Technological Forecasting & Social Change 87 (2014) 325–336

Contents lists available at ScienceDirect

Technological Forecasting & Social Change

FROM MY PERSPECTIVE

Ethical dilemma scenarios and emerging technologies

David Wright [a,*], Rachel Finn [a], Raphael Gellert [b], Serge Gutwirth [b], Philip Schütz [c], Michael Friedewald [c], Silvia Venier [d], Emilio Mordini [d]

[a] Trilateral Research & Consulting, Crown House, 72 Hammersmith Road, London, W14 8TH, UK
[b] Vrije Universiteit Brussel, Pleinlaan 2, 1050 Elsene, Belgium
[c] Fraunhofer Institute for Systems and Innovation Research, Breslauer Straße 48, 76139 Karlsruhe, Germany
[d] Centre for Science, Society and Citizenship, Via Capo di Ferro, 23, 00186 Rome, Italy

ARTICLE INFO

Article history:
Received 3 April 2013
Received in revised form 26 August 2013
Accepted 8 December 2013
Available online 30 December 2013

Keywords:
Ethical dilemma scenarios
Privacy impact assessment
Ethical impact assessment
Near field communications
Biometric technologies
Human enhancement
Drones

ABSTRACT

This paper posits that ethical dilemma scenarios are a useful instrument to provoke policy-makers and other stakeholders, to including industry, in considering the privacy, ethical, social and other implications of new and emerging technologies. It describes a methodology for constructing and deconstructing such scenarios and provides four such scenarios in an orthogonal relationship with each other. The paper describes some different, but closely related scenario construction–deconstruction methodologies, which formed the basis for the methodology adopted in the European Commission-funded PRESCIENT project. The paper makes the point that in ethical dilemma scenarios, it is not immediately apparent what choices policy-makers should select. Hence, there is a need for undertaking a privacy and ethical impact assessment and engaging stakeholders in the process to identify and discuss the issues raised in the scenarios.

1. Introduction

Emerging technologies often raise privacy, ethical, societal and other issues. Project managers and stakeholders can address such issues using different instruments, especially by means of different types of impact assessments, such as privacy, ethical, social, technology and/or surveillance impact assessments. Another useful instrument is a scenario, especially a scenario that provokes project managers, policy-makers and stakeholders into thinking about the issues raised by the emerging technology and how they might deal with those issues. We subscribe to the dictum of scenario guru Peter Schwartz who 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 emphasised that "scenarios can help people make better decisions – usually difficult decisions – they would otherwise miss or deny."[1]

This paper 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.

One of the aims of the PRESCIENT project,[2] funded by the European Commission, was to provide an early identification of privacy and ethical issues arising from new and emerging technologies and their relevance for EC policy, to illustrate these issues in scenarios and to develop a privacy and ethical

* Corresponding author. Tel.: +44 207559 3550.
E-mail address: david.wright@trilateralresearch.com (D. Wright).

[1] Both quotes come from Schwartz [1: 4].
[2] www.prescientproject.eu.

0040-1625/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.techfore.2013.12.008

impact assessment methodology which could be used to resolve the ethical dilemmas raised in the scenarios.

Following an analysis of privacy and data protection as conceptualised from an ethical, socio-economic and legal perspective, the PRESCIENT partners[3] prepared a set of case studies wherein they identified the privacy, data protection and ethical issues arising from several different new and emerging technologies and their applications. The technologies and applications included RFID-embedded travel cards and passports, unmanned aerial systems ("drones"), body scanners, biometrics, DNA sequencing and human enhancement.

Building on the findings from the case studies, the partners developed scenarios highlighting the privacy and ethical issues that might arise with such technologies and, in particular, the ethical dilemmas. The consortium then went on to develop a privacy and ethical impact assessment framework by means of which such privacy and ethical issues could be addressed.

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.

