Executive Summary:
Technology and privacy are two intertwined notions that must be jointly analysed and faced. Technology can be regarded as a social practice that embodies the capacity of societies to transform themselves by creating and manipulating not only physical objects but also symbols, cultural forms and social relations. In its turn, privacy describes a vital, complex aspect of these social relations. Technology influences people's understanding of privacy, and people's understanding of privacy helps drive technology development. Either policy-making takes into account this rich and nuanced interplay between technology and privacy or we run the risk of failing to govern the current, concomitant technology and privacy revolution.

New technologies can often be used in a way that undermines the right to privacy because they facilitate the collection, storage, processing and combination of personal data by security agencies and businesses. The rise of social networking websites have led to a dramatic increase in the amount of personal information available online, which is routinely misappropriated for identity theft or other fraudulent purposes. Employers also mine these sites in order to vet prospective employees. RFID and biometrics can also be used in ways invidious to our privacy.

The use of these new technologies is changing the ways in which we understand privacy and data protection. It is not sufficient to look at privacy as only a legal or human right. It is necessary to reconceptualise privacy in ethical, social, cultural and other dimensions and to see how these different conceptualisations impact each other and how they can be bridged. We think part of the solution is much wider use of privacy and ethical impact assessments before new technologies or projects involving personal data are undertaken.
The PRESCIENT project has addressed the above mentioned challenges in three steps:

* Theoretical analysis of the notions of privacy and data protection from different disciplinary perspectives as conceptualised from an ethical, socio-economic and legal perspective.

* Empirical analysis of challenges to privacy and data protection arising from new sciences and technologies in different fields. The researchers have analysed contactless identification technologies for public transport and in passports; body imaging scanners and unmanned aircraft systems; behavioral and soft biometrics; whole genome sequencing technologies and biocybernetics and technologies for human enhancement. In addition we have analysed citizen concerns and knowledge of the way in which their data are collected, stored and used and their concerns about new technologies and how their concerns have changed over time.

* Design of a common framework for privacy and ethical assessment in the context of the ongoing reform of the data protection regulation in the EU.

Project Context and Objectives:
Privacy is a multifaceted concept that is currently challenged by many developments in science and technologies. Some of the most prominent examples are identification technologies such as RFID, social network services such as Facebook and the creation of large biobanks.

The concept of privacy has always been subject to changes. People define it differently and value it differently. Moreover, privacy often is balanced against other values, such as society’s safety and security. Empirical research is needed to determine how people value privacy, however they define it, in order to understand how citizens understand the right to privacy and its value within the whole context of other fundamental rights.

Privacy is not only respect for confidentiality, although it implies it. Privacy is not only the right to be left alone, although it includes it. Privacy is not only the right to control one's own life, although it entails it. Nor is privacy only data protection, although it also concerns data protection. Privacy is all these things together, and more, because privacy is the word we use to describe an important aspect of one of the main, vital and constitutive polarities that shape human beings, that is, the tension between individuals and the community. How do new technologies impact on this complex and rich concept? What are the privacy issues arising from different emerging technologies? Multidisciplinary analysis is needed in order to appreciate the various philosophical, political, legal, ethical and social meanings of the word “privacy” in the contemporary technological world.

Privacy is also a salient topic in technology policy-making. There is a need for a new social dialogue on privacy rights that includes issues such as the new borders of the private domain, a new business ethics and a dialogue on the balance between civil and government rights. From the privacy issues raised by new technologies, a new taxonomy of privacy problems is needed to help policymakers balance privacy against countervailing values, rights, obligations and interests.

Data protection is both broader and more specific than the right to privacy. The relationship between these concepts is certainly something that needs to be addressed for a reconceptualisation of privacy. Data protection is broader because data protection not only aims to make concrete the protection of privacy, but also tends to protect other rights and interests such as the freedom of expression, the freedom of religion and conscience, the free flow of information and the principle of non-discrimination. It is more specific because personal data are processed. The application of data protection rules does not require an answer to the question of a violation of privacy: data protection applies when the conditions put by legislation are fulfilled. Furthermore, data protection rules are not prohibitive by default; they channel and control the way personal data are processed. Such data can only be legitimately processed if some conditions pertaining to the transparency of the processing and the accountability of the data controller are met.

