertains to the classical notion of (civil and political) human rights whereby states must refrain from acting in order to protect fundamental liberties, they must take no action that could interfere with the full enjoyment of the right.[65] In other words, they are under the negative obligation not to act.[66]

[59] European Commission, Communication from the Commission on impact assessment, COM(2002) 276 final.

[60] European Commission, *Impact Assessment Guidelines*, SEC(2009) 92, pp. 4-6.

[61] Ibid., p. 31 et s.

[62] Ibid., p. 35. These impacts include the following questions to be asked: does the option impose additional administrative requirements on individuals or increase administrative complexity; does the option affect the privacy of individuals (including their home and communications); does it affect the right to liberty of individuals; does it affect their right to move freely within the EU; does it affect family life or the legal, economic or social protection of the family; does it affect the rights of the child; and, does the option involve the processing of personal data or the concerned individual's right of access to personal data?

[63] Which deals with privacy impact assessments provisions within the EU legal framework for privacy and data protection.

[64] Gutwirth et al., PRESCIENT Deliverable 1, 2011, p. 8. See the references in Fn. 27 and 28.

[65] J.-F., Akandji-Kombe, Les obligations positives en vertu de la Convention européenne des Droits de l'Homme. Un guide pour la mise en oeuvre de la Convention européenne des Droits de l'Homme, Strasbourg: Council of Europe, 2006, pp. 5 and 11 ; de Schutter, Olivier, *International Human Rights Law*, Cambridge: University Press, 2010, pp. 241 et s. There is a huge literature on the concepts of positive and negative obligations. Among the many referencesare the following ones: St. Braconnier, Jurisprudence de la Cour européenne des droits de l'homme et droit administratif français, Bruxelles, 1997, pp. 318-322; F. Sudre, « Les 'obligations positives' dans la jurisprudence européenne des droits de l'homme », R.T.D.H., 1995, pp. 363-384; J. Vande Lanotte, Y. Haeck, Het Europees verdrag tot bescherming van de rechten van de mens in hoofdlijnen, Antwerpen, Maklu, 1997, Part. I, pp. 186-196; S. Van Drooghenbroeck, La proportionnalité dans le droit de la Convention européenne des droits de l'homme. Prendre l'idée simple au sérieux, Bruxelles, Bruylant, 2001, pp.135 et s.

[66] That is not to say that opacity tools and negative obligations can be equated. Rather, they constitute two different perspectives to look at one same object: the right to privacy. The "opacity perspective" will put the emphasis upon the normative dimension that is at work in the right to privacy: this right is about determining whether a given action from the government is legal or not. The "obligation perspective" is about what the state should do in order to safeguard such right. In other words, the "opacity perspective" asks the question: "can one interfere with this right?", whereas

Instead, we have coined data protection a *transparency* tool, that is, a tool that channels the normatively accepted exercise of power through the use of safeguards and guarantees in terms of accountability and transparency. Data protection legislations obey such logic: they generally do not dispute the fact that personal data might be processed, but they submit the processing to rules and conditions, they empower data subjects by giving them subjective rights and they establish supervisory bodies in order to make sure that data processors don't abuse their powers.[67] In such case, the state is under an obligation to act, and more precisely, to take guarantees in terms of accountability and transparency. In other words, the safeguard of the right to data protection entails that the state take some measures. This very much resembles the notion of (human rights) positive obligations whereby the state must take the measures that are necessary for the safeguard and full enjoyment of a right,[68] or more accurately, must take measures that are deemed reasonable and adequate in order to protect, guarantee and safeguard the rights of the individual.[69][70]

As a traditional civil and political human right, the right to privacy will in general spur negative obligations.[71] On the contrary, it might be the case that the right to data protection can only be understood in terms of positive obligations. Indeed, it can be argued that data protection accepts *by default* the processing of personal data, as evidenced by article 1 of the directive,[72] and that the very content of the right -the constitutional protection embedded in it, is constitutive of a set of principle that aim at making sure that the data processor does not abuse its power.[73] Some of these principles concern the quality of the processing, that is the manner in which it can be conducted, what can be done or not, but other principles are accountability and transparency measures to be implemented by the data processor. In short, it is not possible to think of the protection offered by "data protection" without thinking the involvement of the data processor (be it the state or a private party). There can be no protection if there is no processing![74]

the obligation perspective asks the question: "how should one protect this right?". There is however some overlap since the cases wherein the "opacity perspective" leads to the conclusion that there should be no interference with the privacy of the individual will correspond to a negative obligation of the State. However, the right to privacy can also lead to positive obligations, cf. *infra*.

[67] Gutwirth et al., PRESCIENT Deliverable 1, 2011, p. 8. See the references in Fn. 27 and 28.

[68] Hokkanen vs Finland, 24.08.1994.

[69] *López-Ostra*, 9.12.1994.

[70] *Mutatis mutandis* with our observations concerning the relation between opacity tools and negative obligations, the point is not to equate *transparency tools* and positive obligations. Rather, and similarly to the "opacity perspective", the point of the "transparency perspective" is to shed light on the normative dimension embedded within (in this case) the right to data protection, and accordingly to spell out the power relations at work within this right, that is, the latitude given by the institutional architecture of the constitutional democratic state to influence and steer citizens' behaviours if one is to use the vocabulary of Michel Foucault (See the references to the work of Foucault *in* De Hert, Paul, and Serge Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in Erik Claes, Anthony Duff et al. (eds.), *Privacy and the criminal law*, Intersentia, Antwerp, Oxford, 2006, pp. 75-85). Yet, in the case of data protection, the balance of forces (between the citizen and the government) sought by the democratic constitutional state entails that in order to be allowed to process citizens' data (and hence, acquire some control over the latter), the government must take some measures, that is, is under an obligation to act; which corresponds to the positive obligation notion. Contrary to privacy, where positive obligations are also possible, the author is at trouble in finding negative obligations with regards to data protection.

[71] The right to privacy has been enshrined all major international human rights instruments. E.g., Art. 12 Universal Declaration Human Rights; Art. 17 International Covenant on Civil and Political Rights; Art. 8 of the European Convention on Human Rights… See also J.-F., Akandji-Kombe, op.cit., p. 5.

[72] Art. 1 states that: "(...) Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" (we underline). It is clear here that the protection offered is always in relation to an already existing processing.

[73] On the troublesome content of this right, see Gloria González Fuster, Gellert R., The fundamental right of data protection in the European Union: in search of an uncharted right, International Review of Law, Computers & Technology, 26:1, 2012, pp. 73-82.

[74] This should come as no surprise. Indeed, one must remember that the situation that led to the advent of the right to data protection was that of the emergence of computerised systems, which themselves gave birth to new practices of

Yet, whereas it seems impossible to think of data protection outside of the positive obligations framework, it is nonetheless possible to conceive of positive obligations in the case of privacy.

Positive obligations understood as measures (legal but also very practical) that the state must take in order to guarantee that citizens are well in a position to enjoy their human rights are part of the ECHR case-law concerning the right to privacy (or, in the wording of the Convention: "the right to respect for private and family life"). They have been devised in the several fields covered by this right, e.g., sexual identity,[75] or the right to a healthy environment.[76]

The question is then whether such obligations exist concerning privacy in relation to the processing of data. We can find some elements in the *Klass* case that concerned wiretapping, and the conditions under which such practice is deemed lawful.[77] In this case, the Court considered that wiretapping could be considered as an interference with Art. 8 of the convention,[78] and spelled out the conditions under which such interference is lawful in accordance to the three-folded Art. 8.2 ECHR test.[79] It appears that in order for the three conditions to be met, the Court ruled that several measures aiming at guaranteeing the *transparency and accountability* of the process had to be implemented.[80] A similar reasoning was held in the Kruslin and Malone cases.[81]

Some might argue that such measures have more to do with the conditions of legality of interferences than with the theory of positive obligations.[82] This reflection seems ancillary to us to the extent that the point here is to show that the respect for privacy can also entail in some cases measures to be taken by the state. Furthermore, that such a point would miss the fact that positive obligations are also a means to implement the horizontal effect of the Convention, which is precisely what is at stake here, entailing that this is a "classical" positive obligations situation.

data processing that spurred the need for a new type of protection; see for e.g., Serge Gutwirth, *Privacy and the Information Age*, Rowman & Littlefield, Lanham, 2002; the preface of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: « The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data". In other words, the processing of personal data by third persons is an intrinsic feature of computerised systems; a computer (and especially a networked computer) cannot function without such third party data processing. Such an observation is totally in line with Bruno Latour's accounts of technological mediation, and (partial) definition of technique and technology as delegation, cf. Bruno Latour, L'espoir de Pandore. Pour une version réaliste de l'activité scientifique, Paris: La Découverte, 2001, pp. 183-250, esp. pp. 185-201; see also Bruno Latour, Aramis ou l'amour des techniques, Paris: La Découverte, 1992.

[75] I. and Ch. Goodwin vs. United Kingdom, 11.07.2002; Van Kück vs. Germany, 12.09.2003.

[76] Hatton et al. vs. United Kingdom, (Grand Chamber), 8.07.2003.

[77] ECtHR, *Klass v. Germany*, 6 September 1978.

[78] ECtHR, *Klass v. Germany*, 6 September 1978, § 50.

[79] As a reminder, the interference must be lawful, pursue a legitimate aim, and be proportional and necessary in a democratic society.

[80] These conditions are made explicit in §§ 51-58. On these measures as a possible implementation of the principle of accountability within the right to privacy, see Raphael Gellert, Gutwirth, S., "Beyond accountability, the return to privacy?" *Managing Privacy Through Accountability*. Ed. Daniel Guagnin et al. Palgrave Macmillan, 2012.

[81] Kruslin vs. France, 24 April 1990, §§ 30-36, in particular §30; Malone *vs. United Kingdom*, 2 August 1984, though in this case the discussion was extended to metering and not wiretapping as such.

[82] J.-F., Akandji-Kombe, op. cit., pp. 12-14. The fact that positive obligations concerning privacy in relation to the processing of data are only triggered in cases of interference with privacy should actually come as no surprise. The situation at hand is that of third party data processing. From a privacy perspective such processing will **always** come as an interference with privacy (contrary to data protection). The question is not whether one's privacy is interfered or not with, but rather, whether such interference is legal or not (which might precisely necessitate such positive measures).

4.1.1.2 Privacy impact assessments as positive human rights obligations

In the previous paragraphs, we have shown that privacy classically triggers negative human rights obligation though positive obligations are not excluded, and that on the contrary, data protection, because it is embedded in third party data processing is embedded within the concept of positive human rights obligations.

In this section, we would like to make sense of this distinction between privacy and data protection in terms of human rights obligation by defining privacy impact assessments as a type of measure that falls within the scope of the positive obligations theory.

As a reminder, PIAs can be defined as a

> *a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. A PIA is more than a tool: it is a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after the project has been deployed.*[83]

In other words, a PIA is a tool that aims at ensuring the safeguard of a right (to privacy) by making sure that citizens' full enjoyment of their right is not threatened by innovations (in the field of information and communication technologies). This is precisely what positive obligations are about: taking measures to ensure the safeguard of a right.

The question is then: **why is a measure that can be qualified as a "positive privacy obligation" embedded within another right, the right to data protection?**

Several elements of response can be put forward.

A very positivist account for such discrepancy is the fact that precisely because it is (near) impossible to think of data protection in terms of negative human rights obligations (that is, in terms of abstention), the whole institutional structure underpinning the positive measures necessary to an adequate implementation of the right is already existing as it is, one might argue, coextensive to the very content of such right.[84]

However, other analyses can draw from the nature of the two rights.

One (quite political) argument to be made relates to the discussion concerning positive obligations and the right to privacy. As we have shown in the previous section, positive human rights obligations concerning privacy in the framework of data processing can only be triggered when privacy is being interfered with.

Positive obligations concerning data protection on the contrary have more to do with the very protection afforded by the right. One needs these measures in order for the guarantees offered by data protection to be effective.

So, it might make more sense to argue that PIAs are needed in order to ensure a good implementation of data protection rather than in order to ensure that interferences with privacy remain within the boundaries of what is legally permitted.[85]

[83] Wright, David, "The state of the art in privacy impact assessment", *Computer Law & Security Review*, Vol, 28, No. 1, Feb. 2012, pp. 54-61 [p. 55].

[84] For a comparison between data protection and anti-discrimination legislation in particular from the perspective of the institutional architecture see Raphaël Gellert, De Vries E., De Hert P., Gutwirth S., "A comparative analysis of anti-discrimination and data protection legislations", in Custers, B., T. Calders, B. Schermer, and T. Zarsky, *Discrimination and privacy in the information society. Data mining and profiling in large databases*, Springer, 2012, pp.61-89.

[85] It is compelling to observe that in its case-law dealing with data processing from the perspective of Art. 8 ECHR, the European Court was able to grant some data protection guarantees under the Art. 8.2 and not Art. 8.1, see PRESCIENT, D.1, p. 6.

Another point is to take into account the scope of the right to privacy. As evidenced in D.1 it is very broad and not limited to situations of data processing. In short, privacy extends from notions of intimacy and seclusion, to social and public aspects of privacy, to the right to make essential personal choices (e.g., sexual orientation), to finally being embedded in liberty, autonomy, and self-determination (i.e., privacy is the ultimate defence line of liberty).[86] Yet, a PIA *a priori* focuses on informational dimensions of privacy.

Since data protection on the contrary solely focuses on the processing of (personal) data, it could be more in line with the scope of PIAs.

4.2 The upcoming data protection framework: from PIA to DPIA

On 25 January 2012, the European Commission released two proposals: one for a general data protection,[87] another for a police and criminal justice data protection directive.[88]

Art. 33 of the proposed regulation explicitly provides for privacy impact assessments, except that they are renamed data protection impact assessments (DPIAs), thereby confirming our previous observation on the institutionalisation of PIAs.

Art. 33 is a long article, with no less than seven different provisions.[89] Its main provisions will be briefly outlined.

[86] Gutwirth et al., PRESCIENT Deliverable 1, 2011, p. 4, see the references in Fn. 4-7.

[87] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012, COM(2012) 11 final.

[88] European Commission, A proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25 January 2012, COM(2012) 10 final.

[89] "Article 33 Data protection impact assessment

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The following processing operations in particular present specific risks referred to in paragraph 1: (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale; (c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale; (d) personal data in large scale filing systems on children, genetic data or biometric data; (e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).

3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.

First, it is now mandatory for the data controller (Art. 33.1) to carry out DPIAs in specific circumstances spelled out in Art. 33.2, though the same article makes room for voluntary DPIAs. Art. 33.5 however, waives the DPIA obligation when, in conformity with a legal obligation, public authorities process data (unless the member state deems it nonetheless necessary to carry it out). Though it seems an *a priori* broad exception, the helps narrow it down by referring to Recital 73 of the proposed regulation.[90] Public authorities or bodies should carry out a DPIA if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the task of the public authority or body is based and which regulates the specific processing operation in question. In other words, this waiver applies only if a specific assessment, equal to DPIA, has already been made in the legislative context.

Art 33(3) sets the minimum DPIA requirements. It should contain "a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation".

Art 33(4) requires the involvement of stakeholders in the process of DPIA, without prejudice to the protection of commercial or public interests or the security of the processing operations. It remains to be seen whether the implementation of this provision will lead to meaningful participation and robust knowledge production or whether it will be used as a mere "PR exercise". In any event, the participatory nature of PIA can be linked to the new data subjects' right to transparency (Art 11ff), especially from an *ex ante* perspective: the possibility to be involved in the processing of their personal data, afforded by this article,[91] turns into a fully-fledged participatory right in this case.

The leaked draft of the proposed Regulation (November 2011) contained a provision on transparency that required the assessment be made easily accessible to the public (Art 30(5)). It has been abandoned, and the actual proposal contains no provision concerning the transparency of DPIAs, though it can be argued that the general transparency elements of the proposal also apply to DPIAs.[92]

Art. 33.6 and 33.7 concern delegated and implementing acts. They cover issues such as the scale and shape of a DPIA or the monitoring of the process.

As far as the proposed Police and Criminal Justice Data Protection Directive is concerned there is no mention of DPIA.[93] There is only a rather weak provision in Art 26 of the draft Directive that calls on the Member States to ensure that controllers in the police and justice sector consult the supervisory authority prior to the processing of certain types of personal data. Yet here this authority has no power to ban processing operations. The point can be made that there is no justification to exempt police and judicial authorities from the duty to carry out a DPIA in those situations where other controllers (private and public) would be obliged to conduct such assessments under the proposed Regulation.[94]

7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87.2."

[90] EDPS, Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012.

[91] Art 29 Working Party, 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, 1 December 2009, WP 168, at 63.

[92] Read Art. 28.1 and Art. 28.2.h in conjunction with Art. 22, in particular the combination of Art. 22.3 and Art. 22.2.c.

[93] The DPIA requirement has been taken out, whereas it was present in the leaked version of the draft Directive of November 2011. Cf. European Commission, A proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25 January 2012, COM(2012) 10 final, and Art 31 of http://www.statewatch.org/news/2011/dec/ep-dp-leas-draft-directive.pdf.

[94] Alexander Dix, PIAs – an essential building block in the new EU regulatory framework, keynote speech at the 2nd Privacy Impact Assessment Framework (PIAF) Workshop, Sopot, 24 April 2012.

4.3 Can we reach meaningful (privacy) protection with DPIAs?

In this last section we ask the following question: given that privacy impact assessments were first enshrined into data protection legislation, and successively renamed (at EU level) data protection impact assessment, what does it tell us about the possibilities for meaningful privacy protection that one could expect from DPIAs? In order to answer this question, we need to go back to the definition, content of these rights, and to the interplays existing between them.

In the first Deliverable, we have come to the conclusion that data protection can be defined as a set of "fair information practices" (FIPs) the aim of which is to ensure that data are processed in a fair, transparent, and accountable manner.[95]

We have also seen that data protection is both broader and narrower than privacy. It is narrower because it only deals with personal data, whereas the scope of privacy is wider as it can also concern the processing of non-personal data for instance.[96] It is broader, however, because the processing of personal data can have consequences not only in terms of privacy, but also in terms of other constitutional rights. For example, data processing can impact upon people's freedom of expression, freedom of religion and conscience, voting rights, etc. Most importantly, the know- ledge of individuals that can be inferred from their personal data may also bear risks of discrimination.[97] This broad relationship with the whole spectrum of fundamental freedoms is embedded within the Directive itself. According to its Art. 1, "*Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*".

Though the case law of the ECJ concerning the right to data protection – including its relation with other fundamental rights – is quite far from being crystal clear,[98] we would like to make the following hypotheses with a view to better understand the legal consequences of the introduction of a DPIA in the EU legal arsenal.

Given that the self-proclaimed aim of the right to data protection is to protect citizens' fundamental rights regarding the processing of their personal data, there are two ways one could conceive of this relation between data protection and the other fundamental freedoms.

The first way would be to consider that if a data processing does not violate the right to data protection because it complies with its different provisions and guarantees, then it ipso facto does not infringe upon the other constitutional rights. This test is quite a lenient one since data protection consists mostly of a set of FIPs.

[95] Gutwirth et al., PRESCIENT Deliverable 1, 2011, p. 5. See also, Gellert, Gutwirth, 2012, p. 7; Bennett, Colin, J., Raab, Charles, D., *The Governance of Privacy – Policy Instruments in a global perspective*, Cambridge, London: The MIT Press, 2006, pp. 12-13. In the same direction, see also, ECJ Advocate-General Siegbert Alber's Opinion on Case *C-369/98, The Queen vs. Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher, §* 41: "there would be no need for data protection if there were a general prohibition of information disclosure".

[96] Gutwirth et al., PRESCIENT Deliverable 1, 2011, p. 7.

[97] Ibid., p. 7.

[98] On the ancillary status of data protection, see ECJ, *Österreichischer Rundfunk*, §. 91. See also, C-275/06, Promusicae v. Telefonica de Espana, § 63; C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinaporssi Oy, Satamedia Oy, § 52; C-553/07, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer. On a more independantist approach, see ECtFInstance, *The Bavarian Lager Co. Ltd v Commission of the European Communities*, §§. 114-115; see also, the Lindqvist case where the Court held that protecting the privacy of the individuals was not the sole purpose of the data protection directive, ECJ, C-101/01, Lindqvist, § 97. On the fact that data protection's purpose is to establish a fair balance between **any** right affected and the free flow of information, Lindqvist, § 97, and that such balance should be internal to data protection, Rijkeboer §25.

The second way on the contrary would be to integrate the respect of other rights within the right to data protection itself, that is, to make the respect of these rights (of the data subject) an integral part of the respect of the right to data protection.[99] This test would be a much stronger test.[100]

These considerations apply to DPIAs.

In the first hypothesis the data protection impact to be assessed will be limited to the provision of the directive, and will thus mainly concern issues of transparency and accountability, leaving privacy and other fundamental rights issues only a very ancillary status. Such a solution would be very lenient, and the benefits it might bring in terms of fundamental rights protection disserves to be asked with renewed acuteness.

In the second hypothesis however, a DPIA would not be limited to assessing innovation's transparency and accountability, but would assess their compatibility with the whole spectrum of human rights. It would be the vehicle to safeguard fundamental freedoms with respect to innovations that apprehend humans through a digital form.[101]

[99] Probably, this internalisation of other human rights within the right to data protection could be undertaken through the proportionality test contained in Art. 6 of the current data protection directive. It can be argued that the ECJ followed this path in the Rundfunk case, § 91; see also Gonzalez Fuster, Gellert, 2012, op. cit., pp. 79-80.

[100] Although, as observed in the previous footnote, its realisation is probably extremely complicated –provided it is a correct understanding of the right to data protection. For instance, would a privacy violation assessed within the framework of data protection *ipso facto* mean the violation of the latter right?

[101] See for instance, van der Ploeg, Irma, The Machine-Readable Body. Essays on Biometrics and the Informatization of the Body, Maastricht: Shaker, 2005.

5. Current approaches to privacy and ethical impact assessment: philosophical and methodological challenges

Silvia Venier, Bruno Turnheim, Emilio Mordini (Centre for Science, Society and Citizenship)

The main aim of PRESCIENT has been to develop a framework by means of which privacy and ethical issues emerging from new technologies can be identified and addressed early on. The framework is presented in Chapter 6.

One of the key challenges of the project was how to integrate *ethical principles* in an instrument mainly derived from the models of technology assessment, in particular from current examples of Privacy Impact Assessment (PIA) frameworks. In this chapter we argue that there is a need to broaden the investigation on the main philosophical and methodological challenges of such an exercise. The purpose of this Chapter is exactly to investigate the theoretical discussion around the notions behind the development of a P+EIA.

In a workshop held in Rome on the 20th – 21st September 2012 on "New directions in Ethical Impact Assessment", some of the themes presented in this chapter have been discussed with a selected group of experts in ethics. The event was organised in the scope of PRESCIENT *Stage 4* on "A new framework for privacy and ethical impact assessment of emerging technologies". The workshop aimed at collecting experts' views on the feasibility and desirability of the development of an impact assessment framework for emerging ICTs that takes into account privacy, data protection, as well as ethical implications. The event was structured around three main roundtables:

- Roundtable 1 "*From Privacy to Ethical Impact Assessment*", discussing to what extent lessons learned from PIA methodologies can be applied to Ethical Impact Assessment, and considering different mechanisms for identifying, assessing and developing solutions for privacy and ethical problems that may emerge as new technologies are developed and deployed;
- Roundtable 2 "*Ethics of Ethical Impact Assessment*", devoted to analysing the ethical issues raised by the notion of Ethical Impact Assessment";
- Roundtable 3 "*A new framework for ethical impact assessment*", discussing criteria for the development of a new framework for privacy and ethical impact assessment of emerging technologies.

The key outcomes of the workshop are presented in the "Rome workshop focus" boxes throughout the text of this chapter. Chapter 5 is structured around six sections.

Section 5.1 discusses current efforts made at the European Union (EU) level towards the reconciliation of technological innovation and ethical values. In relation to the often perceived tension between innovation and values/rights, we argue that whether "constraints" of any kind – included those generated by ethics – are either a barrier to innovation or a support depends on a number of factors, the most important being governance. Good innovation governance interprets constraints as frameworks, which do not drive, or even prevent, innovation but only provide a structured context within which innovators are free to experiment new and original solutions.

Section 5.2 discusses difficulties in clearly understanding the role of ethics in the description and evaluation of emerging technologies. This is due to different sets of reasons, the most important being that technological innovation is happening under uncertain and very complex conditions. This section also provides a short historical overview of the development of the field of technology ethics, and tries to point out that this is a recent field of research, and that better informed and more proactive ethics is need in roder to having the theoretical and methodological tools needed to evaluate emerging technologies from a normative perspective.