2. Theoretical background

The theoretical background for this paper draws on three strands. The first provides an overview of scenario analysis; the second provides some context in terms of ethical theory and philosophy relevant for this paper; and the third relates these two strands to ethical impact assessment which frames the conclusion of this paper, "The way forward".

2.1. Scenarios

There are many different types of scenarios and methodologies for constructing and deconstructing them.

Scenarios are frequently-used tools for looking at the future. However, they are not predictions. Rather, they describe plausible and/or desirable futures and possible ways on how to realise these futures [2,3]. Scenarios may generally be normative or exploratory. They may be "sunny" or "dark", the first describing a positive future, one that we want, while the second describes a future that we do not want [4,5].

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

Herman Kahn, the father of scenario construction for futures research and policy analysis, tended to think in terms of three alternative scenarios applied to any subject: (1) surprise-free or business-as-usual that simply extrapolates current trends with interplay of the trends; (2) worst case scenario based on mismanagement and bad luck; and (3) best case scenario based on good management and good luck [6].

Scenarios can also be structured orthogonally along two important dimensions, 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. Typically, scenarios on such a grid are constructed from the variation in two key drivers. Our scenarios have "tweaked" this traditional approach, as described in more detail below.

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.

Scenarios can be short vignettes of a paragraph or two, or relatively long and detailed of many pages – or even book length (e.g., Huxley's *Brave New World* or Orwell's *1984*). They can be conveyed on film (Spielberg's *Minority Report*) as well as on paper. Jerome C. Glenn and The Futures Group International provide a very good overview of the different types of scenario construction in their chapter on "Scenarios" for the Millennium Project [7].

Technology scenarios can serve many different purposes. They may be used as warnings for policy-makers and industry decision-makers of the risks that may arise with the development of new technologies [8]. They may be developed to describe the kind of future that we want and to prompt us to consider what steps we need to take to arrive at that future (backcasting or roadmapping). 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. Those developing scenarios should be clear about how they intend to use the scenarios, and what they want the scenarios to achieve.

The authors wanted to develop scenarios that highlighted 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?

2.2. Ethics and emerging technologies

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 in which we find ourselves, ethics can also be regarded as a legitimisation process for the pluralism of conceptions of "good lives". Ethics can inform debates. Ethics could become an element in processes of socio-technically distributed innovation, in which products and services are developed or at least refined at societal level [9].

We defined ethics as a philosophical enquiry in concepts involved in practical reasoning, i.e., concepts related to the

[3] The PRESCIENT partners comprised Fraunhofer Information Systems Institute (Germany), Trilateral Research & Consulting (UK), Vrije Universiteit Brussel (VUB, Belgium) and the Centre for Science, Society and Citizenship (CSSC, Italy). The 3-year project concluded at the end of December 2012.

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 a utilitarian framework of weighing 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).

With the emergence of advanced information and surveillance technologies, however, ethics is not only confronted with the justification of intentional actions of individuals, as it can be conceived in these more classical approaches. The development of new ICTs and other security technologies is generally complicating the definition of the role of ethics, as well as the identification of its theoretical approaches and operational instruments needed to address related issues. There are several reasons why the role of ethics is becoming complicated in the assessment of emerging technologies.

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 decentralisation of technology development, distributing responsibilities among many individuals, may result in an anonymous process for which nobody can be held responsible. Individuals may identify themselves in having roles for particular parts of the technology development process, but only part. Hence, if they think about this issue, they believe themselves to be only partly responsible or, in other words, not responsible for the outcomes of the whole process. This raises the issue of how to define and assign critical terms such as "responsibility" or "accountability" [8].

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, 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 emerging technologies, it may also help stimulate public discourse to critically reflect on decisions and priorities which are affecting human nature and society as a whole. This is of particular relevance when dealing with the relationship between contemporary values and rights and emerging technologies.

2.3. Scenarios and ethics in ethical impact assessment

When scenarios show that emerging technologies might raise ethical issues, then project managers and/or policy-makers should consider undertaking an ethical impact assessment, in consultation with stakeholders, to identify and resolve any ethical issues. While the term "ethical impact assessment" seems to be of relatively recent provenance, ethics in technology assessment has been discussed for many years.