Yet with the “technology revolution”, the notion of privacy has started a new journey, beyond the mere legal sphere, which is probably leading privacy to its original roots, the relation between the citizen and the “polis”. We are facing new contexts (think, for instance, of the so-called PAN, personal area network, which describes a technology that could enable wearable computer devices to communicate with other nearby computers and exchange data) and new concepts (as, for example, the idea of genomic and proteomic information), not to mention issues raised by technologies such as biometrics, RFID, smart surveillance systems, body implants, nano devices and the like.
New technologies have specific features that make them quite different from traditional industrial technologies. Compared to technologies that drove the industrial revolution – which were complex, based on collective action, social infrastructure, and technical know-how – emerging technologies are lighter. They are decentralised, dispersed, and disseminated, and their control and use are largely in the hands of individuals, citizens' groups, and small enterprises. They are network technologies as Manuel Castells calls them. In addition, new technologies help to reduce the complexity of human (social, biological, political, etc.) interactions and allow the individual to distance themselves from their observation. As Paul Virilio has emphasised, new technologies always bring about even more and even faster new technologies. Emerging technologies also imply a change in the relationship between science and politics. In the last few decades, representation of science has changed so much that some people may say doing science is another way of doing politics. Indeed, the post-modern technological system is embedded in politics. Researchers are under increasing pressure to demonstrate the policy relevance of their findings and to deliver tangible results. In turn, policy-makers are under increasing pressure to justify their choices of technology to be developed and socio-economic goals to be achieved. As emerging technologies often challenge basic moral assumptions, they provoke directly or indirectly a crisis, or at least a basic uncertainty with regard to moral standards that are either sanctioned by law or remain tacit presuppositions. This amounts to a growing gap between citizens, technology, and politics, notably when the individual's private sphere conflicts with the notion of common good.

Thus the starting point for the PRESCIENT project was the recognition that it was time for reconceptualising privacy, to develop suitable methods in order to assess the impacts that emerging technologies have and to think of privacy as a central element in the governance of science and technology. The PRESCIENT project addressed these issues in two main areas:

1) Conceptualisation of privacy: Until now, privacy has mainly been conceptualised as a legal issue or, increasingly, as a human rights issue. Until the start of PRESCIENT, very little work had been devoted to privacy as a value and its role in the overall architecture of EU values as sketched by the Charter of Fundamental Rights of the EU. The project partners analysed five different emerging technologies to determine whether there are privacy problems posed by new technologies that do not fall easily within commonly used taxonomy of privacy problems. The problem with framing privacy solely in individualistic terms is that privacy becomes undervalued. The interests aligned against privacy – for example, efficient consumer transactions, free speech or security – are often defined in terms of their larger social value. In this way, protecting the privacy of the individual seems extravagant when weighed against the interests of society as a whole. Ethical issues will also need to be addressed, especially as they come in increasing numbers and often "packaged" in terms of complex technology. Such ethical issues will require considerable effort to be understood as well as a considerable effort to formulate and justify good ethical policies. People who both understand the technologies and are knowledgeable about ethics are in short supply just as their need is expanding.

2) Privacy Impact Assessment (PIA): In Europe, policy-makers have been considering the adequacy of data protection legislation, the powers accorded national data protection authorities, the tension between facilitating trade and transborder data flows while ensuring personal data are protected and accessible and not misused once they leave European jurisdiction. There has been a primary focus on legislative consideration. At the same time, the European Commission and others have been concerned about the advent of new technologies and how their possible privacy impacts can be addressed. When the PRESCIENT project started, PIA on the European level was more or less unknown. In 2010 the EC's RFID PIA framework was a groundbreaking initiative. With the EC's proposal for a General Data Protection Directive in January 2012 the project's work became highly topical because in Art. 33 it foresees a so-called Data Protection Impact Assessment. The PRESCIENT project thus could contribute to the political discourse and even make the case for a more extensive use of PIAs modified to take into account ethical considerations. PIAs used in tandem with ethical impact assessments could do much to come to terms with stakeholder apprehensions and, more specifically, a lack of public and stakeholder knowledge about new technologies and their ethical implications before the technologies are widely deployed.

**Project Results:**

1. Legal, social, economic and ethical conceptualisations of privacy and data protection

In the first phase of the PRESCIENT project, 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.

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 was to map these differences, which we will come back to infra. 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.

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.

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, but whose scope is not about giving a substantial definition of a notion. 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).

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 viewpoint; 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.

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.

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 aimed 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 Deliverable 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).

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 (ECHR), 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 ECHR. 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, 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 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. 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.

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

New and emerging technologies often raise privacy and ethical issues. In the scope of the second phase of the PRESCIENT project, the consortium undertook several case studies of new technologies to consider the privacy and ethical issues they raised. Our 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.

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).

2.1 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 Roger Clarke's four different categories of privacy – privacy of the person, privacy of personal data, privacy of personal behaviour and privacy of personal communication – 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.

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.

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 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 person’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” (Clarke 2006). 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 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 (Clarke 2006). 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.

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.

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 and 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

From the information presented in this section, 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 Considering ethical and social issues

In addition to privacy issues, new technologies also raise ethical 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” (van der Ploeg 2005), 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 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 processors 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.

2.3 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. Additionally, 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 into 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.

However, some have criticised PIAs for their focus on privacy to the detriment of other considerations such as ethical or social issues. We 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. 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.

3 The analysis of citizens’ concerns and knowledge about personal data processing

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

- **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 with the question of to what extent can European citizens have access to the personal information and are they able to correct information and find out how their information is being used.