The following sections give an overview and present a critical reflection of contemporary quantitative approaches to technological risk assessment (5.3), as well as privacy impact assessment, PIA (5.4) and ethical assessment methodologies (5.5). Section 5.6 is concerned with summarising some philosophical and methodological challenges in conducting such exercises.

In this chapter, particular attention is paid to research on these themes mainly conducted in the scope of recent European initiatives. Considering the focus of PRESCIENT, current technology assessment approaches and methodologies that are somehow modelled around technology assessment and PIA frameworks have been particularly taken into account. As we will argue, these are part of the complex landscape of the ethical *governance tools* of emerging technologies. The need to include an ethical impact assessment framework into a broader, more nuanced and flexible understanding of the role of ethics in relation to emerging technologies is discussed throughout the chapter.

5.1 Towards reconciling technological innovation and ethical values: the EU approach

A certain tension is intuitively often perceived between technological innovation[102] and the respect of human rights and ethical values. This perceived tension mainly refers to the idea that respecting the values of our democratic societies as well as fundamental human rights would inherently be in contradiction with improving technology *performance*.

But is this the case? Can technological innovation be *compatible* with ethical considerations or even *enhanced* if it happens within a framework dictated by such considerations?

At the European Union (EU) level, *enhancing innovation* and *respecting fundamental rights* have both been placed as cornerstones of the Lisbon strategy[103] (2000-2010), the main aim of which was "to make the EU the most competitive and dynamic knowledge based economy in the world capable of sustaining more and better jobs and with greater social cohesion", as well as central elements of the current Europe 2020[104] strategy (2010-2020), aiming at supporting a *smart*, *sustainable* and *inclusive* growth.

In the European Commission 2003 Communication on "Innovation Policy: updating the Union's approach in the context of the Lisbon Strategy"[105] technological innovation is described as one of the three types of innovation, the others being organisational and presentational[106]. In this Communication, an updated definition of innovation is also provided. Innovation consists in "the successful production, assimilation and exploitation of novelty in the economic and social spheres"[107].

From this definition, it can be assumed that one of the criteria for implementing *successful* technological innovation (i.e., innovation which is assimilated and exploited by European "social sphere" as well) would be to take into particular consideration ethical and societal issues that technological innovation is raising. According to this view, the awareness of ethical considerations, if it becomes an integral part of the technology being developed and used, could bring a competitive advantage for those able to address these aspects properly.

[102] i.e. innovation derived from research and development, R&D

[103] Launched at the European Council Meeting in Lisbon in 2000, the Lisbon Strategy described the EU main priority objectives for the period 2000-2010.

[104] See the European Commission, Communication on "Europe 2020: a European strategy for smart, sustainable and inclusive growth [COM(2010)2020]", Brussels, 3 March 2010.

[105] European Commission, Communication on Innovation Policy: updating the Union's approach in the context of the Lisbon Strategy, COM(2003) 112.

[106] In the updated approach, the Commission emphasizes that "innovation policies must extend their focus beyond the link with R&D", that had been identified in COM (2002) 49 as an essential factor for long term growth and prosperity in Europe.

[107] COM(2003) 112, page 5

Generally speaking, constraints of any kind – included those generated by ethics – could either be a barrier to innovation or a driver[108]. Collective and individual creativity is stimulated by challenges, and challenges are rarely only negative. Yet whether legal, ethical, cultural, social, environmental, political, constraints may become a driver for innovation rather than an obstacle depends on a number of factors, the most important being *governance*. Good innovation governance interprets constraints as *frameworks*, which do not drive, or even prevent, innovation but only provide a structured context within which innovators are free to experiment new and original solutions. Taking into account these considerations, our position is that the respect of ethical principles could provide a competitive advantage to European industry to the extent that researchers and technology developers are provided with an open, dynamic, participatory, ethical framework, rather than with strict, top-down regulations and bureaucratic procedures.

The alignment of technological innovation to broader ethical and societal aspects is in accordance with the European Union's ethos of being a *community of values*[109]. The Charter of Fundamental Rights of the EU has become the key document in this regard, and has also been considered the foundation of an "EU Institutions Ethics"[110].

The EU Charter shapes the way research is funded at the EU level. Since the Fifth FP, the EU incorporated as a precondition in its funding process the adherence to and observation of "fundamental ethical principles"[111]. The potential conflict with the values and principles of the EU Charter is therefore an indicator of the emergence of an "ethical issue" in technological innovation.

Fundamental human rights are thus a central element of the *constitutional* architecture of the European Union. Ethical, human, societal concerns are increasingly seen as integral to the European innovation model. As an example, this is particularly evident in the current debate on how to integrate ethical values in the development of *security* technologies, an interesting field for any ethical and privacy impact assessment. If, in the past, the main focus on security was limited to military threats against the State and the related issues of territorial integrity and national interests, new concepts have recently emerged such as *societal* security and the notion of *human* security which has been used in official documents at the European and international level[112]. Security today incorporates a range of factors, from material assets to intangibles such as fear, mistrust, lack of confidence, feelings of despair or, alternatively, hope, trust, confidence, resilience.

[108] See, for instance, the Porter hypothesis on environmental regulation. Ambec, Stefan, Mark A. Cohen, Stewart Elgie, and, Paul Lanoie, *The Porter Hypothesis at 20: can environmental regulation enhance innovation and competitiveness,* Resources of the Future Discussion Paper (RFF DP 11-01), January 2011.

[109] See, for instance, European Union Delegation to the United States, *The EU: a community of values*, EU Focus Newsletter, November 2005.

[110] Note that an "Ethics of European Institutions" is different from a "European Ethics". The latter would mean that European citizens share common moral principles and values. See Nagenborg, Michael, Rafael Capurro, *Ethical Evaluation*, ETICA Deliverable 3.2.2, [page 4].

[111] See European Parliament and of the Council Decision No 182/1999/EC concerning the fifth framework programme of the European Community for research, technological development and demonstration activities (1998 to 2002), 22 December 1998, Art 7.

[112] In 2006, the CEN BT/WG 161 on Protection and Security of the Citizen adopted the following definition: "Security is the condition (perceived or confirmed) of an individual, a community, an organization, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, disasters (natural and man-made)". See CEN Expert Group, Report on Supply Chain Security, Brussels 14th November 2006, [page 4]. The societal dimension of security is essential also to the ESRIF definition, which reads that "security is inextricably bound to a society's daily political, economic and cultural values, [...] Security from a social perspective has three major characteristics: 1) It is about people — both as the source and the object of insecurity; 2) It is about society — in the knowledge that some threats will target people's identity, culture, and way of life; 3) It is about values – and which proactive and reactive measures can protect Europeans while reflecting their values and way of life". European Security research and Innovation Forum (ESRIF) Final Report, December 2009, [page 13].

The perceived tension between the term “security” and “ethics” was also discussed during the Rome workshop, as presented in the box n1 below.

Box 1 - Rome workshop focus

Security Ethics: an Oxymoron?

Michael Nagenborg, from the International centre for Ethics in the Science and Humanities at Eberhard Karls University Tuebingen, gave a presentation on “*Security Ethics: an Oxymoron?*”. The presentation explored how and when security started to become an ethical issue, and what are the implications for the ethical impact assessment of security technologies. Michael’s starting point was a consideration on the origins of the two words, ethics and security. On one side, “ethics” dates back to the ancient Greece, when philosophers started to develop the understanding that human life cannot be sufficiently guided by habits, conventions and traditions alone. The word “securitas” was coined by Cicero, and referred to a central aspect of living a good life, the “vita beata”, with the meaning of living a life without (*se*) any fear (*cura*). This approach had its root in the Stoic tradition, based on the avoidance of suffering from anxiety and on living in peace without conflicts by becoming fully aware of what lies beyond the influence of human actions.

At the beginning, there was therefore no apparent contradiction between security and ethics. Since Augustine, however, security has been perceived as something that has to be provided and maintained. An active understanding of security (e.g., the idea that security is about “preventing adverse consequences”) has been developed since those days. In today’s world, “security” is a concept that needs to be designed and realised, it is mainly conceived as the result of human actions. In our claims about contemporary security, Michael argued, the concept of a life “without fear” is missing: as a consequence, the perceived sense of insecurity is relatively high in the safest parts of the world. This “permanent notion of insecurity” directly limits the freedom individuals and societies need in order to prosper. It is paradigmatic that the institutionalisation of a fear is exactly the main goal of any terroristic activity. Michael discussed whether we have the problem of “too much” security in our contemporary ages, and proposed that we probably shall think of removing something from our “securitization agenda”. Ethical concerns are not so much about security per se, but about the levels of security and the measures taken to achieve them, and about who should take responsibility for addressing these issues by these means. An assessment of security measures and technologies based on ethical values has to address the discourse of security itself, paying attention not only to intended and unintended consequences and to the impacts on social life, but also aiming at understanding and evaluating how security shapes the world we live in.

Generally speaking, and as stated by the European Group on Ethics in Science and Technology (EGE)[113], the European Commission (EC) wants to promote the *responsible* use of science and technology both within the European Union and worldwide. A comprehensive governance approach to deal with the ethical and societal impact of innovation has recently been proposed at the EU level. In May 2011 the EC Direction General for Research and Innovation hosted a Workshop on *Responsible Research and Innovation* (RRI)[114]. RRI has been 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)*[115].

As the above definition suggest, the “ethical acceptability” of innovation is one out of three “normative anchor points” which should be taken into considerations in a deliberative democracy. According to the author, “ethically acceptable” “refers to a mandatory compliance with the fundamental values of the EU

[113] European Group of Ethics (EGE) in Science and New Technologies to the European Commission, General Report on the Activities of the EGE, 2005-2010.

[114] http://ec.europa.eu/research/science-society/document_library/pdf_06/responsible-research-and-innovation-workshop-newsletter_en.pdf

[115] Von Schomberg, René, Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technology Fields, A report from the European Commission Services, European Union, 2011.

charter of fundamental human rights […] and the safety protection level set by the EU"[116]. Rather than seeing ethical values as impediments or restraints to the conduct of science[117], RRI is thus "driven and guided by values, especially those recognised by the Charter of Fundamental Rights of the European Union and the EU Lisbon Treaty"[118].

RRI develops around both the *product* (a) and the *process* (b) dimensions of innovation. The main deployment methodologies for the product dimension are (1a) the use of technology assessment, privacy impact assessment, and technology foresight, (2a) the application of the precautionary principle, and (3a) the use of demonstration projects in order to move from risk to "innovation governance". At the process level, RRI is implemented through (1b) the deployment of codes of conduct for Research and Innovation, (2b) the use of standards, certification and accreditation schemes and labels for research practice, (3b) the incorporation of ethics as a design factor of technology, (4b) research on and implementation of normative models for governance, and (5b) on-going public debate over these challenges. The so-called "RRI matrix"[119] provides examples of key questions to be answered by stakeholders (both from a product and a process perspective) in order to fully implement the RRI scheme. A big challenge for the proposed principled approach is how to take into account also the emerging issues, since often there is a gap between the proposed aims and the actual (sometimes hidden) agenda (i.e., who is really empowered by the deployment of a technology)[120]. The box n 2 reports a presentation during the Rome workshop on RRI, dealing with concrete projects, implementing the above mentioned "RRI deployment methodologies".

Box n2 - Rome workshop focus

Responsible Research and Innovation (RRI)

During the workshop held in Rome on the 20th 21st September 2012, Aki Zaharia Menevidis, Fraunhofer Institute for Production Systems and Design Technologies, gave a talk on "*Privacy protection and ethical governance*" and presented the work that was carried out in some EU funded projects whose aims have been to apply the RRI concept, such as Radical (Road mapping technology for enhancing security to protect medical and genetic data), Adis (Automatically Detection of Situations that need intervention), Fearless (Fear Elimination as Resolution for Loosing Elderly's Substantial Sorrows), Ethical (International debate on ethical implications of data collection, use and retention for biometric and medical applications) and Responsibility (Global model and observatory for International Responsible Research and Innovation Coordination). The perspectives presented were both the one of the final product (the "solution") and of the overall process (concept, design, development). In the scope of these projects, five basic principles were initially identified in ICT research and development. These are informational privacy, confidentiality, property and ownership, reliability and trustworthiness, purpose and rationality. As a second step a code of conduct was developed (RESPECT code of conduct, "An EU code of ethics for socio economic research" available at http://www.respectproject.org/ethics/412ethics.pdf). The future work will focus on the development of online tools for responsible research and innovation, that will integrate the code of conduct. In his conclusive remarks, Aki pointed out that the scientific assessment of risks encompasses two complementary assessments: the assessment of physical harms (this is mainly dealt with through the precautionary approach) and the assessment of societal harms (here Ethical Impact Assessment frameworks have a crucial role).

[116] Von Schomber, René, "Introduction: Towards Responsible Research and Innovation", in Von Schomberg, René, op. cit, [page 9].

[117] It should be mentioned here that saying that ethical values are *either* an impediment to *or* a driver for innovation might sound as an "artificial" opposition. Ethical values can be better conceived as being both, at the same time. This is also in line with the "structuration theory", which in a nutshell sees institutions (in the sense of collective rule-sets) as both 'enabling and constraining' action. See Anthony Giddens, *The Constitution of Society: Outline of the Theory of Structuration*, Polity Press, Cambridge, UK, 1984.

[118] Basic principles and values at the EU level are dignity, freedoms, equality, justice, citizens' rights, solidarity and sustainability.

[119] The matrix is available at the following link http://renevonschomberg.wordpress.com/implementing-responsible-research-and-innovation

[120] We see here a difference between approaches such as RRI, a heuristic device which seeks to identify problems by providing a *guide* for questioning, and more prescriptive methodologies (telling how to act), or criteria-based accounting procedure (ticking boxes).

Point 1a in the RRI list of deployment methods above refers to one of the main objectives of PRESCIENT has been to integrate ethical principles in a framework mainly derived from the model of Technology Assessment and Privacy Impact Assessment methodologies. This chapter discusses the need to include this tool into a broader investigation on the challenges which are related to dealing with ethics of emerging technologies and are inherent in this approach.

5.2 Towards the inclusion of ethics in technology governance

On general terms, the open debate on where is the "adequate place" of science and innovation in society has recently been addressed by the 2009 MASIS[121] Report on "Challenging Futures of Science in Society"[122]. According to this report, science has to keep on-going the reflection on its role and impacts on society. Through the contribution of new research fields such as technology assessment, impact studies, risk studies, Science and Technology Studies (STS), the MASIS report acknowledges that science is becoming more *reflexive* on its role and impacts on society. The "reflective science" concept mirrors the one of "reflexive modernity", which refers to the fact that late modernity opposes (or *reflects* back on) its earlier version. Social groups are reflecting back on their relationship with the public institutions, which, they believe, are no longer needed in order to fulfil the maximization of the individual self-development and freedom, that had been of the main promises of the transformation brought by early modernity. Reflexivity is "a breach with the instrumental rationality of modernity itself, as it is constantly haunted to clarify the foundations upon which it relies and the conditions under which it performs"[123].

The MASIS report identifies five dimensions along which the role and use of science *in* society can be appreciated. These are:

a. Innovation: contributing to economic growth;
b. Quality of life: contributing to health, education, welfare, social order;
c. Political: contributing to relevant debates;
d. Cultural: conserving cultural heritage and developing inter-cultural dialogues;
e. Intellectual: thinking about the "good society" and the future of human nature.

Ethical reflection has an increasingly crucial role with respect to the challenges raised by technological innovation and by the very concept of reflective science. Ethics can function as a moderator and mediator in the necessary dialogue between science and society. In the multi-cultural realm we find ourselves in, ethics can be perceived also as a legitimization process of the pluralism of conceptions of "good lives".

If the role of ethics should particularly be to focus on the last dimensions (e), ethics can provide its contribution to the debates surrounding each of the other four dimensions as well. In other words, ethics could become an element of processes of socio-technically distributed innovation, in which products and services are developed or at least refined at societal level.

A way to seek to clarify the role of ethics in the governance of emerging ICT can be found in ETICA D4.1[124]. The paper sets the difference between governance tools and governance approaches. According to the authors, governance tools "can be used within a governance approach to explore ethical issues raised, and as part of an exercise to open the cognitive framing in order for the exploration to be successful", while governance approaches are "ranges of possible strategies for constructing a norm". It is usually said the

[121] The MASIS (Monitoring Activities of Science in Society in Europe) expert group was responsible to analyse the emerging trends and cross-cutting issues in science in society in Europe. The 2009 report was addressed to policy makers and researchers in this field, and designed to contribute to the realization of the European Research Area (ERA).

[122] MASIS Report, *Challenging Futures of Science in Society. Emerging Trends and cutting-edge issues*, 2009.

[123] Van Loon Joost, "Virtual Risks in the Age of Cybernetic Reproduction", in Adam, Barbara, Ulrich Beck, Joost Van Loon, *The Risk Society and Beyond. Critical Issues for Social Theory*, SAGE publications Ltd, 2000, [page 176].

[124] Goujon, Philippe, Catherine Flick, *ETICA D4.1: Governance approaches. A critical appraisal of theory and practice.*

latest to fit one of the two governance paradigms, i.e. the *efficiency* paradigm which is based on the norm's efficiency (i.e. to produce an actual change in the actual world), and the *participatory* paradigm, that is meant to be legitimate because of its participatory nature but might fail the effectiveness requirement. According to this distinction, we can consider an ethical impact assessment derived from a PIA framework as a governance *tool*. This can result in the need to include an ethical impact assessment framework into a broader, more nuanced and flexible ethical governance approach, aiming at governing the development and use of new technologies from a wider perspective.

But what does exactly imply to include "ethics" in technology governance? In PRESCIENT D1, we defined *ethics* as a philosophical enquiry in concepts involved in practical reasoning, i.e., concepts related to the ways in which human beings *choose* among possible different courses of actions, according to criteria such as good/bad or right/wrong. Provided that there are events which are *actions* (i.e., events that are controlled, at least in part, by an agent, who contributes to cause them according to some *intentions*), ethics investigates (1) the notions involved in actions, say, ethical principles such as good and evil, right and duty, virtues, obligations, free will, etc., their foundation and their rationale; (2) claims made in these terms, their soundness and consistency; and (3) practical problems which involve the ethical principles and the assessment of the rationale behind each option of action.

As a discipline, ethics can be divided into three main branches: *meta-ethics*, investigating where our moral principles come from (point 1 above), *normative ethics*, trying to come up with moral standards for right and wrong behaviour (point 2 above), *applied ethics*, focusing on specific moral issues within a given context and practical case (point 3 above).

Ethical issues arising from scientific and technological innovation are usually solved through *traditional normative ethical theories*, in terms of either an utilitarian framework of weighting consequences with the aim of maximising happiness (mainly deriving from consequentialism), a deontological framework of rights and responsibilities, which is usually based on foundational principles of obligation (Kantian ethics theories), or a framework emphasising a good character development or good community membership (derived from virtue ethics theories).

In the ICT revolution, however, ethics is not only confronted with the *justification of intentional actions of individuals*, as it can be conceived in these more *classical* approaches. In this section we argue that the development of new ICTs and other security technologies are generally *complicating* the definition of the role of ethics, as well as the identification of its theoretical approaches and operational instruments needed to address ICTs-related issues. This is due to different reasons.

First, scientific and technological advances have the potential to bring *unintentional*, or highly *unpredictable* consequences that are usually the result of *collective* decisions.

Unlike traditional ethical cases, the variables for ethical evaluation of emerging technologies are therefore often vague and unclear. In addition, the decentralization of technology development distributing responsibilities among many individuals may result in an anonymous process for which nobody can be held responsible. Individuals may find themselves, in accordance with which role they identify themselves with, (partly) responsible for particular consequences, but not for the whole process. This raises the issue of how to define critical terms such as "responsibility" or "accountability", in a society that is based on specification and multiplication of roles. In relation to this, von Schomberg writes: "For already a long time, it is not sufficient to construct an ethics of science and technology on the basis of an image of a scientist who intentionally wants to construct a Frankenstein. So as a minimum we would require an ethical framework that addresses both the aspect of unintentional side consequences (rather than intentional actions) and the aspect of collective decisions (rather than individual decisions) with regard to complex societal systems, such as the operation of our economy. We don't have such a theory at our disposal."[125]

Second, technology is opening new possibilities not only of *actions* whose consequences are hardly foreseeable, but of definition of the *very nature* of the individual and of inter-personal relations. Along with other contemporary trends such as globalisation, technological innovation is having a deep impact on the *reference value system* shared by individuals. Contemporary technologies are influencing the understanding of different values, freedoms and rights. In the middle of this revolution[126], we are confronted with crucial questions related to the very nature of being human and of the traits of a good quality of life.

If ethics can be of help to ensure that all alternatives are comprehensively and critically assessed before making a decision, in situations of deep conflict such as those related to the development and use of ICTs, it may also help creating the necessary public discourse to critically reflect on decisions and priorities which are affecting human nature and society as a whole. This is of particular relevance while dealing with the relationship between contemporary values/rights and emerging technologies.

Box n 3 - Rome workshop focus

Ethics of emerging ICTs: between critique and judgement

In his introductory speech, Emilio Mordini, director of the Centre of Science, Society and Citizenship, pointed out that a clarification is needed with respect to the terms "*ethics*" and "*morality*", even if there is no clear agreement on this distinction between scholars. Ethics is a branch of knowledge that deals with moral principles. (Meta-) Ethics aims at reflecting on the legitimacy of these moral principles, at analyzing their origins (i.e., to answer the question "where do these principles come from?") and the rational criteria for selecting – in case this is possible – and agreeing on them in secular, pluralistic, multicultural societies (i.e., to answer the question whether it is possible a shared ethics under these conditions, or whether any ethics is unavoidably culturally bound?). On the other hand, the term "morality" refers to the actual principles as well as to the identification of norms that should govern a person's behavior. The challenge of morality is to answer the question about how to fill the gap between actual behaviors and norms (in case a gap exists). According to this classification, morality (or "applied ethics") makes sense only to the extent that there is a sort of consensus about preliminary, foundational ethical issues. In other words, and considering the identification of ethical issues of emerging ICTs, one could say that we can consider a determined behavior good or bad only after having agreed that (1) it makes sense to search for rationality in human behavior (establishing criteria about what is good and bad) and that (2) it is possible to agree on such criteria.

In her speech "*Ethical and Privacy Impact Assessment in the Big Data Era: an Oxymoron?*" also Antoinette Rouvroy, research associate at the Interdisciplinary Research Centre on Information, Law and Society of the Namur University, pointed out that the distinction between ethics and morality mirrors the distinction she made between *critique* (i.e. questioning on the criteria to assess what is moral/legal) and *judgement* (i.e. strategies to apply principles to concrete situations). *Critique* is defined as "the virtue consisting in challenging the very categories through which one is predisposed to perceive and evaluate people and situations of the world, rather than merely judging them according to these very categories", while *judgement* subsumes events of the world under pre-established categories, norms, principles. *Critique* is further explained as "a practice that suspends judgement" and as an "opportunity to practice new values, precisely on the basis of that suspension". It was finally proposed to conceive EIAs (Ethical Impact Assessment) and PIAs (Privacy Impact Assessment) as an instrument between *critique* and *judgement*. This is due to different reasons. First of all, a more developed diagnosis of the present is needed, as well as the definition of which ethical values are to be protected in the "big data era". Second, this would require a clear understanding of the target (what does EIA exactly assess?). Thirdly, an assessment of how presupposed agents and objects are produced is also needed (e.g. how are desirability and preferences produced? Are they favourable to human flourishing and compatible with deliberative democracy?), as well as the assessment of what emerging technologies allow to disregard or neglect, of what becomes invisible, unspeakable (e.g. to give voice to non-majoritarian views). In Antoinette's understanding, a critique-based EIA should focus on evaluating projects and priorities, as well as on assessing risks.

[125] von Schomberg, René, From the Ethics of Technology towards an Ethics of Knowledge Policy and Knowledge Assessment. A working document for the European Commission services, European Commission's Directorate General for Research 2007.

[126] On technological revolutions, see Freeman, Chris, and Francisco Louça, *As the time goes by: From the Industrial Revolutions to the Information Revolution*, Oxford University Press, 2001.

The implications of this being in the middle of the ICT revolution for the development of an "ethical impact assessment (EIA) framework"[127] have been deeply discussed during the Rome workshop. The box n3 above summarizes some of the most critical points touched, in particular whether EIAs should be conceived as an instrument between *critique* (i.e., questioning the criteria currently used to assess what is moral/legal) and *judgement* (i.e. strategies to apply principles to concrete situations).