Though the ethics of technology and the assessment of technology impacts both have a long tradition dating back until the 1970s, the attempt to systematically assess ethical impacts of emergent technologies is relatively new [10–13].

The first ideas, however, for ethical and social assessments of new technologies have emerged before this. For example, Kuzma et al. wrote a paper entitled "An Integrated Approach to Oversight Assessment for Emerging Technologies", published in the prestigious journal *Risk Analysis* in 2008 [13]. And three years before this, Hofmann published a paper entitled "On value-judgements and ethics in health technology assessment" [14]. So we already see technology assessment experts describing how ethics could be taken into account in their assessments. The year before this, in 2004, Weingarten et al. wrote about "Assessing ethics of trials in systematic reviews" [15]. Ethical issues need to be discussed by stakeholders, hence, some experts such as Michel Decker have considered how best to engage different stakeholders (e.g., in his 2001 edited collection) [16].

About the same time, Gethmann posed some questions about participatory technology assessment [17], but even so, he states that participatory technology assessment concepts "have succeeded in overthrowing the elitist, expert-cratic claim of scientific TA, in favour of a democratic, communicative form involving the participation of citizens" [17]. His paper has a note that it is based on a talk given at the international conference on "Interdisciplinarity in Technology Assessment", held in Bad Neuenahr-Ahrweiler, Germany, in September 2000. Gethmann had published papers on technology assessment before this, in 1999. He acknowledges even earlier antecedents, e.g., in the Netherlands and Denmark, where "the participatory element constitutes the paradigm of TA as a whole. (Eijndhoven and Est 2000 is an example of the situation in the Netherlands, Klüver 1995 and Meyer 1999 are typical examples for Denmark.)" [17].

It is interesting to see how the ideas, concepts and techniques behind the terms have developed since the 1970s with an increasing emphasis placed on ethical technology assessment [18].

Thus, we see that stakeholder consultation and consideration of ethical issues in technology assessment have been discussed since the last century (the 1970s). Building on this

Table 1
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.

potted history, and good practices from these sources, this paper elaborates further the methodology of ethical impact assessment (EIA) by including ethical dilemma scenarios as part of the EIA process, as a means to stimulate stakeholder consultation and discussion of ethical issues arising from emerging technologies. These issues continue to tease researchers today [19].

3. Constructing the scenarios

The following sections describe the process by which the partners created the ethical dilemma scenarios. We think the process by which we created these scenarios has wide applicability to many other technologies and is a useful way to consider, *in advance*, the privacy and ethical issues that might arise from the deployment of new technologies so that policy-makers and technology companies can avoid, mitigate or transfer the risks and, especially, avoid damage to citizen-consumer[4] trust and confidence and to their companies' reputation. Hence, the purpose of the ethical dilemma scenarios is to describe a plausible future in which new or emerging technologies raise ethical issues that require discussion between and among stakeholders as part of a properly structured ethical impact assessment process.

The authors 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 authors agreed to create short "what if" scenarios situated just a few years into the future. The objective of the scenarios was to tell some short, plausible 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.[5]

We created four orthogonal scenarios. Each scenario is orthogonal to the others, but not in the way that most other sets of four scenarios are. Instead of working with two drivers in counter-point to each other, we created a variation on the orthogonal-quadrant-based approach to scenario construction. We started with a "dark" scenario and then created a causal relationship between the dark scenario (Quadrant 1) and the second scenario, i.e., the dark scenario 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). Hence, there is a causal relationship between the contextual factors in each of the four quadrant scenarios and each of the four scenarios describes a plausible future (See Table 1).

3.1. Identify the technologies and applications

As the consortium was 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.