- **Data Protection Authorities (DPAs):** This part explored what role DPAs play in reconciling the rights and interests of data subjects and data controllers.

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.
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 dated 16 October 2012. 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. 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.

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 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.

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.

4 Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies

In the final part of the project the consortium has considered how to address potential privacy risks posed by emerging sciences and technologies and proposes a framework for a Privacy and Ethical Impact Assessment (P+EIA) Framework.

First, building on the findings from the case studies, the partners developed scenarios highlighting the privacy and ethical issues that might arise with emerging technologies and, in particular, the ethical dilemmas. We 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. The 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, we analysed the European Union’s legal environment targeting privacy and data protection impact assessment exercises. We have fleshed 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, we decided to broaden the discussion on the key methodological and philosophical challenges in including ethical values in PIAs. 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. There are, however, 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. In a short historical overview of the development of the field of technology ethics we point 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. Finally we present an overview and a critical reflection of contemporary quantitative approaches to technological risk assessment, privacy impact assessment, and ethical assessment methodologies. Finally, the last section is concerned with summarising some philosophical and methodological challenges in conducting such exercises.

Finally we suggest a framework for assessing privacy impacts, and how to engage stakeholders in the process. We have envisaged a P+EIA process comprising 16 principal steps. 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.


Potential Impact:

The project partners had anticipated that PRESIENT would have a strategic impact in various dimensions:

1 Contribution to the quality of research:

This was realised in particular through WPs 1 and 2 focused on scientific research and its technological or clinical applications. In these work packages we have achieved a new conceptualisation of privacy based on an in-depth analysis of different emerging sciences technologies and technologies.
We have always presented and discussed our preliminary and interim results to peers and to relevant stakeholders in order to ensure the validity of our data and conclusions. For this purpose we have on the one hand created a steady expert group who have reviewed most of the draft deliverable. The comments have been an important input for the final version of these deliverables. On the other hand we have done presentations at workshops and meetings of related projects and discussed and compared our approaches and results.

In the deliverables we always aimed to address two crucial issues affecting the quality of research on privacy and ethics: One is that we will make and clarify the distinction between the legal, ethical and socio-economic approaches to privacy. The legal conceptualisations of privacy are the result of legal practice (case-law) as it works in reference to a legislative (political) framework and as this legal practice is interpreted by the legal scholars ("authorities"). Ethical considerations are much more value-based and normative and stem from a very different way of thinking and researching. Socio-economic aspects, again, raise different perspectives: how is privacy protection perceived? what does it cost? how are individuals and groups experiencing their privacy? is there awareness?

The second crucial issue is the distinction between privacy and data protection. The European Charter of Fundamental Rights (in Articles 7 and 8) distinguish them. PRESIENT has further developed this distinction, and ethicists and social scientists can reflect upon this crucial distinction from their perspective, comment upon it, criticise it or make it more operational for their concerns.

2. Early identification of ethical issues:

Though PRESIENT was not a genuine foresight project we have – in the case studies and in the scenarios - identified important privacy, data protection and ethical issues.

3. Contribution to European policy-making:

In our proposal (written in late 2008) for the PRESIENT project we stated that "policy-makers, starting with the European Commission, need to adopt the privacy and ethics impact assessment framework as set out in this proposal. We believe that adoption of such a framework is a realistic expectation, since it has continued to accord greater importance to ethics and as it has already recommended a privacy impact assessment of RFID applications. " With the proposed General Data Protection Regulation that in Art 33 foresees a "Data Protection Impact Assessment" the EC has even gone beyond our expectations. Here PRESIENT was a very timely project and was able to contribute to the consultations for the new regulation. Moreover we expect that PRESIENT is also able to make a contribution to the implementation of the new regulation.

Use and dissemination of foreground

A principal objective of PRESIENT was to disseminate results as early as possible and to the largest possible relevant audience. Thus, the PRESIENT partners have published their results in numerous articles and presented them at numerous conferences.

The most important peer reviewed journal publications include (among others):

* Hallinan, Dara, and Michael Friedewald, "Public Perception of the Data Environment and Information Transactions: A selected-survey
analysis of the European public's views on the data environment and data transactions", Communications and Strategies, No. 88, 2012, pp. 61-78.


PRESIDENT results have been presented at the following scientific conferences and workshops

* COST LiSS Conference (2011, 2012)
* EACME Annual Meeting (2010)
* Fifth Biannual Surveillance and Society Conference
* IFIP Summer School on Identity Management (2010, 2011)
* ISA Annual Convention (2012, 2013)
* Italian National Congress of STS (2012)
* Youth Media Days Munich (2010)
* Conference of the German Society for Sociology (2010)
* Workshop of the DETECTER project (2010)
* Conference of the PATS project (2011)
* Workshop of the ETHICA project (2011)
* Workshop of the STOA project "Making Perfect Life" (2011)

List of Websites:

http://www.prescient-project.eu