But does an *ethics of technology* actually exist as a mature field of research? Tracing the path back from its origins, a "technology-oriented ethics" has developed largely independently from contemporary approaches of mainstream contemporary Philosophy of Technology (PoT)[128] since the late 1970s, in the form of both a *professional ethics* aimed at engineers, assisting them at shaping their professional responsibility, as well as an *applied ethics* focusing on socio-ethical problems surrounding new *specific* technologies.

With particular regard to one of the applied ethics' fields mentioned above and most developed to date, *computer ethics*, Helen Nissenbaum identifies three central lines of inquiry that have been followed to date[129]. These are:

(1) ethical questions and challenges to *social, moral, political values*: with regard to this point, Nissenbaum suggests that in approaching the changes in ethical values philosophers have been concerned with the status of particular values in society and on how these are affected by technology-induced cases, as well as with wrong and good actions of people in light of these particular changes. Issues that have been discussed in this field include intellectual property rights, responsibility for harmful consequences in the use of computer technologies, responsibility for the nature and severity of computer crime, social justice (i.e., impact on power relations) and quality of life in general, free speech, free movement, digital divide, and, of course, privacy, one of the most critical and enduring issues in this category;

(2) the *nature of computer ethics itself*: with regard to this, Nissenbaum suggests that many philosophers have started raising questions "about the nature of the inquiry itself" (*meta-ethics*), and the responses vary from those who assume that computer ethics problems can be reduced to applied ethics and are accessible by standard ethical theories, to those who think that the changes are so deep that new ethical theories are required;

(3) *ethical obligations* of professional experts in ICTs, as a consequence of their specialised knowledge and training.

An interesting point made by Nissenbaum is about the *porosity* of the intellectual borders of this philosophical community, who is usually enriched by developments in the literature and methods of neighbouring fields, such as philosophy of law, political philosophy, philosophy of technology, information law, science and technology studies (STS). Nissenbaum suggests that the approach of ethics is the one that seeks both to *describe* the systems/technology and also to *evaluate* them in terms of moral, social, political values (as discussed in point 1 above). The dependency of computer ethics to other fields however eventually enlarges the difficulties faced. As an example, it is evident that the scope and agenda for an ethics of ICTs may also depend on how technology is conceptualised (i.e. on the analysis provided by philosophy of technology) as well as on the theories related to the relations between technology and society

[127] For more concrete examples of current EIAs, refer to section 5.5 below.

[128] The Philosophy of Technology contemporary approaches mentioned here are the society-oriented (*Science and Technology Studies, STS*) and engineering-oriented philosophy of technology, which emerged as a result of the so called "empirical turn" in the 80s, which refused technological determinism and focused more on specific technologies and specific phases of technology development. See Brey, Philip, "Philosophy of Technology after the empirical turn", *Techné: Research in Philosophy and Technology*, 14:1, 2010. In this article, Brey also discusses the limitations of contemporary approaches to an applied technology ethics, and proposes an interesting research agenda. This will be discussed more in depth in the following sections.

[129] Nissenbaum, Helen, "Information Technology and Ethics", *Berkshire Encyclopaedia of Human Computer Interaction*, Great Barrington, MA, Berkshire Publishing Group, 2004, pp. 235-239.

(i.e. on information that is mainly derived from STS). A multidisciplinary approach, involving both technical engineering knowledge as well as theories from other social sciences and disciplines, is therefore paramount.

Going back to the claim that the role of ethics is being complicated by emerging technologies, in “Technology and Responsibility: Reflections on the New Tasks of Ethics”,[130] Hans Jonas was one of the first to argue that, since modern technology is changing the very nature of human actions, bringing along new powers and a new dimension of responsibility that were previously inconceivable, the role of ethics needs to be *adjusted* according to these developments.

Jonas also discussed the problematic preconditions of an effective philosophically grounded technology ethics, which are mainly based on the fact that a new form of determinism, more complex and multifarious, has emerged, namely the one exercised by the human artefact itself upon its creator and user. In response to the need to tackle these challenges, Jonas proposed a revision of Kant’s categorical imperative, based on an obligation to respect the continuation of humanity into the indefinite future.

In a more recent article, James Moor, one of the pioneering theoreticians in the field of computer ethics, raises a similar concern, by arguing that *better* ethics for emerging technologies is needed[131]. Current ethics, he holds, is insufficiently equipped to address the revolutionary changes that are being brought about with new and emerging technologies. The revolutionary character of these contemporary ages refers to the fact that this is a period in which technology promises dramatic changes, both in terms of having a significant level of social impact and consequently having a serious ethical impact. Taking into consideration this, Moor argues that ethical approaches that are *better informed* about new technologies and better ethical action in terms of being *more proactive* in identifying and addressing ethical issues in relation to them are required.

In relation to the description and evaluation of ICT, ethics needs therefore to be better informed and more proactive. The question, however, arises on whether it is feasible to develop such an *adjusted* ethical analysis and a normative theory of action while being in the middle of the ICT revolution[132].

Can it be *too early* to discuss the implications of technologies that are *emerging*? How should we deal, from an ethical perspective, with the concepts of risk and uncertainty? Is it possible and what are the best ways to be *proactive* and *anticipate* emerging problems when some aspects of the future are not known?

In order to address these complex questions, it is first important to distinguish uncertainty from risk. While risk refers to situations in which a future situation can be expressed in terms of *probabilities* (and can be therefore scientifically measured), uncertainty has to do with situations in which probabilities cannot be attributed, or are completely indeterminate (the so called “unknown unknowns”).

In one of his works that particularly aims at advancing the state of the art of ethical assessment of new technologies, Sollie argues that the question of what uncertainty entails is still unexplored in technology ethics, although being crucial. According to Sollie, “new technologies are surrounded by uncertainty due to opacity, complexity, multi-agency, long development trajectories, orientation at the future, global character, impact, and the fact that the technology often shifts in application”[133]. Uncertainty results in a lack of information to guide our moral decision making, and hence there is the necessity for ethics to reflect

[130] Jonas, Hans, “Technology and Responsibility: Reflections on the New Tasks of Ethics”, *Social Research*, Vol. 40, N. 1, 1973.

[131] Moor, James H., “Why we need better ethics for emerging technologies”, *Ethics and Information Technology*, Vol. 7, No. 3, 2005, pp. 111-119.

[132] See also David Collingridge’s “control dilemma”, which can be exemplified as follows: “attempting to control a technology is difficult, and not rarely impossible, because its early stages, when it can be controlled, not enough can be known about its harmful social consequences to warrant controlling its development; but by the time these consequences are apparent, control has become costly and slow”. Collingridge, David, *The Social Control of Technology*, Frances Pinter, 1980.

[133] Sollie, Paul, Marcus Duwell, Evaluating New technologies. Methodological problems for the Ethical Assessment of Technology Development, Springer, 2009, [page 147].

upon this concept. "If ethics aims at evaluating technology (not only retrospectively, but also proactively), then it has to account for the inherent uncertainty of technology development"[134].

In the case of emerging technologies, uncertainty may relate to the whole of the situation to be evaluated, namely the object of evaluation (i.e., the *technology*), the subject of evaluation (i.e., the *actors* involved) and the framework of evaluation (i.e., the *ethical theory* to be used). Considering that complex technology developments lack substantial information that is needed for the ethical evaluation, Sollie wonders whether there is any potential to work towards an ethics of technology that allows a proactive ex-ante moral evaluation of technology development. Sollie claims that an adequate ethics of technology needs to account for both *substantive* and *procedural* theories in order to guide proactive moral reasoning under conditions of uncertainty.

On the other hand, we may also think that it is already *too late* to face these challenges. This refers to the difficulties in dealing with the "technological race" or the new "technological determinism"[135], i.e. the fact that there is a continuous drive from science, market, politics, to develop new and improve existing technologies, and that society is increasingly dependent on the contemporary information infrastructures. The difficulties in bridging the gap between technological innovation and current ethical and legal frameworks can also be seen as a consequence of this. The "issue of time" has been also touched upon during the Rome workshop, as the box n4 below shows.

Box n4 - Rome workshop focus

The Issue of Time

In her speech Antoinette Rouvroy talked about the "issue of time" in relation to the governance of emerging technologies. The issue of time includes questioning whether we are already too late in a process that is nowadays ineluctable. The issue of time also includes wondering on how the impression to be always "in a flow" can be addressed.

In current times we have often the impression that the real time of technology development and data processing is completely beyond our control, in the sense that we don't have the time to stop this process, and to reflect about the biggest picture, i.e. what are our society's major goals and long-term projects. According to this view, technology would be above all an instrument to achieve society's long-term goals. In her conclusive remarks, Antoinette argued for the urgent need to re-establish the hierarchy of ends and means, and to guarantee that emerging technologies remain responsive to human needs – rather than the opposite.

Trying to stick to real problems we face while developing and using new technologies, we have already said that ethics is increasingly conceived as a partner to set priorities of technology related policies. It is important to note here that one of the main goals/application of PRESCIENT is to give policy makers, technology developers and relevant stakeholders a clearer idea of these risks, as well as decision makers clearer orientation on how to develop technology policy.

In relation to this, technology ethics has also been seen a research field comparative to technology assessment (TA). According to Armin Grunwald[136], while the *ethics of technology* emphasises the normative implications and the importance of moral conflicts in decisions on technology, *technology assessment* (TA) relies on more descriptive sociological or economic research, as well as on the need for operationalization and concreteness. TA studies the effects of new technologies on industry, the environment and society, evaluating such effects and developing instruments to steer technology development in more desired directions. The TA approach does not aim to give recommendations as to what *should* be done in technology policy (since, it is claimed, decisions are made within the rationality of

[134] Sollie, Paul, Marcus Duwell, op cit., 2009 [page 149]

[135] Jonas, Hans, *The Imperative of Responsibility*, The University of Chicago Press, 1984.

[136] Grunwald, Armin, "Technology Assessment or Ethics of Technology? Reflections on Technology Development between Social Sciences and Philosophy", *Ethical Perspectives*, Vo.6 No.2, July 1999, pages 171-182.

the political system), but only information on what *could* be done. Current technology assessment tools include technological forecasting, impact assessment methodologies, scenario analysis, consensus conferences[137].

The point of Grunwald's analysis that we would like to emphasise here is that there is an (on-going) conflict between the two approaches, which consists mainly of the difficulties faced in finding a right balance between the need for *normativity* and the need for *operationalization*. The box n5 below presents some consideration with respect to this, as discussed during the Rome workshop.

Box n5 - Rome workshop focus

Operationalization: positive and negative implications

The challenges inherent in methodologies that aim at the *operationalisation* of nuanced concepts (like those of "privacy" and "ethics") was also discussed by Emilio Mordini in his introductory speech. Generally speaking, operationalisation refers to creating operational definitions in order to make a concept clearly distinguishable or measurable. It may also involve the need to translate complex decisions into protocols, into clear procedures. In this sense, it is one of the options for the governance of difficult, ambiguous situations and policy decisions. Operationalisation is also conceived as an answer to the need of complex, pluralistic societies to set up procedures that may be assessed and verified in a transparent way, also in order to identify clear cut and unambiguous responsibilities. Rather than allowing common sense or ad-hoc professional experts to govern what is to be done, appropriate decisions are stipulated by formulae, algorithms, decisional software, best practices guidelines, etc. In order to operationalise a complex decision, one needs to (1) split the action/decision into clear cut steps, (2) establish causal relations between steps, (3) define a metric which allows to validate and regularly assess the system, (4) create a routine based on follow-the-rule approach which substitute the previous seat-of-the pants decision.

In the field of ICTs-related risk assessment, the operationalisation of privacy and other ethical issues is currently the option being adopted by the vast majority of scholars dealing with critical issues of emerging technologies. Operationalisation is often unavoidable and desirable, but carries some risks. In his presentation, Emilio argued that there are both positive and negative aspects. The positive ones include the precautionary approach that is behind such procedure, the effort to provide more transparency and clearer allocation of responsibilities, as well as to allow a possibility for public review. Negative aspects include the risks inherent to the strict, defensive observance of protocols and mechanical following of procedures that can be inappropriate (e.g. one may become more interested in procedures than in the outcome), to the distribution to the blame (the so called "blame game"), and the risk related to the difficulty in reprogramming the protocols. One has always to remind that accountability and trust should be the final outcomes of this approach.

Emilio concluded his introductory remarks with two suggestions and one consideration, aiming at finding a balance among different strategies for the governance of complex policy actions. The first suggestion was related to the need to carefully decide and define what can and cannot be operationalised. This needs to be done having in mind the existence of a human tendency to deny what is difficult, hardly intelligible and classifiable, a tendency that may "oblige" us to get rid of the problem simply denying it. Non-"operationalisable" decisions often require an educational approach that cannot be skipped in any case. The second suggestion was to take into account that operationalisation works better in small communities, limited organisations and situations. In large organizations, and wide contexts, where the bureaucratic component tends to prevail, operationalisation is extremely risky because it can be easily turned into a blame avoidance instrument. The final consideration was related to the fact that behind any privacy and ethical decisions there are power relationship that need to be considered. Usually only by empowering the weakest one can achieve the goal of protecting ethical values, privacy and personal data. If you don't modify the distribution of power, any ethical procedure is going to be overcome by the most powerful agents in society.

Grunwald's suggestion on how to overcome the operationalization deficit of technology ethics is that ethical reflection is integrated into already existing or still to be developed "pragmatic sites"[138], i.e., situations in which the result of ethical reflection can find an entry into the planning and decision-making procedures of technology development. Even if this does not imply that reflections on moral conflicts can

[137] One of the ideas behind the development of a Privacy Impact Assessment framework is to make use of these tools, as developed in the TA field, in order to identify current and potential critical issues (see also section 5.3 below).

[138] Grunwald, op. cit. 1999, [page 173].

always provide answers to all relevant questions, Grunwald argues that "as soon as participants in technology development reflect on ethical questions, they open up the possibility for potential effectiveness and therefore, ensure practical relevance"[139]. On the other hand, technology assessment may face its suggested normative deficit by not restricting itself to cost/benefit analysis and including ethical reasoning. As Grunwald suggests, however, these approaches are more *complementary* than contradictory and he proposes a more comprehensive approach called Rational Technology Assessment[140].

Generally speaking, in recent years the trend is towards the merging of the two approaches. The option of *proceduralism* is increasingly taken to be a solution to the limits of the classical ethical theories in relation to emerging technologies[141]. Although other approaches to ethical assessment of new technologies are currently available (see section 5.5 below), on the one side methodologies deriving from TA are included in technology ethics, and on the other ethics is being increasingly conceived as an important partner in technology assessment.

The analysis carried out until now has some interesting implications with respect to the development of a framework for identifying and evaluating ethical issues emerging from ICTs.

It should be clear that the **discussion on the role ethics may play with respect to ICT governance is still on-going and needs to be deepened**. Technology ethics is not a mature field of research and additional contributions are needed with particular regard to general work on ethical theories which should *describe* and *evaluate* emerging technologies. The scope and agenda for a *better* technology ethics depends not only on how technology is conceptualized (also within the scope of its "neighbouring disciplines") but also on the core ethical values that are both shared or emerging. The standard ethical theories at our disposal might not provide sufficient support with respect to this. There is a need to deepen the debate on which ethical theory (on how to identify the *right-making* criteria) among the classical ones (i.e. consequentialism/utilitarianism, Kantian ethics, virtue ethics) is adequate to evaluate emerging technologies, or whether a different ethical approach, specifically targeted to ICT-related issues, is needed. In relation to this, *proceduralism* is emerging as different approach to how to tackle the challenges posed by emerging technologies under uncertain and complex conditions.

In this fast changing, complex context, we argue that the role of ethics can not only be to provide a code of action or a particular normative analysis about specific questions raised by specific technologies. The role of ethics should be also to **investigate more general questions, about the long-term consequences of technology developments, as well as more conceptual, *meta-ethical*, questions**. Within these categories, we include also the questions related to the ethical justifiability of various methods of technology assessment, i.e. questions on how can the consequences of technology for the individual and society be adequately understood and evaluated, or on whether their impact can be adequately measured *from an ethical perspective*[142]. With respect to this point, we argue that an ethical governance tool should take into consideration different values, and should be flexible enough to incorporate new ones, since ethical concerns usually develop along with technologies developments as well as with the research carried out in other neighbouring disciplines (in particular TA and forecasting studies, PoT and STS "co-evolution" concept)

Many of the controversial questions that specific issues raise, such as those related to the concept of privacy, are difficult to resolve because of the conceptual puzzle as described above[143]. **A more developed analysis is also needed on how to tackle the challenges in the application of the ethical theory to real life cases in order to address concrete challenges**.

[139] Ibid., [page 173].
[140] Ibid., [page 180].
[141] Goujon, Philippe, Catherine Flick, *EGAIS Project (The Ethical Governance of Emerging Technologies) D2.1 - Grid-based Questionnaire development*, [page 16].
[142] This was one of the main aims of the Rome workshop.
[143] See Nissenbaum, op. cit., 2004, [page 238].

Finally, particular attention should be paid to the problem of engaging stakeholders in discussion of ethical issues, and in particular on considering under which conditions the affected stakeholders categories (as groups or individuals) can be conceived as "moral agents". The **identification of the moral agents** to be involved in this decision-making process refers also to the consideration of their *moral preferences*.[144]

To sum up, it can be said that while on the one hand there are no doubts that emerging technologies are having a deep impact on the values and principles of our democratic societies, identifying, describing and addressing *ethical* issues raised by ICT remains a challenge. This is due to many different factors, first of all that technologies are emerging rapidly and impacting the way human conceive themselves, their values and their relationships. The philosophical (ethical) interest in the ethical implications of emerging technologies only emerged in recent times, when applied and professional ethics on the whole was on the rise, and, on the other hand, it is constantly evolving alongside developments in technology themselves.

Moreover, being characterized by a diversity of approaches, sometimes it is even doubted that an "ethics of emerging technology" exists as an independent, homogeneous research field. Some scholars have identified the main limitation of contemporary technology ethics in this lack of work in general issues, in contrast with the developments in applied ethics research in specific disciplines, such as nanotechnology, computer ethics, biotechnology, and so on[145]. As a consequence, key questions still to be addressed are whether classical ethical theories are adequately equipped to deal with the challenges of developing effective models for a broader ethical impact assessment of emerging technologies.

The following sections aim at contributing to this debate by analysing the state of the art and clarifying the structure of the recently developed impact assessment frameworks based on the identification and evaluation of privacy and data protection issues (section 5.4) as well as on more "strictly" ethical aspects (section 5.5). Before summarising the main features of these approaches we will briefly discuss risk assessment, technology assessment and impact assessment methodologies (section 5.3).

5.3 Quantitative approaches to inform decision-making on new technologies: risk assessment, impact assessment, technology assessment

We have already said that one of the main trends to identify ethical aspects of emerging technologies is to incorporate these aspects into an analysis framework is mainly derived by Privacy Impact Assessment methodologies.

The expression "impact assessment" is linked to that of risk assessment. The concept of risk, when considered scientifically, takes the form of the *calculation of a probability* that something bad happens. Risk implies a specific form of knowledge of causal relationships between particular conditions, specific actions (decisions) and possible consequences[146]. As already mentioned, a distinction is usually made with the concept of *uncertainty*, which is the product of the actual current limits of science (the unknown) and the "in principle" limits (the unknowable). Our aim here is to point out that what makes the "risk assessment" approach particularly problematic and hardly applicable in ethics is the fact that in this discipline the chief issue would be to first find an agreement on the very definition of what is good and bad, or, using another expression, on the very definition of what is "ethically risky".

Generally speaking, two major approaches can be identified for the definition of "*technological risk*". The *quantitative* approach is based on the calculus of probability of physical harm, and is usually advocated by engineers and technologists, claiming that we need a common denominator for evaluating diverse technological hazards. Such a methodology has the positive side that such risk is measured and can be more adequately evaluated. On the other side, philosophers and other humanistic critics claim that

[144] On the engagement of stakeholders into PIA methodologies, see also section 6.2.

[145] See Brey, Philip, op. cit., 2012

[146] van Loon, Joost, op. cit., 2000

technology risk cannot be defined purely in quantitative terms, and that it includes more than physical harm, since technology often threatens other goods, such as civil liberties, personal autonomy, and fundamental human rights, which can be more properly evaluated from a qualitative perspective.

Since the 1970s, different frameworks have been developed for measuring different types of risks, such as environmental impact assessment, technology assessment, programme assessment (such as those used by the European Commission, EC), societal impact assessment. On a similar level for the concept of "*risk*", the implicit idea behind the use of the term "*impact*" is that the actual consequences of collective human actions can be quite different from the planned ones. The term aims to capture positive and negative, expected and unexpected, intended and unintended consequences of an action / decision. An impact necessarily demands to be measured: it is paramount to evaluate the degree of dependence between the force applied and the effect produced. The measure of an impact always implies a value judgement, i.e. a definition of which effects are positive and which negative, through the adoption of a scale of values. Though evaluation methods can be either qualitative or quantitative, people tend to rely more on *quantitative* evaluation, which may seem more objective.

At the Rome workshop we discussed on the potential balance to be sought between quantitative and qualitative methodologies, taking insight from the context of clinical ethics (see box n6 below).

Box n 6 - Rome workshop focus

Ethical Technology Assessment (ETA)

George Agich, co-director of the international conferences on clinical ethics and consultation, gave a speech on "Ethics between checklist and philosophical enquiry". In his paper, George argued that ethical impact assessment can make a positive contribution to the assessment of risk only if it is not ethical in the conventional sense, but is philosophically engaged in the development of new technologies. A conventional ethical impact assessment would benefit from such an "informed philosophical understanding of the technologies in question". The talk aimed at presenting the model of clinical ethics as a way of doing ethics that is engaged in practices, and argued that the technology assessment may benefit from this approach. The problem is that sometimes in Ethical Technology Assessment, ETA, the knowledge of technology functioning and potentialities seem to be optional, while it is crucial. ETAs should be much more rigorous in understanding the technology and the assessment of technologies should be used to improve the overall process.

One has to acknowledge the complexity of the exercise of technology assessment. Technology have complex development histories and a political dimension, that each ETA effort should not forget. The conventional approach is based on the consideration that ETAs are framed under diffuse, yet often widely accepted, frameworks/theories (principalism, virtue ethics, etc) or concepts/principles (autonomy, beneficience, non-maleficience, justice, privacy, fidelity). It has to be noted that the principles may have different and contradictory applications, and it is always crucial to take the context into account. Secondly the ethical assessment based on an ethical theory often carry the epistemological stance of "view from nowhere", that can impede constructive dialogue between those doing ETA and engineers/developers. The task of ETA should be pragmatic, that is, to engage ethics into a practice, to apply ethical principles but through the knowledge of engineers' concerns and feelings. Engineers have ethical sensibilities but sometimes a different language to explain them.

In the present society, the concept of *risk* becomes fundamental to the way the social world is *organized*. Prediction of the future is a relatively standard activity in many sectors of modern societies. According to Beck, the discourse of risk "characterize a peculiar, intermediate state between security and destruction": it begins where trust in our security and belief in our progress ends and it ceases to apply when the potential catastrophe actually occurs[147]. It is *a cultural perception* and *definition* that characterize risk: a society that conceives itself as a risk society is, to use a catholic metaphor, "in the position of the

[147] Beck, Ulrich, "Risk Society revisited" in Adam, Barbara, Beck, Ulrich, van Loon Joost, op. cit., 2000

sinner who confess his or her sins in order to be able to contemplate the possibility and the desirability of a better life. However, few sinners actually want to repent and instigate change"[148].

Commenting on Beck's concept of "risk society", Anthony Giddens discusses on the meanings of this expression, i.e. not only the fact that modern social life introduces new forms of dangers which humanity has to face, but also that living in such a society means "living with a calculative attitude to the open possibilities of actions, positive and negative, with which, as individuals and globally, we are confronted in a continuous way in our contemporary social existence"[149].

In line with these considerations, while discussing the impacts on our *moral capacity* of two great modern institutions, bureaucracy and business, Bauman argues that they have a number of effects in ethical decision making. The result is *neutralization* of morality by business (through instrumental rationality) and bureaucracy (through procedural rationality), with their emphasis on *rules* more than on *judgement*. "Ours is an era where morality rests with the individual, alone again with her or his choices, no longer able to depend on old certainties"[150].

Bauman discusses the divide between reason and emotion as the trademark of our modern world. In a context where for every problem there is only one reason-dictated solution,

> *the moral world can only be, therefore, a regular, orderly world (an orderly world is one in which probabilities of events are not random; some events are considerably more probable than other, some have virtually no chance of happening). Moral persons [...] can only be guided, consistently and in a systematic fashion by laws, rules and norms; principles which clearly specify what in a given situation one should do and what one should desist from. Morality, like the rest of social life, must be founded on law, and there must be an ethical code behind morality, consisting on prescriptions and prohibitions. Teaching or coercing people to be moral means making them to obey that ethical code. By this reasoning, becoming moral is equivalent to learning, memorising and following the rules*[151].