The consortium decided to focus on several technologies or types of technologies. For example, one of these was human enhancement technologies. The consortium 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. The partners 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, the partners assumed that such technologies would create a two-tier society, i.e., between those who had been enhanced and those who had not been. The consortium also assumed that one impact would be conflict between the enhanced and the unenhanced.

The authors considered various technologies around which we could write our scenarios. We wanted different types of technologies that raised different ethical issues. We also sought to make use of the case studies that we had done in the first stage of the project. After some discussion, we agreed to develop scenarios involving the following:

- Biometrics. We assumed that the reliability of biometrics (such as DNA) would continue to improve rapidly in their reliability and diffusion.
- 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.

[4] "Citizen-consumer" is a construction of Ofcom, the UK communications regulator. See [20].

[5] By "provoke", we mean that the scenarios should be framed in a way that makes policymakers (and other stakeholders) realise that they need to give urgent consideration to the ethical issues that arise from new technologies. We use the term "provoke" to suggest that we are seeking a response from policymakers and stakeholders to our scenarios.

- 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.

3.2. Identify key ethical issues likely to arise

Having identified the technologies, the partners then identified and discussed a range of different ethical issues that these technologies could provoke. These brainstorming discussions took place in face-to-face meetings of the partners as well as in Skype conference calls. We created a spreadsheet with several 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 (e.g., where data collected for one purpose is used for other purposes) and chilling effect (e.g., where people feel inhibited by the pervasiveness of surveillance.

The authors 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 DNA 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, less than two pages long, 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.

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 with different contextual factors that could be situated in four different quadrants in an orthogonal relationship to each other as follows mentioned above.

Having discussed and agreed the parameters of the scenarios, the partners constructed the following four scenarios.

4. Privacy is dead. So what (yawn)?

4.1. Type of scenario: Dark scenario (Quadrant 1)

This dark scenario describes a future wherein corporations and governments manipulate and control citizen-consumers to the point where citizens don't much care about privacy or the related ethical issues.

4.2. The scenario

The scenario describes a typical day in the life of Katherine, a citizen totally accustomed to new developments in the field of ICTs, who takes the full benefit of such innovations without caring for their downsides.

On a Saturday, 3 or 4 years in the future, after a hard week's work as an estate agent, Katherine aims to enjoy herself shopping and going out with her friends to a dance club. She uses public transportation to go to the shopping district. Her smartphone is equipped with near field communication (NFC) technology. It automatically proceeds to the payment as soon as she passes close to a reader. Once the transaction is completed, she immediately receives an advert on her smartphone with offers for different types of transport tickets.

Since NFC technology was first introduced as a means for mobile payment (it started in public transportation systems) a few years ago, tremendous progress has been achieved especially in terms of database interoperability. In e-government, the government has centralised its databases. There is thus a massive aggregation of data from and/or about bank accounts, health records, ID cards, population registers, marital status, social entitlements, as well as DNA and biometric information. All of this information is stored in the NFC chip in Katherine's smartphone, and is accessible to any smartphone reader.

As a cost-savings measure, the government has gradually sub-contracted to private companies many of its public services, as well as the associated operations (data collection, aggregation, mining, profiling). With access to massive sets of data, private companies can better target advertising.

Like many of her friends, Katherine uses a personal online shopping application to reserve items. As soon as she enters the first shop, her smartphone is read at a distance by RFID readers, which precisely indicate to her in which part of the store they are located. Because all of 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 access to it.

When she returns 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. An industry expert and a privacy activist are in the middle of a heated debate. The activist 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 points out the intrusiveness of this technology, its processing of huge quantities of personal data. Consent is absent. Other

principles such as data minimisation, data quality and purpose specification are mindlessly violated.

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? Personalised advertising, he argues, is a typical case of power inequality where citizens are at the mercy of opaque systems. Such power inequality can and does result in discriminatory practices based upon their income and social status. He criticises the collusion between government and private businesses in the aggregation and processing of vast amounts of data from hundreds of different sources.

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.