Bauman concludes that "we seem to require now an entirely new brand of ethics", a new ethics which probably should be increasingly interested in *emotions*, more than in *pure rationality*.

The concept of risk becomes particularly relevant for ethics[152] when, for instance, we consider the distinction between risk decision makers and those who have to deal with the consequences of the decision of others. What constitutes "acceptable risk"? How should risk be distributed? In a decision-making process, where uncertainty (and not clear, measurable risk) is prevalent, the concept of *precaution* might apply.

The *precautionary principle* has been partly founded upon a growing acknowledgment by environmental science of its own limitation. In Europe, the precautionary principle is enshrined in the 1992 Maastricht Treaty as one of the three principles upon which the 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.

Although this principle operates in context of scientific uncertainty, it is considered by its proponents to be applicable only when, on the basis of the best scientific advice available, there is good reason to believe that harmful effects might occur. One of the difficulties in the application of this principle today is

[148] Beck, Ulrich, op. cit., 2000

[149] Giddens, Anthony, Modernity and self-identity. Self and society in the late modern times, Stanford University Press, 1991.

[150] Bauman, Zygmund, *Alone Again, ethics after certainty*, Demos Papers, 1994

[151] Bauman, Zygmund, op. cit., 1994

[152] Risk management and risk assessment are usually considered as a managerial theme, more than an ethical one, even if some scholars have considered risks not only as factual but also as value statements. In this case, risks would be something in between, a "mathematicized morality", since they are also related to standards of a tolerable or non-tolerable life. See Beck, Ulrich, op. cit., 2000 [page 215]

that there is often an irreducible conflict between different interests, so the debates necessarily involve politics. According to Von Schomberg[153], scientific and public controversies often remain inconclusive when there is a lack of consensus on the normative (ethical) basis of such assessment mechanism. It would therefore be necessary to think about a specific ethical governance that could allow for an analysis of those values underlying the precautionary principle and its applications. An operational definition of the precautionary principle specifically targeted to the European Union Policies is also proposed[154]:

Where, 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.

Going back to the link between innovation and ethics, however, it has to be noted that the precautionary approach has been highly criticized. According to David Deutsch the principle is an expression of *blind pessimism* and inhibits development of knowledge:

Blind pessimism is a blindly optimistic doctrine. It assumes that unforeseen disastrous consequences cannot follow from existing knowledge too (or, rather, from existing ignorance). Not all shipwrecks happen to be record-breaking ships. Not all unforeseen physical disasters need be caused by physics experiments or new technology. But one thing we do know is that protecting ourselves from any disaster, foreseeable or not, or recovering from it once it has happened, requires knowledge; and knowledge has to be created. The harm that can flow from any innovation that does not destroy the growth of knowledge is always finite; the good can be unlimited. There would be no existing ship designs to stick with, nor records to stay within, if no one had ever violated the precautionary principle. [155]

5.4 Broadening the scope of a Privacy Impact Assessment

Privacy and data protection related issues are, of course, key concerns of a privacy impact assessment (PIA). The goal of PRESCIENT was broader than PIA, i.e., it was to develop a Privacy and Ethical Impact Assessment framework, taking into account, not only privacy and data protection issues, but also the identification and evaluation of *ethical issues*. [156]

In this section, we will give a brief overview on the state of the art of PIAs. Since more detailed and comprehensive information can be found in the references mentioned in this section, as well as in Section 6.1 on “A guide to Privacy and Ethical Impact Assessment”, the aim here is to focus more on those aspects which are among the principal challenges for an effective implementation of an integrated privacy and ethical impact assessment, and to critically reflect on these tensions.

The concept of PIA emerged and grew *outside* Europe from about the mid-1990s, in Australia (2006), Canada (2002), New Zealand (2002) and US (1996). Scholars doing pioneering work in PIA include, among others, Blair Stewart, Roger Clarke[157] and David Flaherty[158]. Roger Clarke defines PIA as (2011,

[153] Von Schomberg, René, “The precautionary principle and its normative challenges”, in Fisher, E., J. Jones and R. Von Schomberg, *Implementing the precautionary principle: Perspectives and Prospects*, Edward Elgar Publishing Limited, 2006

[154] Von Schomberg, René, op. cit., 2006

[155] Deutsch, David, The beginning of Infinity, Explanations That Transform the World, Penguin Books, 2012, [page 201].

[156] On this, see Wright, David, and Emilio Mordini, “Privacy and Ethical Impact Assessment”, in Wright David, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

[157] http://www.rogerclarke.com/DV/#PIA see also Clarke, Roger, “Privacy Impact Assessment: Its Origins and Development”, *Computer Law & Security Review*, Vol. 25, No.2, April 2009, pp. 123-135

111) “a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme”. Clarke conducted a comparative study on PIA guidelines. Based on ten criteria[159] for assessing the quality of such guidelines, Clarke classifies the quality of PIA guidelines in three groups: inadequate, moderate quality and high quality.[160] In Europe, the 2007 (rev. 2009) UK ICO’s *PIA Handbook*[161], the Slovenian PIA in e-government (2010), and the Irish PIA guidance (2010) are the most known examples[162]. The UK Information Commissioner’s Office’s *PIA Handbook* includes templates that specify questions to be asked for assessing compliance of a project with data protection. The Handbook identifies four types of privacy: privacy of personal information, bodily privacy, personal behaviour privacy and of personal communication[163].

With reference to international institutions, ISO 22307:2008 PIA for financial services defines a methodology that organisations in the privacy and public sectors can use to identify privacy issues and mitigate risk associated with processing the financial data of costumers and consumers, business partners and citizens. The European Union has endorsed a privacy impact assessment framework for RFID, which identifies privacy goals based on the EU Data Protection Directive[164], which was also endorsed by the Article 29 Working Party. The Madrid Resolution adopted by the International Conference of Privacy and Data Protection Commissioners in November 2009 encourages also the implementation of privacy impact assessments prior to implementing new information systems and/or technologies for the processing of personal data. As is discussed in depth in chapter 4, the proposed new data protection reform has identified PIA as a crucial element in data protection related issues.

A recently EU funded project, Privacy Impact Assessment Framework (PIAF)[165], looked in detail into the issue of the development of a PIA framework, and gave a comprehensive overview of PIAs around the world. Best practices examples have been also presented and open issues discussed in a recently published volume on PIA[166]. The book discusses various privacy impact assessment frameworks from Australia, Canada, New Zealand, the UK and the US. PIA is defined as “a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts”[167]. However, PIA is not simply a matter of identifying privacy risks but also of engaging stakeholders in the process of finding solutions. A PIA is thus conceived as a *process* that involves risk assessment and stakeholder consultation. According to the PIAF project, PIA can be conceived as “the culmination, in the privacy protection field, of social, political and legal processes of more than 50 years, with their roots in environmental, social impact assessments and technology impact assessment of the past”[168].

[158] See Flaherty, David, *Protecting Privacy in Surveillance Societies*, The University of North Carolina Press, 1989.

[159] These are: clear status of the guidance document (voluntary, mandatory, etc), ease of discoverability of the document, clear statement on applicability, clear statement that PIA-responsible persons are needed, early commencement of PIA is stressed, stress of sufficient scope, stakeholder engagement, stress that this is a process and not a product, clear description of the PIA process, definition of the role of oversight agencies.

[160] Clarke, Roger, “What’s ‘Privacy’?”, *Australian Law Reform Commission Workshop*, 28 July 2006.

[161] http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx

[162] See also http://www.piawatch.eu

[163] As discussed in the previous chapter, PRESCIENT has expanded the categorisation of privacy into 7 categories: privacy of the person, privacy of thoughts and feelings, privacy of location and space, privacy of data and image, privacy of behaviour and action, privacy of personal communication, privacy of association (including group privacy).

[164] This is probably the first time that the Commission formally speaks of “privacy and data protection impact assessment”. See European Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification, C(2009) 3200.

[165] See also chapter 6 on this. PIAF project website is available at the following link http://www.piafproject.eu

[166] Wright David and Paul de Hert (eds), op. cit., 2012.

[167] Ibid., p. 5

[168] See http://www.piafproject.eu

PIAs usually target *informational privacy*, i.e., the aspect of privacy coinciding with *data protection*. By its very nature, data protection is the most *operationalizable* trait of privacy (i.e. it is about somehow more easily *identifiable impacts*, or about checking the *respect of regulations* -- EU data protection law in this case). PIAs thus deal with the information privacy applications of a broader, more nuanced and difficultly definable concept.

On the relation between privacy and data protection from an ethical perspective, see also box n 7 below.

Box n 7 - Rome workshop focus

Privacy and data protection

The important distinction between *privacy* and *data protection*, intertwined but different notions, was enlightened by Emilio Mordini in his introductory remarks. Etymologically the word "privacy" derives from the Latin *privatus*, past participle of *privo*, which means "I cut away", I deprive. Privacy thus refers to the state of something that is separated, isolated, secluded from others. Privacy is a moral concept when it is framed in terms of claims about the moral status of the individual self, about its dignity and relations to the others. Privacy is a very nuanced notion, as it refers to something that is linked to the concept of "appropriate space". Emilio argued that privacy for humans might be conceived as having the same role that the concept of territoriality has among animals. As discussed in PRESCIENT D1, the modern and western idea of privacy does not belong primarily to ethics. It is a term originated by the social and political theory to describe what is not public business, notably, which is not business of the law and the government (whatever kind of government it is). The notion of privacy becomes an ethical term when it is framed in terms of right, say, the (a) *right to privacy*, or when it is framed in terms of good, say, (b) *privacy as a value* or as an (c) *instrument to achieve other values (e.g., being free, flourishing, achieving some virtues, affirming his own dignity, etc)*. This opens three main issues, say, 1) the foundation of the notion of privacy as an ethical concept; 2) the ethical and political implications of privacy claims; and 3) ethical problems raised by emerging technologies vis-à-vis the notion of privacy.

On the other side, the concept of "data protection" emerges from the contemporary "information society" revolution. It was shown that each revolution in history has been characterized by the emergence of a new commodity. Data, the commodity of the present days, is generated by technologies of digitalization which turn almost everything into measurable items and finally into digits that can be manipulated, stored, and marketed. In this context, *personal data* is a special subcategory which includes data generated by the digitalization of the person and of its private sphere. Data protection deals with normative issues related to this new kind of commodities, and refers to the regulation of a complex array of activities with the purpose of guaranteeing the free flow of this marketable information. With particular reference to the concepts behind the expression "*personal data protection*", ethics should investigate the moral justifications behind the protection of such information (i.e. explain why should we protect them, what is the rationale of this protection) as well as the modalities in which that protection can be realized (what does this protection exactly mean and how can be realized).

Emilio argued that the concept of data protection has generated a technical conception of privacy, that is now better framed and understood in terms of risk management and technical ability to protect or to penetrate the (informational) private sphere.

It has to be noted that even if the standard target of many approaches to PIA is every initiative involving the "processing of personal information", some have argued that a PIA should address not only information privacy, but other types of privacy as well.[169]

The challenge still remains on *how* nuanced and less easily identifiable individual or societal values, rights and freedoms, that may be impacted by emerging technologies, can be *best integrated* into such frameworks. Before addressing this question, one should not forget that the key challenge and open question is to first identify and agree on what these freedoms and rights are, i.e. to agree on what type of information society is desirable, and what values constitute that society. And in order to agree on these, one should keep in mind that ethical decision making does not work only on the basis of a "consensus

[169] See Finn, Rachel, David Wright and Michael Friedewald, "Seven types of privacy", in Gutwirth, Serge, Ronald Leenes, Paul De Hert et al. (eds.), *European data protection: coming of age?*, Springer, Dordrecht, 2013.

mechanism"[170]. Ethical decision making is a complex, context dependant process, in which not only law but cultural and moral pluralism play important roles as well.

Some aspects of the issues of *complexity* and *uncertainty* have also to be considered. As specialised tools for risk management, PIA's effectiveness depends on a regular review of proportionality between the benefits of a given ICT or security technology or other initiative impacting privacy and its privacy intrusiveness. A lack of information may make it difficult to identify *emerging* ethical issues, which is a pressing need in any *anticipatory* (or prospective) technology assessment exercise. There is a general lack of argumentation on how this can be effectively achieved, and how we may be able to deal proactively with complex technologies[171].

In order to overcome the criticism about the fact that conventional PIAs are usually too narrowly focused on informational privacy, in his contribution on "A human rights perspective on Privacy and Data Protection Impact Assessment", Paul de Hert suggests that privacy impact assessment can be seen as an assessment of new technologies' compatibility with human rights. This can be achieved through seven basic tests, i.e. by addressing the following questions:

- is the technology used *in accordance with and as provided by the law*?
- is the technology *serving a legitimate aim*?
- does the technology *respect the inviolability of the essence of all human rights*?
- is the technology *necessary in a democratic society*?
- is the technology *providing no unfettered discretion*?
- is the technology *proportionate, appropriate and least intrusive means*?
- besides the respect for privacy, is the technology *consistent with other human rights*?

The reference frameworks for implementing this test are the European Charter of Human Rights, ECHR and the case law of the European Court of Human Rights (ECtHR). According to the author, it is also clear that "a right to have technology assessed before their launch is emerging as a human right"[172].

A second example on how to broaden the scope of a PIA, including a more qualitative analysis, is offered by Charles Raab and David Wright in their contribution on "Surveillance: extending the limits of Privacy Impact Assessment"[173]. This article discusses how to develop a privacy impact assessment that is particularly finalized to the investigation of the impacts upon privacy that *surveillance* technologies might have. The authors point out that surveillance technologies may affect different connotations related to *privacy*, which is conceived both as an individual right and a societal value. Conventional PIAs (PIA_1) need to be accompanied by other types of impact assessments, such as those addressing the technology compliance with other individual values and human rights (PIA_2), as well as the impact on groups and categories (PIA_3) and on the society and the political system as a whole (PIA_4).

As discussed until now, in technology assessment methodologies, the balance between the need for operationalization and the importance of introducing qualitative, normative, evaluative reflections cannot be found so easily. In the following section, we present an overview of contemporary approaches to *ethical* impact assessment of emerging technologies.

[170] See Stahl, Bernd Carsten, and Kutoma J. Wakunuma, *ETICA D5.3 Project Nomenclature (Now Glossary) - Ethical issue determination,* 2009, [page 29]. Among these conditions, there is the Hume principle that "values cannot be inferred from facts". It is not because there is a consensus on a determinate issue that this is ethically justified.

[171] See Mordini, Emilio, "New Security Technologies and Privacy", in European Commission, *Ethical and Regulatory Challenges to science and research Policy at the Global Level*, 2012.

[172] de Hert, Paul, "A human rights perspective on Privacy and Data Protection Impact Assessment", in op. cit., 2012.

[173] See Raab, Charles and David Wright, "Surveillance: extending the limits of Privacy Impact Assessment", in op. cit., 2012

5.5 Current ethical approaches to technology impact assessment

With the expression "*ethical impact assessment*" we refer to an *instrument*, which is currently usually conceived as a framework for examining the ethical implications of new technologies, which should aim at (a) identifying, and (b) addressing *current* or *emerging ethical issues* arising from the *development* (research and development stage) and *deployment* (application stage) of new technologies, particularly in the field of ICTs.

Through this *anticipatory* methodology (i.e. aiming at foreseen ethical issues at a very early stage of technology development), the aim is to incorporate ethical reflection into the process of research and innovation. This is also conceived as a *participatory* methodology, since it aims at involving *relevant* stakeholders in the assessment process.

The discussion about how to develop a *methodology* for morally designing and evaluating technology under complex and uncertain dynamics is still in its infancy. Some of the key results in this field are summarized in the following paragraphs. They particularly have been developed in the field of surveillance technology ethics, ICT research ethics, and more generally technology ethics.

In the field of *ethics of surveillance technologies*, in an article published in 1997, Gary T. Marx was one of the first to propose a matrix aimed at uncovering ethical issues of new technologies[174]. The matrix is derived from a broadened approach to the Principles of Fair Information Practice (i.e., data protection principles) and identifies a set of factors (i.e., the means of the collection, the data collection context, and the uses/goals) against which new technologies should be judged. Each factor is further developed around a set of questions. As the author emphasises, the most overarching and important idea behind the framework is the Kantian idea of respect for the dignity of the person.

Marx's methodology is based on a mixed approach grounded both on categorical principles and on empirical consequences. In order to offer a sound reply to the criticism around his methodology's lack of a formal "normative argument" (offering justification for the principles, indicating their logical implications and leading to clear conclusions), Gary T. Marx states that "in matters so complex and varied we are better served by an imperfect compass than a detailed map. […] A chart of new territories needs to begin with simple coordinates and rough estimates". The proposed matrix is a contribution in this direction, by offering a tool to identify societal norms that the author believes both do and should inform an ethics of surveillance.

David Lyon also discusses the fact that everyday surveillance, as a central means of social sorting, of classifying and categorizing populations and persons for risk assessment and management, requires new ethical approaches to be developed[175]. All these surveillance-oriented processes are not value-free but deeply impact the life of those under surveillance. In addition, they may affect the ways in which individuals conceive society and social relations.

In the past three decades, privacy and data protection regulations have been one of the most important achievements in order to deal with these challenges. However, Lyon holds, they are probably not the perfect remedies for contemporary hidden, ubiquitous, normalized surveillance practices. Lyon argues that "a fresh ethical approach is called for because we are only just starting to understand how today's surveillance works"[176]. The first step of Lyon's proposed research methodology is to understand how surveillance technology operates and what can be the personal and societal consequences. The second is "to find an agreement on what constitutes the human dignity and the social justice that may be compromised

[174] Marx, Gary T., "Ethics for the new surveillance", *The Information Society*, 14: 171-185, 1998

[175] Lyon, David, *Facing the future: Seeking ethics for everyday surveillance*, Ethics and information technology, 3: 171-181, 2001,

[176] Ibid., [page 174]

by those systems"[177]. He then proposes an approach that considers personhood as central, highlighting its social and embodied dimensions.

In the field of *professional ICTs ethics*, the Menlo report[178] seeks to offer guidance to ICT researchers by proposing a framework articulated on four core ethical principles. The described principles are *respect for persons* (including both individuals and society, and considering organisations), *beneficence* (two general rules specified under this obligation are (1) do not harm and (2) maximize possible benefits and minimize possible harms), *justice* (addressing fairness in determining who ought to receive the benefits of the research and bear its burdens), and *respect for law and public interest*. In order to properly apply any of these principles, the report also states that it is first necessary to perform a systematic and comprehensive stakeholder analysis.

Some scholars involved in the elaboration of the Menlo Report elaborated what they called an "Ethical Impact Assessment" framework for ICT research[179], which should assist researchers in formulating policies, processes, and methodologies that align with ethical principles throughout three research lifecycle phases, i.e. research collection, research use or management, and research disclosure. This EIA is defined as an "incipient prototype, modelled after the more established privacy risk management framework, the PIA"[180]. For each principle, a set of questions is also proposed in order to apply it a specific context.

In the discussion of the current limitations in contemporary approaches to Philosophy of Technology[181], Brey suggests that, in addition to the lack of work in theories for general technology ethics (in contrast with what happens in applied ethics for specific disciplines, such as nanotechnology, computer ethics, biotechnology), we are also missing effective models for (a) *ethical technology assessment* and for the (b) *ethical development of new technologies*.

Brey identifies some contemporary approaches to (a) in the EIA (Ethical Impact Assessment) derived from Privacy Impact Assessment[182], in the methodology developed in the scope of the ETICA project[183], and in the ATE (Anticipatory Technology Ethics) approach methodology which should overcome the main criticisms of the previous ones[184]. Contemporary approaches to (b) include Nissenbaum's embedded values theory and derived approaches such as Value Sensitive Design (VSD) and Disclosive Technology Ethics.

According to Brey, the *phase* of the technology development at which this methodology is aimed plays a crucial role. If, as Moor argues, ethical problems multiply as technology moves from the introduction to the power stage, ethics at the research and development phase still need to be properly addressed, and adequate models on how to incorporate ethical reflection in the design of new technologies still need to be

[177] Ibid., [page 180]

[178] The Menlo report was the result of an interdisciplinary working group sponsored by the US Department of Homeland Defense (DHS), which commenced in 2009. See DHS Working Group, *The Menlo Report, Ethical principles guiding ICT Research*, September 2011.

[179] Kenneally, Erin, Bailey, Michael, and Maughan, Douglas, "A Framework for Understanding and Applying Ethical Principles in Network and Security Research", in *Workshop on ethics in Computer Security Research* (*WECSR '10*), Tenerife, Canary Islands, Spain, January 2010. David Wright also introduced the term "EIA" in relation to ICTs. See Wright, David, "A framework for the ethical impact assessment of information technology", *Ethics and Information Technology*, Vol. 13, No. 3, September 2011, pp. 199-226. First published online 7 July 2010. Wright coined the term even earlier in a SENIOR project report. See Wright, David, *Report on Best Practices and Roadmap towards the Roadmap*, Deliverable D4.1, Prepared for the European Commission, 12 Nov 2009.

[180] See Kenneally, Erin et al., op. cit, 2010 [page 2]

[181] See Brey, Philip, "Philosophy of Technology after the Empirical Turn", *Techné: Research in Philosophy and Technology*, Vol. 14, n.1, 2010.

[182] See David Wright, op. cit., 2010.

[183] See Stahl, Bernd Carsten, et al., "Identifying the Ethics of Emerging Information and Communication Technologies, ICTs: An essay on Issues, Concepts, Method", International Journal of Technoethics, Vol. 1, n.4, October-December 2010, pp. 20-38.

[184] See Brey, Philip, "Anticipatory Technology Ethics for emerging IT", *Nanoethics*, Vol. 6, n1, April 2010, pp1-13.

developed. Impact assessment at this stage is still largely speculative, will focus on general ethical issues in relation to new techniques and on speculative ethical analysis of possible future applications.

In addition, since the challenges posed by *uncertainty* can be only solved by being more informed about new technologies, as was already argued by Moor (2005), the role of forecasting studies is thus paramount in *informing* such a comprehensive technology ethics. According to Brey, the aim of the *forecasting approach* is to speculate on future devices, relying on existing forecasting studies. Such studies are undertaken in two related fields: futures studies (aiming at studying what possible or probable futures may look like, and including Delphi methods, environmental scanning, causal layered analysis, scenarios, and so on) and technology assessment approaches (studying the effects of the new technology on industry, the environment, society, and developing instruments to steer technology in more desired directions). According to Brey, the forecasting approach has the advantage that might be able to identify more potential ethical issues, but the disadvantage that is based on forecasts that are to some degree speculative and may be incorrect.

In a more recently published essay[185], Brey critically evaluates the three contemporary approaches to an ethics of emerging ICTs, and presents the ATE.

The first approach considered is the one proposed by Palm and Hansson (2006), and has been referred to as *Ethical Technology Assessment* (eTA). This has been one of the first ethical approaches explicitly targeted at emerging technologies, and advocating the need for an ethical assessment.

The approach relies on studies in technology assessment, providing insight into both the technology in question and its social consequences, and on close interactions with developers of technologies. The main goal is not to predict far into the future but to continually assess current practices in technology development and provide feedback to designers and policy makers. This is done by confronting projected features of the technology or projected social consequences with ethical concepts and principles.

The checklist proposed is based on nine items, which should serve to identify the most common ethical issues in emerging technologies. These are dissemination and use of information; control, influence, power; impact on social contact patterns; privacy; sustainability; human reproduction; gender, minorities, justice; international relations; impact on human values. With respect to this last point, Palm and Hansson also argue that the eTA should not be committed to any particular moral theory.

According to the review offered by Brey, the checklist developed is somewhat limited, since principles such as autonomy, dignity, informed consent, distributive justice are not included. The approach is also vague as it does not specify in detail what kind of knowledge needs to be acquired from technology developers and technology assessment studies and how the ethical analysis shall be performed.

The *Ethical Impact Assessment* (EIA) methodology proposed by David Wright (2010)[186] extends the ethical checklist, which is structured around the ethical principles provided by Beauchamp and Childress (2001) and adds privacy and data protection, key elements of an impact assessment framework for emerging technologies. The framework contains ethical values and principles along with a set of questions raised by these values and principles. The paper also discusses seven elaborate techniques to engage stakeholders.

According to Brey, it is however not clear how forecasting takes place and is incorporated in this methodology, how can technology developers and other stakeholders come up with this information, and how participants are capable of answering these questions. Considering the vagueness in respect to this, Brey concludes that this framework seems more suited for ethical impact assessment of *concrete* ICT design projects. In addition, the reference principles were particularly targeted to the medical context, are based on very abstract concepts, and it is not clear how they can be applied in the ICT field.

[185] Brey, Philip, "Anticipating ethical issues in emerging IT", *Ethics and Information Technology*, Vol. 14, n.4, December 2012, pages 305-317.

[186] David Wright, op. cit., 2010. Wright's use of the term "ethical impact assessment" appears to be the first such.

The last approach discussed by Brey in his essay is the one developed in the scope of the ETICA project. This is based on three main steps, i.e.:

- *Identification* of ethical issues: by making use of projections, ETICA aims at providing a comprehensive overview of ethical issues for emerging technologies that are likely to play out in the medium term future[187]; an extensive overview of ICT ethics is also constructed and key ethical issues[188] are summarized in a normative issues matrix;
- *Evaluation stage*: a list of values and principles is presented and it is showed that any technology in the list may promote certain values while threatening others. "Value conflicts" emerge in this case, while if technology has only undesirable effects it is unlikely to cause any controversy;
- *Governance stage*: recommendations are elaborated for policy makers and other relevant stakeholders.

According to Brey, this is possibly the most elaborate ethical approach to emerging technologies that has been developed to date. It considers a *wider range* of ethical issues and emerging technologies, it engages in ethical *evaluation* and develops *recommendations* for governance. The main criticism is that the main source for collecting information is *literature* that does not use methods of *future research*. It only offers an aggregation of predictions about future technologies instead of validating them.

ETICA D4.1 – section 2[189] addresses the need to construct the theoretical background on which ETICA found their grid analysis. The issue of the "*effectiveness of ethical norms, from the conditions of their emergence to their implementation*" is addressed in this report. The framing in which the technology assessment is carried out predetermines the results. In order to construct the norm, one has to consider that since "neutrality is fiction"[190], when one tries to analyse an ethical issue, they do so within some *preconceptions*, which may have a big impact on the judgement made by the actor involved. This is why they claim that "ethical reflexivity demands an opening of the framing", though the capacitation process, by which an actor acquires a new capacity (i.e. the capacity of being reflexive upon their own framing). In addition, it is also important to understand how technology is conceptualized by an actor (i.e. deterministic/instrumental/substantial perspectives, critical theory, and so on).[191]

Finally, Brey proposes his own methodology, which he calls *Anticipatory Technology Ethics* (ATE). ATE distinguishes three levels of ethical analysis: the technology, artefact and application levels. At each of these levels, various "objects of ethical analysis" (i.e. something raising ethical issues) are defined: things, properties or processes. This approach presents a larger variety of *objects* (objects of ethical analysis) than ETICA.

Brey argues that different forecasting methods are required for the technology, artefacts and application level. If engineers are best positioned to inform the ethicist on the technology level, for artefacts and applications, ethicists should utilize existing studies in forecasting and TA, and initiate experts surveys and roundtable discussions.

[187] ETICA targets "high level socio-technical systems that have the potential to significantly affect the ways humans interact with the world". The term "emerging" refers to systems that are likely to be socially and economically relevant in the coming 10 to 15 years.

[188] ETICA identifies several "recurring issues", related to privacy, data protection, intellectual property, security. Other less obvious and currently not regulated issues are: autonomy, freedom, agency; possibility of persuasion or coercion; responsibility and liability; possibility of machine ethics; access and digital divide; power issues; consequences of technology for our view of humans; conceptual issues (e.g. notions of emotions, intelligence); link between integration of ethics into law; culturally different perceptions of ethics.

[189] Goujon, Philippe, and Catherine Flick, *ETICA D4.1 - Governance Approaches. A Critical Appraisal of Theory and Application*.

[190] Winner, Langdon, Do artefacts have politics?, *Daedalus*, Vol. 109, No. 1, Modern Technology: Problem or Opportunity? (Winter, 1980), pp. 121-136.

[191] See ETICA D4.1, table at page 25.

With respect to the ethical *analysis*, two stages should be considered: the first when ethical issues are *identified* and the second when they are *evaluated*. A third one can include *recommendations* to policy makers.

At the *identification stage*, the descriptions of the technology are cross-referenced with ethical values and principles. The ATE checklist includes: harms and risks (health and bodily harms, pain and suffering, psychological harm, harm to human capabilities, environmental harm, harms to society), rights (freedom of movement, speech and assembly, autonomy, human dignity, privacy, property, as well as other basic human rights as specified in human rights declarations), distributive justice (including intergenerational justice), wellbeing and the common good (e.g. supportive of democracy, culture and cultural diversity, happiness, desire-fulfilment, and so on).

Ethicists can determine whether a particular technology may negatively impact moral values and principles, through what Brey calls "*operationalization*" of the value or principle, i.e., providing a description specifying real-world conditions for the principle's realization or frustration. Ethicists may arrive at the values that should be cross-referenced with technology, through an ethical checklist including values that are widely accepted in society. It may be useful to develop specific checklist for specific types of technology. Brey acknowledges the disadvantage that checklist are "necessarily incomplete".

At the *evaluation stage*, the potential importance of ethical issues, the likelihood that they become a significant issue in society, as well as their relation to each other, including potential value conflicts are the elements to be assessed.

A third optional stage is the one in which the results of evaluation are *applied for various purposes*, which may include either a "design feedback stage", or "responsibility assignment stage" (when moral responsibilities are assigned to different relevant actors), or a "governance stage" (governance recommendations are made for policy makers to deal with the outcomes of the evaluation stage).

The following box n 8 presents the discussion had during the Rome workshop around one of the most critical concepts which needs particular attention while dealing with the assessment, from an ethical perspective, of emerging technologies' implications: the concept of justice.

Box n 8 - Rome workshop focus

How to incorporate justice in ethical impact assessment of emerging technologies

David Hunter, from the Department of Philosophy of the University of Birmingham, talked about “Risks, hazards and uncertainty: how to incorporate justice into ethical impact assessment”. David presented a paper on “How to object to radically new technologies on the basis of justice: the impact of uncertainty and time, synthetic biology as an example”. In his introductory remarks David pointed out that the challenges to performing ethical impact assessment of emerging technologies are related both to the difficulty in predicting the impacts of new technologies and to the fact that people don’t usually agree on ethics and on the role ethics may have in this field. The very notion of “ethical impact assessment” of emerging technologies raises both epistemic and normative uncertainty. A proposed solution might be to rely on participatory democracy as a method to agree on the importance of an ethical principle. If there is no room for actually discussing (and agreeing) on the so called ethics “background theories”, a good starting point can be to agree that a given principle is important.

Generally speaking, it ought to be kept in mind that there have been two broad arguments that provide a presumption in favour of the permissibility of new technologies. These include to appeal to the potential *benefits* that might be derived from technology and a more general claim to *liberal rights*. Usually the onus is on those who object to new technologies to show that in a particular case either these arguments don’t apply, or that there is some over-ridding ethical concern that trumps these arguments. The appeal to the principle of justice might be important with respect to these arguments. In its concrete application, this principle aims at analysing how technology impact on the power relations in society, i.e. whether it advantages the already powerful social groups, or further disadvantages the less powerful ones.

There are three broad strategies to object to radically new technologies on the grounds of social justice, each corresponding to a different conception and interpretation of this concept. In his presentation, David explored these strategies and argued that only one of them is particularly effective and it applies to only a limited number of cases of radical new technologies.

The first strategy is referred to as “*procedural justice*” and is based on the establishment of a fair procedure for the distribution of benefits derived from the technology. The focus of these theories are more on how decisions are made (i.e. the fairness of the process used to determine the distribution of benefits and burdens related to the technology), rather than on the outcome of those decisions. This might be a practical response to an inability to agree about more substantive principles . However, David suggested that even if this strategy may offer important insights on how to ensure that the introduction of a technology is ethical, it rarely provides a basis for objecting to new technologies in themselves.

The second strategy is “*outcome justice*”, based on the claim that inequalities in society should not be increased by the introduction of new technologies. This approach is endorsed by much bioethics literature, when justice concerns are raised with regards to new technologies. However, David argues that some of the strength of this argument based on the outcomes is merely apparent and provides two kinds of reasons for this. Problems that are common to outcome-based theories is that “they are action guiding only insofar as the outcome is reliably predictable”. Where there is significant uncertainty involved, outcomes are less reliable in guiding our actions. The second problem is the problem of time, i.e., on explaining at which time point should one aim at maximizing utilities and why shall we prioritize that time over the future, since often analysing the impact of a now inequality does not take into account future benefits. The difficult question to ask is whether the creation of inequalities at a specific point in time provides sufficient grounds to reject a new technology.

David’s paper argues that the “*patter-based approaches*” are the best way for a justice approach to the introduction of emerging technologies. These strategies aim at evaluating whether a technology is negatively impacting on a particular patter of distribution of resources. In order to evaluate the just patter of distribution one should consider whether the new technologies are conferring abilities or advantages that are multi-generational and transferable to members of a particular group, or whether they could confer significant first mover advantages. The main problem here is the need to outweigh justice with other competing values: in other words, if a technology has a negative impact on the patter of distribution but this is mitigated by how the technology is introduced, or by the fact that it enhance other values.

As anticipated in 5.1, Sollie has also deeply investigated how to deal particularly with the problem of *uncertainty* in evaluating emerging technologies in a responsible manner, and under which conditions is ethical impact assessment of emerging technologies possible.[192] Sollie proposes three questions to which any ethics of technology which is to be regarded as adequate should formulate answers:

(a) *Theoretical* aim of ethics: what are the right-making criteria? How are they justified?

(b) *Practical* aim: how do they guide our practical moral reasoning? Are they consistent with practicability?

(c) How does this ethical theory deal *proactively* with complexity and uncertainty (how does it construe a justified relation between a substantive and procedural approach)?

In a more recent book, Sollie investigates each of these questions from the perspective of Gewirthian ethics, and he demonstrates that the Principle of Generic Consistency (PGC) respects the theoretical and practical adequacy-requirements[193].

The previous section have been devoted to a critical overview of contemporary approaches to the ethical *assessment* of emerging technologies. With particular regard to the ethics of *developing* new technologies (in particular, computers), this is based on the idea that technology can have built-in tendencies to promote or demote particular values. Scholars were recently interested in researching whether there could or should be an ethics of computer systems separate from the ethics of using them.

The *embedded values* approach in computer ethics was formulated initially by Helen Nissenbaum[194]. Built-in moral values means that computer systems should be subjected to ethical analysis, independently from the ethical evaluation of the actual use of the system. This can be also understood as an example of the fact that new technologies are impacting upon the same way we are used to traditionally conceive ethics (i.e., concerned solely with the analysis of human conduct). This also broadens considerably the scope of ICTs ethics.

To be clear, built-in consequences are never absolute, but always relative to a set of typical context of uses. Technological artefacts are capable of either promoting or harming the realization of values when they are used.

In the box n 9 below, we present an overview on how this approach on "embedded values" was discussed during the Rome workshop.

[192] See Sollie, Paul, "Ethics, technology development and uncertainty: an outline for any future ethics of technology", *Journal of Information, Communication and Ethics in Society*, Vol. 5 Iss: 4, 2007, pp.293 - 306

[193] Sollie, Paul, "Ethics of Technology at the Frontier of Uncertainty: a Gewirthian Perspective", in Sollie, Paul and Marc Duwell, *Evaluating New Technologies*, *Methodological Problems for the Ethical Assessment of Technology Developments* Springer, 2009

[194] Nissenbaum, Helen, "Values in the Design of Computer Systems", *Computers and Society*, March 1998, pp. 38-39.

Box n 9 - Rome workshop focus

Are there values in algorithms?

Martin Peterson, associate professor of philosophy at Eindhoven University of Technology, proposed a speech on "Are there ethics in algorithms? Searching for ethics in contemporary technologies". The presentation aimed at scrutinising the recent debate over the moral status of technological artefacts and presenting the arguments to consider some of them as value-laden. The speech was structured around three claims: (1) algorithms are value-laden since they may contains ethical assumptions, (2) algorithms may influence our decision, but (3) algorithms are not to be considered as moral agents.

Martin firstly defined the term "algorithm" as a "finite sequence of well-defined instructions that describe in sufficiently great detail how to solve a problem". The mainstream view in contemporary philosophy of technology is that algorithms are value-laden since they may contain ethical assumptions (claim 1) and influence our decisions (claim 2). With regard to claim 1, a value judgment is defined as "a proposition expressing a view on how things ought to be, or what is good or bad, or desirable or undesirable". In accordance with this definition, Martin argued that some algorithms comprise a value judgment "if two or more persons who accept different value judgements would have a rational reason to design or use the algorithm differently". The example to support this claim was the one of medical imaging technologies, and the decision about how sensitive the device should be, that is related to the issue of the trade-offs between false negatives and false positives.

The third claim on the moral agency of technological artefacts was also discussed and three views were proposed. According to the so called "strong view", technological artefacts are (together with humans) moral agents (see, for instance, Verbeek, Peter-Paul, "Persuasive Technology and Moral Responsibility. Towards am ethical framework for persuasive technology", paper for Persuasive06, University of Eindhoven). The "moderate view" claims that there is an intermediate position, that attributes moral relevance to artefacts without making them morally responsible or morally accountable for their effects. The "weak neutrality thesis"' claim is that artefacts are neutral means to the end pursued by agents.

Martin discussed the claims of the "strong" and "moderate view" in order to offer a defence of the "weak neutrality thesis". The four claims of the strong view are that: (1) technological artefacts actively co-shape peoples' being in the world", (2) humans and technologies do not have a separate existence anymore, (3) technologies have thus an intentionality (in a morally relevant meaning) and therefore (4) moral agency is distributed over both humans and technological artefacts. The problematic issue of claim 1 is that technologies hardly can be *active* in producing an effect (active would be the designer or inventor). Moreover, it is not possible to state that technologies have an intentionality *in a morally relevant sense*. According to the moderate view (see Illies and Meijers), "technological artefacts are morally relevant in the sense that they sometimes affect the attractiveness of the possible actions that make up an Action Scheme (i.e., the set of possible actions with different attractiveness that is available to an agent or group of agents in a given situation). In line with this perspective, however, Martin argues that everything would be morally relevant.

Martin then discusses then the claim that a change in the realm of "can" (what is *possible*) implies a change in the realm of "ought" (what is *morally required*). Questioning whether mere possibilities really matter, Martin proposes the consideration that if our "first order" responsibility is to carry out morally right actions, the "second order" responsibility is to make sure that there are some morally good actions to choose. The weak neutrality thesis accepts the first two claims of the strong neutrality thesis (i.e., that artefacts never figure as moral agents and are never morally responsible for their effects) but rejects the third one, i.e., that technological artefacts never affect the moral evaluation of an action, since sometimes they do. The conclusion is that algorithms are essentially value-laden, but this does not entail the claim that they are moral agents.

Based on the embedded values approach, two major derivative approaches have been developed: disclosive ethics, and value sensitive design.

The "*disclosive computer ethics*" theory[195] claims that ethical implications are disclosed by systems. It is concerned with the moral deciphering of embedded values and norms in computer systems, applications and practices. Brey proposes four key values as starting points for disclosive studies: justice, autonomy, democracy and privacy. He also argues that the research in disclosive computer ethics should be multi-level, distinguishing between a disclosure level (when morally opaque practices and computer systems are analysed from the point of view of one or more relevant moral values, with the aim to identify whether the system/practice promote or demote such value), a theoretical level (when the moral theory is developed and

[195] Brey, Philip, "Disclosive Computer Ethics. The Exposure and Evaluation of Embedded Normativity in Computer Technology ", *Computers and Society*, Vol. 30, n.4, 2000, pages 10-16.

refined, particular attention is paid for new values and new moral dilemmas and for the reconceptualization of such values and dilemmas), and an application level (when the moral theory is applied to the analysis which are the outcome of the research at the disclosure level). This should also be a multi-disciplinary activity, involving ethicists, computer scientists and social scientists.

The second approach derived from the embedded value theory is the so-called "*value sensitive design*" (VSD) theory, aiming at analysing how considerations of values can be made part of the technology design process[196]. The idea is that the values of all relevant stakeholders are taken into account, and carefully balanced against each other at the design stage. The focus of Value Sensitive Design is on "human values with ethical import", such as privacy, freedom from bias, autonomy, trust, accountability, identity, calmness, universal usability, ownership, human welfare, environmental sustainability[197].

VDS relies on a tripartite methodology, based on conceptual analysis (i.e. on developing philosophically informed working conceptualizations on moral values), empirical (i.e. on conceptualising the human context of the technology use), technical investigations (i.e. focusing on how existing technological properties and underlying mechanisms support or hinder human values).

To sum up this section, a state of the art analysis of current "*ethical impact assessment*" needs to take into consideration different approaches, which have been developed only recently. A principled framework (i.e. developed on the basis of some key principles which have to be *applied* to particular situations) is usually the core element of an "ethical impact assessment". Other elements include the need to collect relevant information from technical expertise and forecasting studies, as well as to include relevant stakeholders in the assessment process. Following the identification and evaluation of ethical issues, governance recommendations can be also provided.

The PRESCIENT project is based on the idea that such an instrument would better serve these needs if derived from privacy and data protection impact assessment (PIA) models. We believe that a critical, more general reflection on the role ethics may and should play in this process is paramount, as well as a philosophical analysis of key concepts and values involved.

5.6 Philosophical and methodological challenges

A wide range of "ethical issues" are arising from the development and use of ICTs. As discussed in the previous section, among the current "ICT-ethics" trends, there are those towards incorporating ethics into R&D at the early stage of technology development (i.e. approaches mainly derived from the embedded values theory), and towards developing frameworks in order to identify and address potential ethical issues of technologies (i.e. impact assessment frameworks relying on participatory exercises, mainly derived from Privacy Impact Assessment methodologies, or anticipatory methodologies such as those developed in the scope of the ETICA project or presented as the Anticipatory Technology Ethics, ATE).

When trying to identify, address and assess ethical issues of emerging technologies, however, researchers have to take into account that they are confronted with a set of critical challenges. This chapter particularly aimed at discussing the risk that ethics might be perceived by stakeholders solely as a bureaucratic barrier to technological innovation, instead of an added value and it argued that ethical reflexivity is key in respect to this. This conclusive section provides some final considerations on the main challenges in quantifying/determining the impact of a technology on ethical principles and fundamental human rights and proposes a set of key open issues that still have to be properly addressed.

Expectations on emerging technologies include many aspects, such as technical feasibility, social usability and *moral desirability*. Differently for a pure technology assessment methodology (mainly

[196] Friedeman, B., and P. Kahn, "Human Values, Ethics and Design", in Jacko J., and A. Sears, *The Human-Computer Interaction Handbook*, 2003

[197] Ibid., [page 1187]

focused on the first two types of expectations), ethics has a "particular interest for those technologies and applications and social consequences that may cause harm, violate rights, affect well-being, or cause unjust distribution of goods"[198]. An ethical issue is one that embodies questions about whether an action is good or bad, right or wrong, appropriate or inappropriate. In addition, ethics needs to consider the potential impact of technologies on different social groups (which is relevant to issues of distributive justice), as well as the possibility of abuse of such techniques.

A framework for ethical impact assessment would be complete if explicitly based on an *established reference framework* or *general philosophical / ethical theory*. Most often traditional ethical theories can provide this adequate framework for assessing ethical problems associated with technology. The main traditions of philosophical thought (utilitarianism, Kantian ethics, virtue ethics) sometimes conflict (as an example, the approach of utilitarianism vs. the concept of human dignity). One should be aware that making these decisions necessarily implies certain presuppositions on the nature and status of moral judgements. To be sure, this would not imply that engineers and technology users become ethical experts, but it demands the awareness that the ethical impact assessment is not an "objective", neutral, operation, but it is value-laden and it critically depends on the ethical perspective chosen by those who will carry out it.

To overcome this difficulty, the "principled approach" recognises that it is difficult to try to make decisions based only on *one* ethical theory, and it therefore translates different theories into a series of conditional principles. The need to be pragmatic can be satisfied by considering that a wide range of values may all legitimately contribute to an ethical decision, without having to be grounded in one overall principle or theory. Moral principles then need to be *applied* to situations created by technologies. Among the key challenges of assessment of technology approaches is a need to address the question on how a norm should be applied to a particular context.

Principles however cannot be said to exhaust every legitimate ethical concern. This is for various reasons, First because "principalism" is value-laden and could be (and has actually been) contested[199]. Second because technological innovations themselves test the limits of conventional ethics. Morality, like society and technology, is constantly evolving, both being influenced by and influencing other expectations. Taking this considerations into account, one would say that innovation in technology requires innovation in our moral reasoning as well.

What is an "ethical issue" changes over time and in different contexts. The fundamental rights and liberties which represent the institutional architecture of the European Union (i.e. the articles of the Lisbon Treaty and Charter of Fundamental Rights) are nowadays representing the basis upon which the ethical assessment of emerging technologies is currently carried out at the EU level. Technologies themselves (i.e. the *object* of ethical evaluation) however have the potential to modify our perceptions of what the ethical issues may look like. As argued in section 5.2, robust theoretical analysis on this still has to be developed.

Due to the *uncertainty* and *complexity* derived from the assessment of emerging technologies, fixing the key ethical principles in a framework should probably be conceived as an on-going activity, a perennial work in progress, an unfinished task rather than a stable framework given once and for all. As more information about a prospective technology comes to light, an ethical review may need to be revisited.

In addition, no proper assessment is possible if not all the cards are on the table, if stakeholders are not provided with all relevant details. In every ethical reflection, availability of good information is mandatory. This also implies a continuous, reflective, exchange of experiences and ideas between technologists and ethical experts, who should learn to work together from the initiation of the design phase.

[198] Brey, *op. cit*, 2010

[199] For instance one of the main criticisms raised against principalism is that it risks to become a sort of "minimalistic ethics", which defends only trivial and obvious principles in order to find a societal consensus.

Ethics, we argue, is not per se conservative, because the normative basis of a society is no immutable and rigid boundary condition, which decides on the acceptability or desirability of a new technology, but can itself be called in question by new technologies and be opened for further development. The ethics of technology doesn't just apply current normativity to a technology, but reflects the relationship of existing (reconstructed) normativity to new technical opportunities. Ethical reflection in technology assessment is explorative, constructing and experimental.

Finally, one has to consider that an *ethical norm* does not necessarily need to result from a *consensus* or compromise process. The nature of post-modern society, with a coexistence of pluralistic and relativistic views, may also preclude any occasion for ethical consensus. Since we cannot assume that we all agree and share the same values, how can a principle be identified and adequately applied?

In relation to this, more attention needs to be paid into the problematic tension between the values of stakeholders and supposedly universal moral values supported by experts. On one hand, going back to experts' normative expectations in order to guarantee that the values to be integrated are *ethical* values, somehow closes down a process which needs to be *participatory*. When considering the development and deployment of new technologies that are bound to impact on citizens, we must encourage more participatory decision processes. It is not useful to create an unnecessary division between experts on ethics and other stakeholders. However, on the other hand, it must be clear that societal consensus is not per se an ethical criterion and should not substitute for ethical reasoning and ethical desirability, as history has sadly demonstrated on quite a number of occasions. At the end of the day, a value is worth being protected only because of its inner reason, as the result of self-standing and contained argumentation.

Recently proposed suggestions[200] on an agenda for an improved Philosophy of Technology that takes into consideration ethical aspects include

(a) the need to develop more and better theories of values in the field, and on ways to distinguish/compare these values (i.e. above all the *ethical* from the *non-ethical* ones);

(b) the need for more and better theories of the relations between technologies and the individual or aspects of society;

(c) with particular regard to technology ethics, the need to develop (c1) more and better theories of the moral agency of artefacts (i.e. how they embody moral values and norms)[201], (c2) more and better theories of technologically mediated agency by humans, (c3) theories and methods of ethical technology assessment (i.e. to study and evaluate the ethical consequences of new technologies), and (c4) better methods for the ethical analysis and guidance of social and political debates, and on how to involve relevant stakeholders.

According to Brey[202], a *theory* of assessing ethical impacts of emerging technology (point c3 above) should interpret and criticise the role of technology in altering a *determined* (determined how? according to a determined ethical theory? politically negotiated?) set of *contemporary* (the question still remain on how to proactively identify *potential* future issues) ethical values. A theory of this sort requires the development of four questions:

- theoretical (how does technology play a role in the establishment of ethical principles?),
- factual (what is the actual role of technology?),
- normative (what role should technology play),
- practical (what steps can be taken to move closer to the normative ideal?).

Some key open questions are offered below for consideration in the scope of integrating ethics into current technology assessment methodologies and procedures:

[200] See Brey, op. cit., 2010
[201] See also STS contributions
[202] See Brey, op. cit., 2010

a) The **complexity and uncertainty of issues** that ethics seeks to address pose a challenge to come up with a single, all-inclusive, but widely acceptable, theory on ethical decision making vis-a-vis technological innovation. Where does the ethical dimension of technology come from? Under which conditions is an ethical assessment of emerging ICTs possible? How should we agree on what constitutes an ethical issue in relation to ICTs?

b) Ethics is an **unfinished activity**. The development of new technologies should be subject to an on-going ethical impact assessment. The ethical implications of a new technology may not be full appreciated at the outset. Indeed, they may not become apparent until after a technology is deployed. This is an ever-present risk.

c) **Difficulties in applying the principles:** Can guidance be given for dealing with ethical issues in an effective way? Taking into account uncertainty and complexity related considerations, under which circumstances should the project manager (representing those who propose to develop a new technology) be held morally accountable for the consequences of that development?

d) **Stakeholders** should be told when they are facing an ethical issue. Careful consideration needs to be given to which categories represent relevant stakeholders in an ethically critical situation.

6. PRESCIENT Privacy and Ethical Impact Assessment Framework

David Wright (Trilateral Research & Consulting)

This section presents the PRESCIENT Privacy and Ethical Impact Assessment Framework. The new framework is based on an integration of the results of research carried out throughout the project's lifecycle as discussed in the previous sections, and on current available privacy impact assessment guidelines such as those of the UK.

New technologies, projects, products, services, policies and programmes may raise not only privacy issues but also other social and ethical issues. Heretofore, PIAs have focussed on privacy, preferably all types of privacy, but still, only privacy. However, as mentioned above, some social and/or ethical issues could also be considered as part of a PIA (an "extended" PIA) or in the content of an ethical impact assessment.[203] Among such issues are those relating to, for example, autonomy, dignity, informed consent, trust, asymmetries of power, fairness, equity and so on.[204] Most of the steps in an ethical and/or social impact assessment would be the same as those outlined above. The *process* would be the same, even if there are somewhat different issues to consider and a wider range of stakeholders (e.g., ethicists, sociologists) to engage.

Like a PIA, an ethical and/or social impact assessment would be used as a way to ensure ethical and/or social implications are adequately examined by stakeholders before deployment of a new technology or project so that mitigating measures can be taken as necessary. Rather than conducting an ethical or social impact assessment before or after a PIA, an organisation could conduct a privacy and ethical impact assessment in one process, in what could be called an extended privacy impact assessment or a P+EIA. To be clear about our terminological use of ethical impact assessment, we mean an assessment that considers the ethical issues or impacts posed by a new project, technology, service, programme, legislation or other initiative, that engages stakeholders and that seeks to identify risks and solutions in consultation with those stakeholders.

6.1 A guide to Privacy and Ethical Impact Assessment

This section includes a synthesis of the key document developed in the scope of the PIAF project: A step-by-step guide to privacy impact assessment, including a threshold assessment, to determine whether a PIA is necessary, and a template for a PIA report.

The European Commission's proposed new Data Protection Regulation would make data protection impact assessments (otherwise known as privacy impact assessments, PIAs) mandatory "where processing operations present specific risks to the rights and freedoms of data subjects"[205].

In view of the hundreds of thousands of companies and government departments that process personal data across Europe, Article 33 of the proposed Regulation could have far-reaching consequences – in the costs and benefits of conducting a PIA.

Europe has the opportunity to construct a state-of-the-art PIA methodology in advance of the adoption of the new Regulation. Europe can select features from the PIA methodologies used in Australia, Canada, Ireland, New Zealand, the UK and US, the countries with the most experience in PIA. The EC-funded project, called PIAF (in which two of the PRESCIENT partners were also partners), reviewed these various

[203] Raab, Charles, and David Wright, "Surveillance: Extending the limits of privacy impact assessment", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

[204] The project results presented in this section have already been published as: Wright, David, "A framework for the ethical impact assessment of information technology", *Ethics and Information Technology*, Vol. 13, No. 3, September 2011, pp. 199-226.

[205] For an in depth discussion on the provisions on PIAs in the EU legal framework see chapter 4 of the present deliverable.

methodologies and has proposed an "optimised" PIA for Europe (and elsewhere) based on the best practices of the aforementioned countries. This chapter identifies 16 steps, which are summarised below, in a P+EIA process based on the best practices and adapted from that recommended by PIAF. It also argues that Europe should adopt a broader approach to privacy than simply data protection as provided in the proposed Regulation. PRESCIENT identified seven types of privacy; consequently, a "full-blooded" P+EIA should address all seven types.[206] Furthermore, as many new technologies, products, services, policies and programmes also raise ethical and social issues, an "extended" PIA methodology should also address those issues. While some organisations may regard a PIA (or an "extended" PIA dealing with ethical and social issues as well) as a hassle, in fact, a P+EIA offers many benefits, as also discussed below.

This chapter proposes a privacy and ethical impact assessment methodology, which takes into account the seven types of privacy and which is sufficiently flexible to take ethical issues and principles into account. The paper outlines the key elements and structure of such a methodology.

6.1.1 Different PIA methodologies

Europe can look to other countries for help in answering such questions, which is to say that several other countries have been using PIAs, in some instances, for more than a decade. The countries with the most experience are Australia, Canada, Ireland, New Zealand, the UK and the US. The following paragraphs offer a thumbnail sketch of the principal PIA policies and methodologies.[207] While there are differences in the methodologies, all of them are concerned with identifying risks to privacy and ways of overcoming those risks. Elsewhere, the author has made a comparative assessment of the various PIA policies and practices using a set of 18 criteria derived from the PIA literature, notably papers prepared by PIA pioneers such as Roger Clarke, Blair Stewart, David Flaherty, Nigel Waters and Elizabeth Longworth.[208] The 18 assessment criteria include the following:

1. Is PIA regarded as a process?
2. Does the PIA guide contain a set of questions to uncover privacy risks?
3. Does the PIA guide target companies as well as government?
4. Does the PIA address all types of privacy (informational, bodily, territorial, locational, communications)?
5. Is PIA regarded as a form of risk management?
6. Does the PIA guide identify privacy risks?
7. Does the PIA guide identify possible strategies for mitigating those risks?
8. Does the PIA guide identify benefits of undertaking a PIA?
9. Does the PIA guide support consultation with external stakeholders?
10. Does the PIA guide encourage publication of the PIA report?
11. Does the PIA guide provide a privacy threshold assessment to determine whether a PIA is necessary?
12. Does the PIA guide provide a suggested structure for the PIA report?
13. Does it advocate undertaking a PIA for proposed legislation and/or policy?

[206] European regulatory authorities are generally referred to as data protection authorities while in the US, Canada, Australia, New Zealand and many other countries, they are generally referred to as privacy commissioners. Despite the differences in terminology, both tend to focus only on the protection of personal data or personally identifiable information. With some exceptions, most pay little attention to other types of privacy, as described in this paper.

[207] More detailed information on these countries can be found in Wright, David, et al., PIAF Deliverable D1, September 2011 (www.piafproject.eu) and Wright, David, and Paul De Hert, "Introduction to Privacy Impact Assessment", Chapter 1, in David Wright and Paul De Hert, *Privacy Impact Assessment*, Springer, Dordrecht, 2012, which contains a systematic comparison of different PIA methodologies.

[208] Wright, David, Rachel Finn and Rowena Rodrigues, "A comparative analysis of privacy impact assessment in six countries", *Journal of Contemporary European Research*, Vol. 9, No1, 2013.

14. Does the guide say that PIAs should be reviewed and updated throughout the life of a project?
15. Does the guide explicitly say that PIA is more than a compliance check?
16. Does the PIA policy provide for third-party, independent review or audit of the completed PIA report?
17. Is PIA mandated by law, government policy or must a PIA accompany budget submissions?
18. Do PIA reports have to be signed off by senior management (to foster accountability)?

In Australia, the Office of the Privacy Commissioner (OPC) published its *Privacy Impact Assessment Guide* in August 2006, and a revised version in May 2010.[209] The *Guide* is addressed to government agencies, the private sector and the not-for-profit sector (i.e., civil society organisations). However, there is no legislative requirement in Australia to conduct a PIA. The *Guide* does not impose a particular PIA style ("There is no one-size-fits-all PIA model.") but suggests a flexible approach depending on the nature of the project and the information collected. The *PIA Guide* says that "Consultation with key stakeholders is basic to the PIA process." The Privacy Commission encourages organisations, "where appropriate", to make the PIA findings available to the public.[210] The *Guide* says publication "adds value; demonstrates to stakeholders and the community that the project has undergone critical privacy analysis; contributes to the transparency of the project's development and intent".

In Australia's Victoria state, the Office of the Victorian Privacy Commissioner (OVPC) has produced "one of the three most useful guidance documents available in any jurisdiction, anywhere in the world".[211] The current OVPC *PIA Guide* dates from April 2009.[212] It is the second edition of the guide originally published in August 2004. The OVPC *PIA Guide* is primarily aimed at the Victorian public sector, but it says it may assist anyone undertaking a PIA. The *Guide* says that public consultation as part of the PIA process not only allows for independent scrutiny, but also generates confidence amongst the public that their privacy has been considered. Public consultation may generate new options or ideas for dealing with a policy problem. If wide public consultation is not an option, the *Guide* says the organisation could consult key stakeholders who represent the project's client base or the wider public interest or who have expertise in privacy, human rights and civil liberties.

In Canada, the Treasury Board Secretariat (TBS) issued PIA Guidelines in August 2002.[213] It promulgated a new Directive on Privacy Impact Assessment in April 2010.[214] The directive ties PIAs with submissions to the Treasury Board for program approval and funding. This is one of the strongest features of Canadian PIA policy. PIAs have to be signed off by senior officials, which is good for ensuring accountability, before a submission is made to the Treasury Board. The PIA is to be "simultaneously" provided to the Office of the Privacy Commissioner. Institutions are instructed to make parts of the PIA publicly available. Exceptions to public release are permitted for security as well as "any other confidentiality or legal consideration".

[209] Office of the Privacy Commissioner, Privacy Impact Assessment Guide, Sydney, NSW, August 2006, revised May 2010.

[210] The Privacy Commissioner acknowledges (Office of the Victorian Privacy Commissioner, 2009, p. xviii) that there may be circumstances where the full or part release of a PIA may not be appropriate. For example, the project may still be in its very early stages. There may also be security, commercial-in-confidence or, for private sector organisations, other competitive reasons for not making a PIA public in full or in part. However, transparency and accountability are key issues for good privacy practice and outcomes, so where there are difficulties making the full PIA available, the Commissioner encourages organisations to consider the release of a summary version.

[211] Clarke, Roger, "PIAs in Australia: A work-in-progress report", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

[212] Office of the Victorian Privacy Commissioner (OVPC), Privacy Impact Assessments – A guide for the Victorian Public Sector, Edition 2, Melbourne, April 2009.

[213] Treasury Board of Canada Secretariat, Privacy Impact Assessment Guidelines: A framework to Manage Privacy Risks, Ottawa, 31 August 2002.

[214] Treasury Board of Canada Secretariat, Directive on Privacy Impact Assessment, Ottawa, 1 Apr 2010.

In December 2010, Ontario's Office of the Information and Privacy Commissioner released a revised PIA guide, replacing the 2001 version. Three PIA tools were also released at that time and provide detailed instructions, checklists, templates and other resources to help projects complete the PIA process. The *Privacy Impact Assessment Guide* for the Ontario Public Service says ultimate accountability for privacy protection rests with the Minister, as head of each government institution.[215] The Ontario Guide states that "The potential damage to the individual must take precedence in your assessment over organizational risks".[216]

In 2001, the Office of the Information and Privacy Commissioner (OIPC) of Alberta introduced its first Privacy Impact Assessment (PIA) questionnaire. In January 2009, the OIPC revised the PIA template and guidelines.[217] Not only are PIAs mandatory for health care projects, they must be submitted to the OIPC before implementation of a new system or practice. If the OIPC finds shortcomings, projects can be turned down or forced to make costly retrofits.

The Health Information and Quality Authority in Ireland is an independent authority, established under the Health Act 2007, to drive improvement in Ireland's health and social care services. Among other things, it aims to ensure that service users' interests are protected, including their right to privacy, confidentiality and security of their personal health information. In this context, the Authority produced a PIA Guidance in December 2010[218] following its review of PIA practice in other jurisdictions[219], which found a growing convergence in what constitutes best practice in relation to PIAs. The Guidance says the primary purpose in undertaking a privacy impact assessment is to protect the rights of service users. Where potential privacy risks are identified, a search is undertaken, in consultation with stakeholders, for ways to avoid or mitigate these risks. The Health Information and Quality Authority favours publication of PIA reports as it builds a culture of accountability and transparency and inspires public confidence in the service provider's handling of personal health information. Completed PIA reports are to be presented in a reader-friendly format.

The origins of privacy impact assessment in New Zealand date back to at least 1993, to the legislative requirement under section 98 of the Privacy Act 1993 to undertake Information Matching Privacy Impact Assessments (IMPIAs).[220] The Office of the Privacy Commissioner (OPC) published a PIA Handbook in October 2002 (reprinted in 2007).[221] It recommends that PIA reports be made publicly available, either in full or summary on an organisation's website. The Handbook mentions consultation with stakeholders but does not outline the consultative process. The agency conducting the PIA may consult the Privacy Commissioner. PIAs are generally not mandatory in New Zealand, however, section 32 of the Immigration Act 2009 explicitly requires PIA be conducted if biometric data are processed.

The Information Commissioner's Office (ICO) in the United Kingdom published a PIA handbook in December 2007 and became the first country in Europe to do so. The ICO published a revised version in June 2009.[222] The Cabinet Office, in its Data Handling Review, called for all central government departments to "introduce Privacy Impact Assessments, which ensure that privacy issues are factored into

[215] Office of the Chief Information and Privacy Officer (OCIPO), Privacy Impact Assessment Guide for the Ontario Public Service, Queen's Printer for Ontario, December 2010.

[216] Ibid., p. 48.

[217] O*ffi*ce of the Information and Privacy Commissioner (OIPC) of Alberta, Privacy Impact Assessment (PIA) Requirements, For use with the Health Information Act, January 2009.

[218] Health Information and Quality Authority, Guidance on Privacy Impact Assessment in Health and Social Care, Dublin, December 2010.

[219] Health Information and Quality Authority, International Review of Privacy Impact Assessments, 2010.

[220] Office of the Privacy Commissioner, Guidance Note for Departments Seeking Legislative Provision for Information Matching, 16 May 2008, Appendix B.

[221] Office of the Privacy Commissioner, Privacy Impact Assessment Handbook, Auckland/Wellington, 2007.

[222] Information Commissioner's Office (ICO), Privacy Impact Assessment Handbook, Wilmslow, Cheshire, UK, Version 2.0, June 2009.

plans from the start".[223] It stressed that PIAs will be used and monitored in all departments. PIAs have thus become a "mandatory minimum measure".[224] The Handbook places responsibility for managing a PIA at the senior executive level (preferably someone with responsibility for risk management, audit or compliance). The ICO emphasises identification of and consultation with stakeholders in its Handbook.

In the United States, privacy impact assessments for government agencies are mandated under the E-Government Act of 2002. This Act states that PIAs must be conducted for new or substantially changed programmes which use personally identifiable information. Section 208 of the Act requires that PIAs must be reviewed by a chief information officer or equivalent official, and should be made public, unless it is necessary to protect classified, sensitive or private information. Agencies are expected to provide their Director with a copy of the PIA for each system for which funding is requested. Each agency Director must issue guidance to their agency specifying the contents required of a PIA.[225]

Additionally, the creation of the Department of Homeland Security (DHS) via the Homeland Security Act of 2002 mandates that the DHS conduct privacy impact assessments and creates a Chief Information Officer position with responsibility for these privacy assessments.

On 26 Sept 2003, the Office of Management and Budget (OMB) issued a Memorandum to heads of Executive departments and agencies providing guidance for implementing the privacy provisions of the E-Government Act.[226] The OMB specifies what must be in a PIA and, in doing so, puts an implicit emphasis on the end product, the report, rather than on the process of conducting a PIA.

The review of the above PIA methodologies reveals important differences in approach. Some address only data protection, while others address the four types of privacy identified by Clarke (see section 2.2 above). Some favour or oblige publication of the PIA report, while others are silent on that prospect. Some favour consultation with external stakeholders, while for others that is not an issue. Some encourage or oblige third-party review or audit, most do not. Some are explicit in making senior officials responsible for the adequacy of a PIA, others are not. Much can be (and has been) learned from a review of these different methodologies in designing a more optimised approach to P+EIA, as discussed further below. The Irish and UK PIA handbooks both are based on extensive reviews of other PIA methodologies. Hence, we can see a distinct evolution in enhancing the PIA process, which is also reflected (albeit briefly) in Article 33 of the proposed Data Protection Regulation.

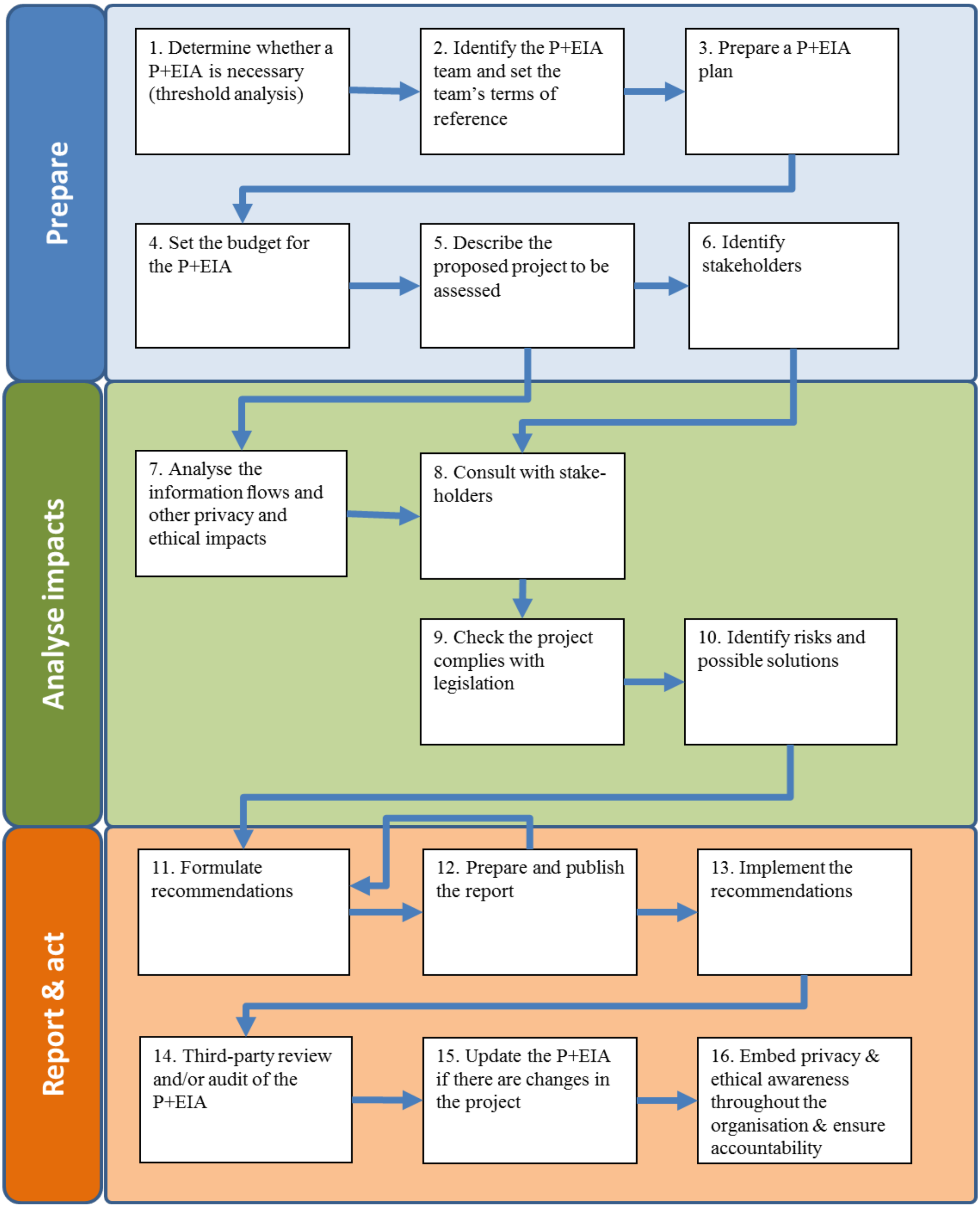
In our discussions with industry and government representatives in the past year or so, it seems that most prospective users prefer a streamlined, short, easy-to-understand and easy-to-use P+EIA methodology which is what we have produced below, taking into account the six-page "Step-by-step guide to privacy impact assessment".[227]

6.1.3 P+EIA methodology for Europe

We envisage a P+EIA process comprising 16 principal steps, as set out below (and as depicted in the figure below). Depending on the perceived privacy and/or ethical risks, it may not be necessary for an organisation to follow all of these steps and some may follow them in variations of the sequence set out here. However, we regard the steps below as generally necessary if a P+EIA is to have "teeth", if it is to be effective in identifying and minimising or avoiding privacy and ethical risks. "Generally" is the operative word. If the privacy or ethical risk is regarded as relatively trivial, affecting only a few people, it may not be necessary to follow all of the steps set out below (e.g., it may not be necessary to consult external

[223] Cabinet Office, Data Handling Procedures in Government: Final Report, June 2008, p. 18.
[224] Cabinet Office, Cross Government Actions: Mandatory Minimum Measures, 2008.
[225] E-government Act of 2002, Pub.L.107-347.
[226] Office of Management and Budget, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Washington, DC, 26 Sept 2003. http://www.whitehouse.gov/omb/memoranda/m03-22.html
[227] http://www.piafproject.eu/Events.html

stakeholders or even to publish the P+EIA report). At the end of each step, we identify which countries promote such steps. The P+EIA *process* should always be distinguished from a P+EIA *report*. Production of a report is only part of the process, which continues even after the assessor has finished writing the report. Although the 16 steps below are those recommended in the PIAF project, we have adapted them here to take into account any ethical and/or societal impacts raised by a project, emerging technology, new service, programme, legislation or whatever (hence, in the steps below we refer to a P+EIA, privacy and ethical impact assessment).


Prepare
1. Determine whether a P+EIA is necessary (threshold analysis)
2. Identify the P+EIA team and set the team's terms of reference
3. Prepare a P+EIA plan
4. Set the budget for the P+EIA
5. Describe the proposed project to be assessed
6. Identify stakeholders
Analyse impacts
7. Analyse the information flows and other privacy and ethical impacts
8. Consult with stake-holders
9. Check the project complies with legislation
10. Identify risks and possible solutions
Report & act
11. Formulate recommendations
12. Prepare and publish the report
13. Implement the recommendations
14. Third-party review and/or audit of the P+EIA
15. Update the P+EIA if there are changes in the project
16. Embed privacy & ethical awareness throughout the organisation & ensure accountability

1. *Determine whether a PIA or EIA is necessary (threshold analysis)*

Generally, if the development and deployment of a new project (or technology, service…) impacts upon privacy, the project manager should undertake a PIA. The same can be said of a project which raises ethical issues. A P+EIA should be undertaken when it is still possible to influence the design of a project or, if the project is too intrusive upon privacy or raises serious ethical issues or has a negative societal impact, the organisation may need to decide to cancel the project altogether rather than suffer from the negative reaction of consumers, citizens, regulatory authorities, the media and/or advocacy gadflies. Australia, Victoria state, Canada, Ontario, Alberta, Ireland and the US (DHS) use threshold analyses (typically a small set of questions) to determine whether a PIA should be conducted. The UK uses a threshold analysis to determine whether a "full-scale" or "small-scale" PIA should be conducted.

2. *Identify the P+EIA team and set the team's terms of reference, resources and time frame*

The project manager should be responsible for the conduct of a P+EIA, but she may need some additional expertise, perhaps from outside her organisation. For example, the project manager may decide that an ethicist or someone well-grounded in ethics should be part of the P+EIA team. The project manager and/or the organisation's senior management should decide on the terms of reference for the P+EIA team, its nominal budget and its time frame. The terms of reference should spell out whether public consultations are to be held, to whom the P+EIA report is to be submitted, the budget for the assessment, the time frame, whether the P+EIA report is to be published. The UK especially recommends this step. The minimum requirements for a P+EIA will depend on how significant an organisation deems the privacy, ethical or societal risks to be. That an organisation may well downplay the seriousness of the risks makes third-party review and/or audit (see step 14) necessary.

3. *Prepare a P+EIA plan*

The plan should spell out what is to be done to complete the P+EIA, who on the P+EIA team will do what, the P+EIA schedule and, especially, how the consultation will be carried out. It should specify why it is important to consult stakeholders in this specific instance, who will be consulted and how they will be consulted (e.g., via public opinion survey, workshops, focus groups, public hearings, online experience…). Australia and the UK explicitly advocate preparation of plans for a PIA. Some countries, including Australia and the UK, say there is no "one size fits all" for PIA reports, while others, such as Alberta and Ireland, provide templates for such reports. If the regulator does not specify a P+EIA template, the author would encourage organisations to follow the P+EIA process advocated here.

4. *Agree the budget for the P+EIA*

Once the project manager and/or assessor have prepared a P+EIA plan, they can estimate the costs of undertaking the P+EIA and seek the budgetary and human resources necessary from the organisation's senior management. Their plan may require an increase in the nominal budget initially set by senior management or the assessor may need to revise her P+EIA plan based on the budget available. If the assessor is unable to do an adequate P+EIA, she should note this in her P+EIA report.

5. *Describe the proposed project to be assessed*

The description can be used in at least two ways – it can be included in the P+EIA report and it can be used as a briefing paper for consulting stakeholders. The description of the project should provide some contextual information (why the project is being undertaken, who comprises the target market, how it might impact the consumer-citizen's privacy, what personal information will be collected, what ethical issues it might raise, what societal impacts it might have). The project description should state who is responsible for the project. It should indicate important milestones and, especially, when decisions are to be taken that could affect the project's design. All existing PIA methodologies include this step.

6. *Identify stakeholders*

The assessor should identify stakeholders, i.e., those who are or might be interested in or affected by the project, technology or service. The stakeholders could include people who are internal as well as external to the organisation. They could include regulatory authorities, customers, citizen advocacy organisations, suppliers, service providers, manufacturers, system integrators, designers, academics and so on. The assessor should identify these different categories and then identify specific individuals from within each of the category, preferably to be as representative as possible. The range and number of stakeholders to be consulted should be a function of the privacy, ethical and societal risks and the assumptions about the frequency and consequences of those risks and the numbers of consumer-citizens who could be impacted. Australia, Victoria state, Ireland and the UK take this step.

7. *Analyse the information flows and other privacy and ethical impacts*

The assessor should consult with others in the organisation and perhaps external to the organisation to describe the information flows and, specifically, who will collect what information from whom for what purpose; how will the organisation use the collected information; how will the information be stored, secured, processed and distributed (i.e., to whom might the organisation pass on the information), for what purpose and how well will secondary users (e.g., the organisation's service providers, apps developers) protect that information or will they pass it on to still others? This analysis should be as detailed as possible to help identify potential privacy risks. The assessor should consider the impacts not only on information privacy, but other types of privacy as well (see below) and, in the instance of ethical impact assessment or societal impact assessment, what ethical issues the project might raise or what impacts the project might have.[228] Australia, Victoria state, Canada, Ontario, Alberta, Ireland and New Zealand say that a PIA should describe information flows. This step could be taken immediately after step 5 and concurrently with step 6.

8. *Consult with stakeholders*

There are many reasons for doing so, not least of which is that they may identify some privacy or ethical or societal risks not considered by the project manager or assessor. By consulting stakeholders, the project manager may forestall or avoid criticism that they were not consulted. If something does go wrong downstream – when the project or technology or service is deployed – an adequate consultation at an early stage may help the organisation avoid or minimise liability. Furthermore, consulting stakeholders may provide a sort of "beta test" of the project or service or technology. Consulted stakeholders are less likely to criticise a project than those who were not consulted. Australia, Victoria state, Ireland and the UK urge consultation with stakeholders. This step could be taken after step 5, but it would be better after step 7, since the latter may uncover additional privacy, ethical or societal risks not apparent after only step 5.

[228] In the guidance documents associated with its calls for security research proposals issued in July 2012, the European Commission included a new annex 7 to the guidance document aimed at helping applicants to identify societal impacts. The annex contains 10 questions, such as the following: 3. What threats to society does the research address? (e.g. crime, terrorism, pandemic, natural and man-made disasters, etc.). 7. Are there other European societal values that are enhanced by the proposed research e.g. public accountability & transparency; strengthened community engagement, human dignity; good governance; social and territorial cohesion; sustainable development etc. 8. If implemented, how could the research have a negative impact on the rights and values enshrined in the Treaties (e.g. freedom of association, freedom of expression, protection of personal dignity, privacy and data protection etc.)?

9. Check the project complies with legislation

A privacy and ethical impact assessment is more than a compliance check, nevertheless, the assessor or her legal experts should ensure that the project complies with any legislative or regulatory requirements or relevant codes of conduct. Australia, Victoria state, Canada, Ireland, New Zealand, the UK and the US note the importance of this step.

10. Identify risks and possible solutions

The assessor and her P+EIA team, preferably through stakeholder consultation, should identify all possible risks, who those risks will impact and assess those risks for their likelihood (frequency) and consequence (magnitude of impact) as well as the numbers of people who could be affected. Assessing risks is a somewhat subjective exercise. Thus, the assessor will benefit from engaging stakeholder representatives and experts to have their views. Deciding how to mitigate or eliminate or avoid or transfer the risk is also a somewhat political decision as is the decision regarding which risks to retain. Information security risks, such as those contained in ISO 27005[229], do not address specific privacy risks. Hence, some PIA methodologies, e.g., those of Australia, Victoria state, Canada Alberta, Ontario and New Zealand, mention specific privacy risks. Recently, the French data protection authority published two booklets on privacy risk management.[230]

11. Formulate recommendations

The assessor should be clear to whom her recommendations are directed – some could be directed towards different units within the organisation, some to the project manager, some to the CEO, some to employees or employee representatives (e.g., trade unions), to regulatory authorities, third-party apps developers, etc. If stakeholders have sight of draft recommendations, before they are finalised, they may be able to suggest improvements to existing recommendations or make additional ones. All PIA methodologies call for recommendations.

12. Prepare and publish the report, e.g., on the organisation's website

Some organisations may be afraid to publish their P+EIAs because they fear negative publicity or they have concerns about competitors learning something they don't want them to. Such concerns seem overwrought. There are solutions. The organisation can simply redact the sensitive bits or put them into a confidential annex. In cases where the report raises genuine issues of commercial confidentiality or national security (as distinct from a report which might embarrass the organisation or expose it for doing something it should not be doing, e.g., selling personal data indiscriminately), keeping the report confidential may be justified.[231] As in Step 11, if the assessor gives stakeholders sight of the draft P+EIA report, they may be able to suggest improvements before it is finalised. Australia and Ireland encourage publication, the US requires it. Canada publishes summaries.

13. Implement the recommendations

The project manager and/or the organisation may not accept all of the P+EIA recommendations, but they should say which recommendations they are implementing and why they may not implement others. The organisation's response to the assessor's recommendations should be posted on the organisation's

[229] http://www.iso.org/iso/catalogue_detail?csnumber=56742

[230] Commission National de l'Informatique et des Libertés (CNIL), Gérer les risques sur les libertés et la vie privée, la method [*Methodology for privacy risk management*], Paris, June 2012 [31 p.]. The English translation was published in November 2012. The second booklet is entitled *Measures for the privacy risk treatment* [92 p.].

[231] However, stakeholders external to the organisation should still be engaged in the P+EIA process. They could participate on the basis of a non-disclosure agreement. Similarly, even if the report is kept confidential, it should still be subject to independent third-party review or audit to verify the legitimacy of the report.

website. This transparency will show that the organisation treats the P+EIA recommendations seriously, which in turn should show consumers and citizens that the organisation merits their trust. Canada, Ireland, New Zealand and the UK say a PIA report should justify any remaining risks. Victoria state says an organisation will need to consider how residual risks will be managed.

14. Third-party review and/or audit of the P+EIA

Existing PIA reports are of highly variable quality, from the thoughtful and considered to the downright laughable. Some PIA reports exceed 150 pages, others are only a page and a half in length, the sheer brevity of which makes them highly suspect. Independent, third-party review and/or audits are the only way to ensure P+EIAs are properly carried out and their recommendations implemented. The Office of the Privacy Commissioner of Canada has indicated and extolled the benefits of independent audits.[232] Data protection authorities and/or national ethics committees do not have the resources to audit all P+EIAs, but they could audit a small percentage, enough to make organisations ensure their P+EIAs are reasonably rigorous. Alternatively, independent auditors could undertake this task, just as they audit a company's financial accounts. Yet another alternative would be for organisations such as the International Association of Privacy Professionals (IAPP) to certify privacy auditors. The Government Accountability Office (GAO) audits PIAs in the US. The DHS has built independent, third-party review into its PIA process. The Office of the Privacy Commissioner audits PIAs in Canada. New Zealand also favours third-party review. The UK envisages review and audit of a PIA, but doesn't say who should do it. The European Commission has made a provision for the audit of PIAs in Article 33 of its proposed Data Protection Regulation.

15. Update the P+EIA if there are changes in the project

Many projects undergo changes before completion. Depending on the magnitude of the changes, the assessor may need to revisit the P+EIA as if it were a new initiative, including a new consultation with stakeholders. Australia says a PIA may need to be revisited as a project progresses. So does Ontario, the UK and the US Office of Management and Budget (OMB).

16. Embed privacy and ethical awareness throughout the organisation and ensure accountability

The chief executive officer is responsible for ensuring that all employees are sensitive to ethical issues, the privacy implications, the possible impacts on privacy, of what they or their colleagues do. The CEO should be accountable to her supervisory board or shareholders for the adequacy of P+IA. In Canada, PIA reports have to be signed off by a senior official (e.g., a deputy minister). Ireland also says PIA reports should be approved by senior management. In the US, the chief information officer or privacy officer is expected to review and sign off PIAs. Some PIA methodologies (e.g., Canada) explicitly say that organisations should provide guidance and training to managers and staff. Embedding an awareness of good ethical practices and of sensitivity to ethical issues also seems to be worth undertaking by organisations who do not wish to see any harm or damage to their image and reputation.

6.1.4 Ethical and social issues to be considered in a P+EIA

The ethical issues raised by a new project, technology, service or other initiative need to be considered in each case and in each context. The ethical issues raised by one technology could well be different from those raised by another technology. Each case must be considered on its merits. Having said that, we can

[232] Stoddart, Jennifer, "Auditing Privacy Impact Assessments: The Canadian Experience", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

identify some ethical and/or social issues that often arise with the development of new technologies, services, etc. Among these are the following:

- *Autonomy* (being let alone) – Does the project or new technology subject the individual or groups to surveillance (listening, watching, tracking, detecting)?
- *Dignity* – Does the project or technology intrude upon the individual's dignity, as body scanning, fingerprinting or electronic tagging arguably do.
- *Profiling and social sorting* – Does the project, technology, application or service sort individuals into groups according to some predetermined profile? Are some groups advantaged or disadvantaged as a result of the sorting?[233]
- *Informed consent* – Have individuals freely given their explicit informed consent to being tracked or targeted?
- *Freedom of speech and association* – Does the technology "chill" freedom of speech and association (e.g., are "smart" CCTV cameras installed in public places able to eavesdrop on conversations)?
- *Trust* – Will the technology or project impact trust and/or social cohesion? Will groups or individuals believe they are not trusted by others, especially those who are in a stronger position of power?
- *Asymmetries of power* – Will the project or technology enhance the power of some at the expense of others?
- *Security* – Is a new technology or project being introduced to improve security (and whose security is actually being improved)? Will a perceived increase in security take precedence over other values such as privacy? How can we know if the claims of the security proponents are valid? Who determines if security should take precedence?
- *Unintended consequences* – Does the project or technology have some consequences other than the purpose for which it is being deployed?
- *Alternatives* – Are there alternatives to the project or technology which are less intrusive upon an individual's rights or the impacts on society?

The above issues are only indicative. Each project would need to be assessed for the ethical issues it may raise – and quite possibly not just assessed once, but perhaps several times, as the organisation, in consultation with stakeholders, may discover new ethical issues as the project progresses. The key features of an ethical and societal impact assessment or extended privacy impact assessment is the engagement of stakeholders to identify risks and find solutions, publication of the impact assessment report and third-party review of the report and its recommendations.

6.1.5 Benefits

An organisation might figuratively throw up its hands in despair in having to consider many different privacy, ethical and societal impact issues and in engaging stakeholders before launching a new technology or product or service or policy, especially if it is obliged to do so under the proposed new Data Protection Regulation in Europe (at least, in regard to privacy issues). Some might see the cost and time needed to conduct a P+EIA as reasons not to do a P+EIA or to do P+EIA in the most cursory fashion possible. Certainly, it is true that the cost and time needed will vary significantly depending on the complexity and seriousness of the privacy or ethical risks. However, the costs of fixing a project (using the term in its widest sense) at the planning stage will be a fraction of those incurred later on. If the privacy and ethical impacts are unacceptable, the project may even have to be cancelled altogether. Thus, a P+EIA can help

[233] As mentioned above, the European Commission has included a set of societal impact questions to be addressed by proposers of new projects in its guidance document, one of which is "9. If implemented, how could the research impact disproportionately upon specific groups or unduly discriminate against them?" See Annex 7 of European Commission, *Guide for applicants collaborative projects*, Annexes, specific to call: SEC-FP7-2013-1.

reduce costs in management time, legal expenses and potential media or public concern by considering privacy, ethical and societal impact issues early. It helps an organisation to avoid costly or embarrassing privacy mistakes or ethical pitfalls. It provides a way to detect potential privacy problems and/or ethical issues, take precautions and build tailored safeguards before, not after, the organisation makes heavy investments.

Although a P+EIA should be more than simply a check that the project complies with legislation, it does nevertheless enable an organisation to demonstrate its compliance with privacy and other relevant legislation in the context of a subsequent complaint, privacy audit or compliance investigation. In the event of an unavoidable privacy risk or breach, or other ethical complication, occurring, the P+EIA report can provide evidence that the organisation acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any liability, negative publicity and loss of reputation.

A P+EIA enhances informed decision-making and exposes internal communication gaps or hidden assumptions about the project. A P+EIA is a tool to undertake the systematic analysis of privacy issues arising from a project in order to inform decision-makers. A P+EIA can be a credible source of information. It enables an organisation to learn about the privacy pitfalls, ethical issues or societal impacts of a project directly, rather than having its critics or competitors point them out.

A P+EIA can help an organisation to gain the public's trust and confidence that privacy and ethical review have been built into the design of a project, technology or service and that the organisation has considered a range of ethical issues. Trust is built on transparency, and a P+EIA is a disciplined process that promotes open communications, common understanding and transparency. Customers or citizens are more likely to trust an organisation that performs a P+EIA than one that does not. They are more likely to take their business to an organisation they can trust than one they don't.

An organisation that undertakes a P+EIA demonstrates to its employees and contractors that it takes privacy and ethical issues seriously and expects them to do so too. A P+EIA is a way of educating employees about privacy and ethical issues and making them alert to problems that might damage the organisation. It is a way to affirm the organisation's values. An organisation may wish to use a P+EIA as a way to check out third-party suppliers, to verify that they will not create privacy or ethical problems. A proper P+EIA also demonstrates to an organisation's customers and/or citizens that it respects their privacy and is responsive to ethical concerns.

We assume regulators are likely to be more sympathetic towards organisations that undertake P+EIAs than those that do not. A P+EIA is a self- or co-regulatory instrument which may obviate the need for "hard" law. Thus, if organisations are seen to carry out proper (full-blooded) P+EIAs, they may escape the more onerous burdens imposed by legislation.

6.1.6 Conclusion

Organisations that carry out privacy impact assessments should be concerned not only about privacy of personal data and privacy of communications, but also the other types of privacy as well, and ethical issues if proposed project raises or might raise ethical issue. The integrated privacy and ethical impact assessment methodology described above provides organisations and their stakeholders, including the public, with a useful, logical, well-structured and coherent typology in which to frame their privacy and ethical studies.

6.2 Engaging stakeholders

Why engage stakeholders?

There are various reasons why project managers should engage stakeholders and undertake a consultation when developing new technologies or projects[234]. 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 which the project manager might not have considered and may have some good suggestions for resolving complex issues.[235] Also, technology development is often too complex to be fully understood by a single agent, as Sollie and others have pointed out.[236] 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."[237] 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."[238] 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.[239]

Types of stakeholders

In a privacy and ethical impact assessment, the project manager or assessor should aim to engage stakeholders, including those who are developing or intend to develop an information technology project, policy or programme that may have ethical implications. More specifically, this would include *industry* players when they are developing a new technology or planning a new service as well as *policy-makers* and *regulatory authorities* when they are considering a new policy or regulation. In addition, the ethical impact assessment framework should be of interest to *civil society organisations*, so that when they become aware of proposals or plans for new technologies, they can advocate the framework's use and their involvement in

[234] These PRESCIENT project results have already been published as Wright, David, "A framework for the ethical impact assessment of information technology", *Ethics and Information Technology*, Vol. 13, No. 3, September 2011, pp. 199-226.

[235] 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.

[236] 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]. Moor also supports better collaboration among ethicists, scientists, social scientists and technologists. Moor, James H., "Why we need better ethics for emerging technologies", *Ethics and Information Technology*, Vol. 7, No. 3, 2005, pp. 111-119 [p. 118].

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

[238] US National Research Council, Committee on Risk Perception and Communications, *Improving Risk Communication*, National Academy Press, Washington, D.C., 1989, p. 9.

[239] Stern and Fineberg, pp. 23-24.

the decision-making process. Other stakeholders, such as *academics*, may find the ethical impact assessment framework of interest too and, as a consequence, may be able to suggest improvements or to analyse its use. It might also be of interest to *the media* as background to any stories they prepare on the introduction of a new technology or service, which in turn will help raise the awareness of the public and other stakeholders about the associated ethical issues. Last, but not least, the assessor could make special efforts to engage *the public* in any consultation regarding a new or emerging technology, especially if it will impact the public in some way.

These broad categories can, of course, be made more fine-grained. For example, policy-makers could include representatives from different levels of governmental organisations such as the European Commission, inter-governmental organisations, such as UN and NATO, Member State governments or local governments. This category could include regulatory, legislative, administrative or public authorities. In addition to the European Commission, other EU institutions of possible relevance might include ENISA, EDPS, FRONTEX, EUROJUST, etc., as well MEPs and MPs at the European and Member State level.

To take another example, industry stakeholders could include manufacturers, suppliers, distributors, service providers, vendors, system integrators, industry associations and professionals.

Selection criteria

Nominally, an ethical impact assessment of a new or emerging technology should target stakeholders interested in or affected by the outcome. In the first instance, the policy-maker or technology developer or project manager should identify the stakeholders he or she thinks relevant, but in most cases he or she should be open to or even encourage other stakeholders to contribute to the assessment.[240] To ensure those participating in an ethical impact assessment are truly representative of the relevant stakeholder groups, the technology developer or policy maker may need to make some special efforts to engage the relevant stakeholders in order to avoid something akin to regulatory capture.

The project manager or assessor may need to apply some further selection criteria. A key criterion to be taken into account is the scale of the privacy and ethical impact assessment. If the impacts of a new or emerging technology are not expected to be that great, not expected to affect many people or are confined to a particular geographic area, then the project manager may choose to restrict her invitation to stakeholders to those she estimates to be most relevant. On the other hand, if a new or emerging technology or service is expected to impact virtually everyone across a society, then the project manager will need to scale up her consultation processes accordingly. Another determining factor (selection criterion) is the available budget for the consultation. The project manager may find her hands somewhat tied by her organisation's senior management because, for whatever reason, they may not want to give her as big a budget as she thinks is warranted by the impact of the technology. If such is the case, and the organisation is subsequently criticised by the media and others for not undertaking an adequate consultation, then the organisation's image, reputation and credibility may be damaged.

Methods of engaging stakeholders

This section identifies various ways in which the assessor or the decision-maker can engage stakeholders in considering the principles, values and issues raised by new or emerging technologies.

[240] Dekker says ethical reflection in technology assessment requires an engagement of experts from different disciplines for two reasons: "Firstly, the technical, economical, legal and social aspects are deeply cross-correlated with the ethical reflection. And secondly, participating in such interdisciplinary discussions enables an ethical reflection which keeps in touch with the real world." See Decker, Michael, "The role of ethics in interdisciplinary technology assessment", *Poiesis & Praxis*, Vol. 2, Nos. 2-3, April 2004, pp. 139-156.

Beekman et al. rightly argue that "It is unlikely that a single tool will suffice for a full assessment of the whole range of divergent ethical issues involved in the introduction and application of new technologies." Thus, they developed a toolbox, in which particular tools are more applicable for certain purposes and/or in certain contexts.[241]

In a separate paper, Beekman and Brom argue that if the issues at stake and technology have societal impacts, lay perspectives need to be taken into account. Instruments to facilitate broadening the debate need to be comprehensive, transparent and democratic tools that give all arguments fair and balanced consideration.[242]

Consultations and surveys

Consultations and surveys are frequently used by policy-makers to gather the views of stakeholders before implementing policies. Typically, in a consultation, the government will pose a set of questions posted on its website and invite comments from interested stakeholders. Stakeholders may have the opportunity not only to respond to the questions, but also to prepare papers in which they elaborate their views on the policy issue at stake. Consultations have the virtue that they are open and transparent. Anyone can respond to the questions and, if they wish, to send in a letter or paper. They are transparent too in that the government will publish the results of the consultation on their website, so that one can see who responded and how (although in some cases of commercial or competitive sensitivity, the stakeholder can request that its views not be published). The snag is that the response rate is usually quite low and confined to those who are aware of the consultation and have a vested interest (even if their vested interest is acting on behalf of civil society organisations and/or the public) in the outcome of the deliberation. Furthermore, the policy-maker cannot be assured that the outcome of the consultation genuinely represents a cross-section of the public.

Hence, policy-makers and the private sector sometimes resort to surveys that are intended to provide a reflection of the public's views of a particular issue (within plus or minus three per cent). The snag with surveys is that they do not necessarily reflect informed views and usually they do not provide an opportunity for a detailed or nuanced response. Survey questionnaires are designed to elicit responses that can be easily quantified statistically. Thus, the questions are relatively simple so that the response is either yes, no or don't know or multiple choice, in which case the choice is limited to those contained in the questionnaire.

While consultations and surveys are useful tools, they are dangerous if the policy-maker were to rely solely on them as inputs in making a policy decision. Additional tools are needed.

[241] Beekman, Volkert, et al., Ethical Bio-Technology Assessment Tools for Agriculture and Food Production, Final Report of the Ethical Bio-TA Tools project, LEI, The Hague, February 2006, p. 6. Although Rowe and Frewer do not focus specifically on ethical tools, nevertheless, they do provide a long list of different mechanisms for engaging stakeholders, including the public, some of which could be used to facilitate an ethical impact assessment. See Rowe, Gene, and Lynn J. Frewer, "A Typology of Public Engagement Mechanisms", *Science, Technology & Human Values*, Vol. 30, No. 2, 2005, pp. 251-290. Also of interest in this regard is Essays 9 & 10 in Chapter 8 in Renn, Ortwin, *Risk Governance: Coping with Uncertainty in a Complex World*, Earthscan, London, 2008, pp. 273-352. Renn says, "A combination of analytic and deliberative instruments (or stakeholders and the public) is instrumental in reducing complexity, necessary for handling uncertainty and mandatory for dealing with ambiguity. Uncertainty and ambiguity cannot be resolved by expertise only" (p. 350). The two essays are useful guidance for ethical impact assessment as well as risk governance.

[242] Beekman, Volkert, and Frans W.A. Brom, "Ethical tools to support systematic public deliberations about the ethical aspects of agricultural biotechnologies", *Journal of Agricultural and Environmental Ethics*, Vol. 20, No.1, Feb. 2007, pp. 3-12 [p. 6].

Expert workshops

The European Commission, European agencies (such as ENISA[243]) and many other organisations convene expert workshops or stakeholder panels, often to complement consultations and sometimes surveys. Ideally, such workshops bring together representatives from various stakeholder groups to discuss issues. The workshops often consist of a mixture of presentations by those representatives and discussions on one or two or, at least, a limited number of issues, which can be addressed in the course of a one or two-day meeting. Sometimes, just a single workshop is held, at other times, there may be more, say, three, over a period of six months or so. At still other times, the convened experts may agree to work collaboratively on a report in between the workshops. Usually, the workshops result in a report, which is posted on the host organisation's website. The success of the workshop depends very much on the chairperson of the workshop and how the meeting is structured and, to some extent, the chemistry that develops between the participants. Often the time for discussion is derailed by too many presentations. The principal benefit of an expert workshop is that it allows more in-depth, face-to-face discussion by a range of different stakeholders than, say, a consultation or a survey. If the experts convened for a workshop such as those convened by ENISA are tasked with preparing a report, there is another important advantage, which is that they produce a consensus report, i.e., there is an opportunity for stakeholders to learn from each other and to reach a shared view. The principal disadvantage is that, despite inviting representatives from different stakeholder groups, the host organisation may still not get a representative view of the ethical considerations of a cross-section of individual stakeholders (as distinct from stakeholder groups).

Delphi

A Delphi is an iterative process for exchanging views and arguments between experts. The method is structured around the notion of a virtual committee where the exchange of ideas is conducted anonymously and remotely through a series of opinion exchanges (in the form of "rounds"). The ethical Delphi is used to map the ethical considerations that experts believe are pertinent and significant. It indicates the extent of agreement as well as drawing out divergence in expert opinion on a given topic. The ethical Delphi can be used to characterise and map the ethical issues raised by the use of novel technologies. One of the benefits of the ethical Delphi is the combination of "scoring" and reasoned arguments where it is possible to see the importance of an issue (using a Likert scale) and the relevant arguments.

Consensus conferences

The participatory consensus conference was initially developed by the Danish Board of Technology and represents a further development from the original consensus conferences arranged by US Office of Technology Assessment (OTA). The aim of the OTA conferences was to expose expert views and to reach consensus among experts regarding a given topic. Consensus is still (in most cases) an aim, but instead of striving for consensus among experts, consensus is sought among laypersons. The reason given for the importance of involving laypersons in such conferences is typically to give citizens the opportunity to influence decisions having impact on their lives, to affect the public debate or to overcome limitations in expert knowledge. Laypersons should be entitled to choose the type of experts they want invited to and question at the consensus conference.

[243] ENISA is the acronym of the European Network and Information Security Agency. www.enisa.europa.eu.

Citizen panels

A variant on the consensus conference is the citizen panel. Skorupinski and Ott argue that "The model of consensus conferences needs further advancement, especially in regard to the questioning of experts. The rigid form of lay people questioning experts should be replaced by a more dialogic modus." In this respect, they say, the model of citizen panels seems to be superior to consensus conferences.[244] Citizen panels are groups of randomly selected citizens who are asked to compose a set of policy recommendations on a specific issue. The objective is to provide citizens with the opportunity to learn about the technical and political facets of a given issue and to enable them to discuss and evaluate these options and their likely consequences according to their own set of values and preferences. Citizens are informed about the potential options and the corresponding consequences before they are asked to evaluate these options. Citizen panels require a large investment of time and money and are not suitable for all types of problems and all contexts. If the problem is highly technical, it may be impossible to bring citizens up to the necessary level of understanding.

The search for consensus

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. The policy-maker or technology developer can use some or all of the ways mentioned in the preceding section to facilitate the process. 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.

Palm and Hansson caution that "the search for consensus in controversial issues should not be overemphasized since it may lead to the closure of issues at a too early stage. In ethical TA, conflicts and different opinions should be highlighted rather than evened out." They also urge that the assessment "should seek to identify all relevant stakeholders, i.e., a broad spectrum of agents and therefore also a broad spectrum of responsibilities". They see the task of an ethical assessment as being "to delineate and analyze the issues and point out the alternative approaches for the final analysis that are available".[245]

It would make life easier, undoubtedly, if the stakeholders reach a consensus about how to deal with the ethical considerations raised and if the decision-maker agreed with the consensus. In real life, that does not always happen, so the decision-maker will need to decide which considerations are given greatest weight and to explain why he or she took that decision. The decision-maker should make clear to stakeholders when he or she first reaches out to them what the rules of the game will be, how and by whom that ultimate decision will be made. When a decision-maker ends up disagreeing with the results of the consultation processes, this calls for explicit argument, as Beekman et al. point out. It does not follow that the decision-makers should always follow the results of a consultation. Consultation methods, such as those mentioned above, are not decision-making machines for ethics. However, when such a situation occurs, the decision-maker must state why he or she prefers a different conclusion.[246]

[244] Skorupinski, Barbara, and Konrad Ott, "Technology assessment and ethics", *Poiesis & Praxis*, Vol. 1, 2002, pp. 95-122 [p. 119].

[245] Palm and Hansson, op. cit., pp. 550-551.

[246] Beekman et al., p. 26.

7. References

Achterhuis, H., *American Philosophy of technology, The Empirical Turn*, Indiana university Press, Bloomington, , 2001.

Adam, Barbara, Ulrich Beck, Joost Van Loon, *The Risk Society and Beyond. Critical Issues for Social Theory*, SAGE publications Ltd, 2000

Akandji-Kombe, J.-F, *Les obligations positives en vertu de la Convention européenne des Droits de l'Homme. Un guide pour la mise en oeuvre de la Convention européenne des Droits de l''Homme*, Strasbourg: Council of Europe, 2006

Ambec, Stefan, Mark A. Cohen, Stewart Elgie, and, Paul Lanoie, *The Porter Hypothesis at 20: can environmental regulation enhance innovation and competitiveness,* Resources of the Future Discussion Paper (RFF DP 11-01), January 2011, http://www.rff.org/documents/RFF-DP-11-01.pdf

Anthony Giddens, *The Constitution of Society: Outline of the Theory of Structuration*, Polity Press, Cambridge, UK, 1984.

Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, Brussels, 23 March 2012, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Article 29 Data Protection Working Party, 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, 1 December 2009, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

Bauman, Zygmunt, *Alone Again, ethics after certainty*, Demos Papers, 1994

Beekman, Volkert, and Frans W.A. Brom, "Ethical tools to support systematic public deliberations about the ethical aspects of agricultural biotechnologies", *Journal of Agricultural and Environmental Ethics*, Vol. 20, No.1, Feb. 2007

Bennett, Colin J., Charles Raab, *The Governance of Privacy – Policy Instruments in a global perspective*, Cambridge, London: The MIT Press, 2006

Brey, Philip, "Anticipatory Technology Ethics for emerging IT", *Nanoethics*, Vol. 6, n1, April 2010, pp. 1-13

Brey, Philip, "Philosophy of Technology after the empirical turn", *Techné: Research in Philosophy and Technology*, vol. 14, n.1, 2010

Bruno Latour, *Aramis ou l'amour des techniques*, Paris: La Découverte, 1992

Bruno Latour, *L'espoir de Pandore. Pour une version réaliste de l'activité scientifique*, Paris: La Découverte, 2001

Cabinet Office, Cross Government Actions: Mandatory Minimum Measures, 2008. http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf

Cabinet Office, Data Handling Procedures in Government: Final Report, June 2008, p. 18. http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf

CEN Expert Group, Report on Supply Chain Security, Brussels 14th November 2006, http://www.cen.eu/cen/Sectors/Sectors/Services/Documents/FINALREPORTCENSCSNovember2006.pdf

Clarke, Roger, "PIAs in Australia: A work-in-progress report", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012

Clarke, Roger, "Privacy Impact Assessment: Its Origins and Development", *Computer Law & Security Review*, Vol. 25, No.2, April 2009

Clarke, Roger, "What's 'Privacy'?", *Australian Law Reform Commission Workshop*, 28 July 2006. http://www.rogerclarke.com/DV/Privacy.html

Collingridge, David, *The Social Control of Technology*, Frances Pinter, 1980

Commission National de l'Informatique et des Libertés (CNIL), Gérer les risques sur les libertés et la vie privée, la method [*Methodology for privacy risk management*], Paris, June 2012

Decker, Michael, "The role of ethics in interdisciplinary technology assessment", *Poiesis & Praxis*, Vol. 2, Nos. 2-3, April 2004

Deutsch, David, *The beginning of Infinity, Explanations That Transform the World*, Penguin Books, 2012

van Drooghenbroeck, S., *La proportionnalité dans le droit de la Convention européenne des droits de l'homme. Prendre l'idée simple au sérieux*, Bruxelles, Bruylant, 2001

ENISA, Being diabetic in 2011: Identifying emerging and future risks in remote health monitoring and treatment, European Network and Information Security Agency, Heraklion, 2009

European Commission Communication on Europe 2020: a European strategy for smart, sustainable and inclusive growth, COM (2010) 2020, Brussels 3rd March 2020. http://ec.europa.eu/research/era/docs/en/investing-in-research-european-commission-europe-2020-2010.pdf

European Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification. C(2009) 3200, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:EN:PDF

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

European Commission, Communication from the Commission on impact assessment, COM(2002) 276 final.http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0276:FIN:EN:PDF

European Commission, Communication on Innovation Policy: updating the Union's approach in the context of the Lisbon Strategy, COM(2003) 112, http://ec.europa.eu/invest-in-research/pdf/download_en/innovation_policy_updating_union.pdf

European Commission, Impact Assessment Guidelines, SEC(2009) 92, pp. 4-6. http://ec.europa.eu/enterprise/policies/sme/files/docs/sba/iag_2009_en.pdf

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012, COM(2012) 11 final

European Communication on Innovation Policy: updating the Union's approach in the context of the Lisbon Strategy, COM(2003) 112, http://ec.europa.eu/invest-in-research/pdf/download_en/innovation_policy_updating_union.pdf

European Council, Framework Decision of on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 27 November 2008 OJ L350/60, 30.12.2008.

European Data Protection Supervisor, EDPS, Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012

European Group of Ethics, General Report on the Activities of the European Group of Ethics in Science and New Technologies to the European Commission, 2005-2010, http://ec.europa.eu/bepa/european-group-ethics/docs/gar_ege_2005-2010_web.pdf

European Parliament and the Council, Decision No 182/1999/EC concerning the fifth framework programme of the European Community for research, technological development and demonstration activities (1998 to 2002), 22 December 1998

European Parliament and the Council, Decision No 182/1999/EC of 22 December 1998 concerning the fifth framework programme of the European Community for research, technological development and demonstration activities (1998 to 2002), Decision n 182/1999/EC

European Parliament and the Council, Directive 1995/46/EC 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. OJ L 281, 23.11.1995

European Parliament and the Council, Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O. J. L 201, 31/07/2002

European Parliament and the Council, Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, 13/04/2006

European Security research and Innovation Forum (ESRIF) Final Report, December 2009, http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf

Finn, Rachel L., and David Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review*, Vol. 28, No. 2, Apr. 2012, pp. 184-194. http://www.sciencedirect.com/science/journal/02673649

Finn, Rachel L., David Wright, Michael Friedewald, Raphaël Gellert, Serge Gutwirth, Bärbel Hüsing, Piret Kukk, Emilio Mordini, Philip Schütz, and Silvia Venier, "Privacy, data protection and ethical issues in new and emerging technologies: Five case studies", Deliverable 2, PRESCIENT Project, 2011. http://prescient-project.eu/prescient/inhalte/download/PRESCIENT_D2.pdf

Finn, Rachel, David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert et al. (eds.), *European data protection: coming of age?*, Springer, Dordrecht, 2013

Fisher, E., J. Jones and R. Von Schomberg, *Implementing the precautionary principle: Perspectives and Prospects*, Edward Elgar Publishing Limited, 2006

Flaherty, David, *Protecting Privacy in Surveillance Societies*, The University of North Carolina Press, 1989.

Freeman, Chris, and Francisco Louça, *As the time goes by: From the Industrial Revolutions to the Information Revolution*, Oxford University Press, 2001

Friedeman, B., and P. Kahn, "Human Values, Ethics and Design", in Jacko J., and A. Sears, *The Human-Computer Interaction Handbook*, 2003

Friedewald, Michael, Dara Hallinan, Raphaël Gellert, Serge Gutwirth, Silvia Venier, Emilio Mordini, and David Wright, "Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data", Deliverable 3, PRESCIENT Project, 2012. http://prescient-project.eu/prescient/inhalte/download/PRESCIENT_Deliverable_3_Final.pdf

Gellert, R., E.De Vries, P. De Hert, S. Gutwirth, "A comparative analysis of anti-discrimination and data protection legislations", in Custers Bart, Toon Calders , Bart Schermer, Tal Zarsky, *Discrimination and privacy in the information society. Data mining and profiling in large databases*, Springer, 2012, http://works.bepress.com/serge_gutwirth/90

Gellert, Raphael and Gutwirth, Serge, "Beyond accountability, the return to privacy?" in Daniel Guagnin et al., *Managing Privacy Through Accountability*, Palgrave Macmillan, 2012

Giddens, Anthony, *Modernity and self-identity. Self and society in the late modern times*, Stanford University Press, 1991

Gloria González Fuster, Gellert R., "The fundamental right of data protection in the European Union: in search of an uncharted right", *International Review of Law, Computers & Technology*, 26:1, 2012.

Goold, Benjamin J., "Surveillance and the political value of privacy", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009, pp. 3-6.

Goujon, Philippe, Catherine Flick, *ETICA D4.1: Governance approaches. A critical appraisal of theory and practice*, http://ethics.ccsr.cse.dmu.ac.uk/etica/deliverables/D41final.pdf

Grunwald, Armin, "Technology Assessment or Ethics of Technology? Reflections on Technology Development between Social Sciences and Philosophy", *Ethical Perspectives*, Vo.6 No.2, July 1999, pages 171-182http://www.kuleuven.be/ep/viewpic.php?LAN=E&TABLE=EP&ID=237

Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Lanham, 2002

Gutwirth, Serge, Raphaël Gellert, Rocco Bellanova, Michael Friedewald, Philip Schütz, David Wright, Emilio Mordini, and Silvia Venier, "Legal, social, economic and ethical conceptualisations of privacy and data protection", Deliverable 1, PRESCIENT Project, 2011. http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf

Hansson, Sven Ove, "Philosophical problems in cost-benefit analysis", *Economics and Philosophy*, Issue 23, 2007, pp. 163-183.

Health Information and Quality Authority, *Guidance on Privacy Impact Assessment in Health and Social Care*, Dublin, December 2010. http://www.hiqa.ie/resource-centre/professionals

Health Information and Quality Authority, *International Review of Privacy Impact Assessments*, 2010. http://www.hiqa.ie/standards/information-governance/health-information-governance

De Hert, Paul and Serge Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in Erik Claes, Anthony Duff et al. (eds.), *Privacy and the criminal law*, Intersentia, Antwerp, Oxford, 2006, pp. 75-85

Information Commissioner's Office (ICO), *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 2.0, June 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

Jonas, Hans, "Technology and Responsibility: Reflections on the New Tasks of Ethics", *Social Research*, Vol. 40, N. 1, 1973

Jonas, Hans, *The imperative of responsibility. In search of an ethics for the technological age*, University of Chicago Press, 1984.

Kenneally, Erin, Bailey, Michael, and Maughan, Douglas, "A Framework for Understanding and Applying Ethical Principles in Network and Security Research", in *Workshop on ethics in Computer Security Research* (*WECSR '10*), Tenerife, Canary Islands, Spain, January 2010

Kroes, P., and A. Meijers, *The Empirical Turn in the Philosophy of Technology*, Amsterdam, JAI, 2000.

van Loon, Joost, "Virtual Risks in the Age of Cybernetic Reproduction", in Adam, Barbara, Beck, Ulrich, Van Loon Joost, *The Risk Society and Beyond. Critical Issues for Social Theory*, SAGE publications Ltd, 2000

vande Lanotte, Johan, Y. Haeck, *Het Europees verdrag tot bescherming van de rechten van de mens in hoofdlijnen*, Antwerpen, Maklu, 1997

Luiz Costa, "Privacy and the precautionary principle". *Computer Law & Security Review*, *28*(1), 2012

MASIS (Monitoring Activities of Science in Society in Europe) Report, *Challenging Futures of Science in Society. Emerging Trends and cutting-edge issues*, 2009, ftp://ftp.cordis.europa.eu/pub/fp7/sis/docs/sis_masis_report_en.pdf

Mepham, B., “A framework for the ethical analysis of novel foods: the ethical matrix”, *Journal of Agricultural and Environmental Ethics*, Vol 12, 1996, pp. 165-176

Meuwese, A., *Impact Assessment in EU Law-making*, Ph.D. Thesis, Uni. Leiden, 2008, pp. 102-104. https://openaccess.leidenuniv.nl/bitstream/handle/1887/12589/Thesis.pdf?sequence=3

Mitcham, Carl, *Thinking Through Technology. The Path between Engineering and Philosophy*, University of Chicago Press, 1994

Moor, James H., “Why we need better ethics for emerging technologies”, *Ethics and Information Technology*, Vol. 7, No. 3, 2005, pp. 111-119

Mordini, Emilio, “New Security Technologies and Privacy”, in European Commission, *Ethical and Regulatory Challenges to science and research Policy at the Global Level*, 2012, http://ec.europa.eu/research/science-society/document_library/pdf_06/ethical-and-regulatory-challenges-042012_en.pdf

Nagenborg, Michael, Rafael Capurro, *Ethical Evaluation*, ETICA Deliverable 3.2.2, http://ethics.ccsr.cse.dmu.ac.uk/etica/deliverables/D322final.pdf

Nissenbaum, Helen, “Information Technology and Ethics”, *Berkshire Encyclopedia of Human Computer Interaction*, Great Barrington, MA, Berkshire Publishing Group, 2004, pp. 235-239

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books, Stanford CA, 2010.

Office of Management and Budget, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Washington, DC, 26 Sept 2003. http://www.whitehouse.gov/omb/memoranda/m03-22.html

Office of the Chief Information and Privacy Officer (OCIPO), Privacy Impact Assessment Guide for the Ontario Public Service, Queen’s Printer for Ontario, December 2010.

Office of the Information and Privacy Commissioner (OIPC) of Alberta, Privacy Impact Assessment (PIA) Requirements, For use with the Health Information Act, January 2009. www.OIPC.ab.ca

Office of the Privacy Commissioner, Guidance Note for Departments Seeking Legislative Provision for Information Matching, 16 May 2008, Appendix B. http://privacy.org.nz/guidance-note-for-departments-seeking-legislative-provision-for-information-matching/#appendix

Office of the Privacy Commissioner, Privacy Impact Assessment Guide, Sydney, NSW, August 2006, revised May 2010. http://www.oaic.gov.au/publications/guidelines.html#privacy_guidelines

Office of the Privacy Commissioner, Privacy Impact Assessment Handbook, Auckland/Wellington, 2007. http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf

Office of the Victorian Privacy Commissioner (OVPC), Privacy Impact Assessments – A guide for the Victorian Public Sector, Edition 2, Melbourne, April 2009. http://www.privacy.vic.gov.au/privacy/web2.nsf/pages/publicationtypes?opendocument&Subcategory=Guidelines&s=2

Ortwin, Renn, *Risk Governance: Coping with Uncertainty in a Complex World*, Earthscan, London, 2008

Palm, Elin, Hansson, Sven Oven, “The case for ethical technology assessment (eTA)” *Technology Forecasting and Social Change*, 73, 543-558, 2006.

van der Ploeg, Irma, *The Machine Readable Body: Essays on biometrics and the Informatization of the body*, Shaker, Germany, 2005.

Punie, Yves, Ioannis Maghiros, and Sabine Delaitre, "Dark Scenarios as a constructive tool for future-oriented technology analysis: Safeguards in a world of ambient Intelligence", in *Proceedings of the Second International Seville Seminar on Future-Oriented Technology Analysis: Impact of FTA Approaches on Policy and Decision-Making*, Seville, 28-29 September 2006. http://foresight.jrc.ec.europa.eu/documents/papers/paper%20dark%20scenarios%20FTA%20conf%20Sept.pdf

Raab, Charles and David Wright, "Surveillance: Extending the Limits of Privacy Impact Assessment", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012

Rowe, Gene, and Lynn J. Frewer, "A Typology of Public Engagement Mechanisms", *Science, Technology & Human Values*, Vol. 30, No. 2, 2005, pp. 251-290. http://sth.sagepub.com/cgi/content/abstract/30/2/251

von Schomberg, René, *From the Ethics of Technology towards an Ethics of Knowledge Policy and Knowledge Assessment. A working document for the European Commission services*, European Commission's Directorate General for Research, 2007. http://ec.europa.eu/research/science-society/pdf/ethicsofknowledgepolicy_en.pdf

von Schomberg, René, *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technology Fields, A report from the European Commission Services*, European Union, 2011, http://ec.europa.eu/research/science-society/document_library/pdf_06/mep-rapport-2011_en.pdf

de Schutter, Olivier, *International Human Rights Law: Cases, Materials, Commentary,* Cambridge University Press, 2010.

Schwartz, Peter, *The Art of the Long View*, John Wiley & Sons, Chichester, 1998 (first published 1991)

Skorupinski, Barbara, and Konrad Ott, "Technology assessment and ethics", *Poiesis & Praxis*, Vol. 1, 2002, pp. 95-122

Sollie, Paul, "Ethics, technology development and uncertainty: an outline for any future ethics of technology", *Journal of Information, Communication and Ethics in Society*, Vol. 5 Iss: 4, 2007, pp.293 - 306

Sollie, Paul, Marcus Duwell, *Evaluating New technologies. Methodological problems for the Ethical Assessment of Technology Developmen*t, Springer, 2009

St. Braconnier, *Jurisprudence de la Cour européenne des droits de l'homme et droit administratif français*, Bruxelles, 1997, pp. 318-322

Stahl, Bernd Carsten, and Wakunuma, Kutoma J., *ETICA D5.3 Project Nomenclature (Now Glossary) - Ethical issue determination,* 2009, http://ethics.ccsr.cse.dmu.ac.uk/etica/deliverables/D53ProjectNomenclatureGlossaryfinal.pdf

Stahl, Bernd Carsten, et al., "Identifying the Ethics of Emerging Information and Communication Technologies, ICTs: An essay on Issues, Concepts, Method", *International Journal of Techno-ethics*, Vol. 1, n.4, October-December 2010, pp. 20-38, http://www.tech.dmu.ac.uk/~bstahl/publications/2010_etica_methodology_IJT.pdf

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.

Stoddart, Jennifer, "Auditing Privacy Impact Assessments: The Canadian Experience", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012

Sudre, F., *Les 'obligations positives' dans la jurisprudence européenne des droits de l'homme*, R.T.D.H., 1995, pp. 363-384;

Treasury Board of Canada Secretariat, Directive on Privacy Impact Assessment, Ottawa, 1 Apr 2010. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text

Treasury Board of Canada Secretariat, Privacy Impact Assessment Guidelines: A framework to Manage Privacy Risks, Ottawa, 31 August 2002. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp

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

Weber, K. Matthias, Nicolai, Marcus, "The ethical dimension of technology watch and assessment", *Proceedings of a seminar on Opportunities for integrating ethical aspects into the IPTS Technology Watch Activities*, IPTS, Seville, March 1996

Wright, David and Paul de Hert*, Privacy Impact Assessment*, Springer, 2012.

Wright, David, "A framework for the ethical impact assessment of information technology", *Ethics and Information Technology*, Vol. 13, No. 3, September 2011, pp. 199-226. http://www.springerlink.com/content/nw5v71087x60

Wright, David, "Alternative futures: AmI scenarios and Minority Report", *Futures*, Vol.40, No.5, June 2008, pp. 473–488.

Wright, David, "Should Privacy Impact Assessments be mandatory?", *Communications of the ACM*, Vol. 54, No. 8, August 2011, pp. 121-131.

Wright, David, "The state of the art in privacy impact assessment", *Computer Law & Security Review*, Vol. 28, No. 1, Feb. 2012, pp. 54-61, http://www.sciencedirect.com/science/journal/02673649

Wright, David, and Kush Wadhwa, "Introducing a privacy impact assessment policy in the EU Member States", *International Data Privacy Law*, Vol. 3 Issue, 1 February 2013 [forthcoming], http://idpl.oxfordjournals.org/content/early/recent

Wright, David, et al, PIAF D2, *Empirical research on contextual factors affecting the introduction of privacy impact assessment frameworks in the Member states of the European Union*, published August 2012, http://www.piafproject.eu/ref/PIAF_deliverable_d2_final.pdf

Wright, David, et al, PIAF Deliverable D1, *A Privacy Impact Assessment Framework for data protection and privacy rights*, 2011.

Wright, David, Rachel Finn and Rowena Rodrigues, "A comparative analysis of privacy impact assessment in six countries", *Journal of Contemporary European Research*, Vol. 9, 2013 [forthcoming]

Wright, David, Serge Gutwirth, Michael Friedewald et al. (eds.), *Safeguards in a World of Ambient Intelligence*, Springer, Dordrecht, 2008