4.3. Ethical dilemma

This scenario highlights the ethical dilemma raised by the conveniences offered by new technologies and the sacrifices made in privacy. Should policy-makers and privacy advocates be concerned that citizen-consumers do not regard privacy as very important, certainly not as important as the conveniences offered as a consequence of massive data aggregation, data mining and profiling? Or is putting such a question to a policy-maker, like asking the fox if the chicken coop needs more protection? The scenario 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.

5. Bionic soldiers

5.1. 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). The scenario highlights popular pushback against a two-tiered society of enhanced citizens and "ordinary", non-enhanced citizens.

5.2. The scenario

Two weeks ago, the chairmen of the country's two largest political parties approached Carl, a respected military expert. They were asking for his opinion on draft legislation aiming to reregulate the prescription and usage of pharmaceutical and technical human enhancement. In recent years, everyone accepted for army recruit training was given a so-called performance-enhancing kit. Many soldiers used drugs such as Ritalin or modafinil 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 a widely used drug called *NH*, i.e., a neuro-enhancer, developed by and exclusively produced for the military. NH not only increases one's focus and alertness, it induces calm. Although he would never admit it in public, Carl 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 the soldier's one and only family.

Soldiers are also entitled to an implanted *wonder chip*, which is not only a unique identifier and tracking device – which could be a life-saver if a soldier is kidnapped – 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 webpages from the military make information and knowledge ubiquitously accessible. However, navigation through the matrix is mind-controlled and, thus, needs to be learned and constantly improved in numerous training sessions. Soldiers are increasingly relying on that visual piece of information they get from the matrix.

Carl's friend William, a university professor, told him recently that he had spotted a group of his students taking NH in order to improve their test performances. Upon closely questioning them, William discovers that these students are the children of high-ranking army officials who had given NH to their children. He also found out that one of the older students who had already served in the army still has a wonder chip implant which explains why he is an exceptional student far beyond his peers.

Instead of calling for a ban on enhancement, William has argued with Carl that the market for enhancement products, such as NH and the wonder chip, should be opened up, so that civil society could enjoy the advantages of such developments, an argument that found many supporters, not only in the UK, but across Europe.

The main reason Carl is against any legal changes with regard to the exclusiveness of human enhancement products for the military has always been for national security. What would happen if terrorists or hostile nations could profit from these developments if they were available on the open market? Carl isn't convinced by the social equity argument William had put forward. Carl is more concerned that these human enhancements are the first steps towards creating cyborgs. Despite Carl's misgivings, however, the defence industry welcomes a new mass market for their products.

The arguments for and against human enhancement seem to be equally balanced. Recognising that polarisation in society between the enhanced and not-enhanced might lead to dangerous societal consequences, William wants to achieve enhancement for everyone, while Carl favours enhancement only for soldiers in order to prevent civilians from becoming cyborgs.

5.3. Ethical dilemma

This scenario highlights the ethical dilemma and the social tension that arise when society has two types of individuals, those who have been enhanced and those who haven't, especially between the military and civilians. Should social equity prevail, so that all citizen-consumers can be enhanced, if they so choose? Can society justify two classes of individuals, those who have been enhanced and those who haven't been? How great could the risk be that terrorists or hostile militaries might also eventually obtain such enhancements? After NH and the wonder chip, what other enhancements might be adopted? Are these enhancements also mind-altering? In addition to social equity, the scenario raises other ethical issues, notably

fairness and power asymmetries, as well as societal security issues.

6. DNA sensitivities

6.1. 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 biometric technologies and who should have access to such data.

6.2. The scenario

Laura, 45 years old, is an accountant for a large company. 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 2017, AD is a growing concern. The disease currently affects approximately 15% of the population aged 65 years and older, and almost 60% 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.

Louisa is in an experiment where she has been given a new device developed to help AD patients deal with 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, the watch vibrates and displays the person's name. This can help Louisa to remember the name of the person at whom she looks.

Since her mother has been diagnosed with AD, Laura decides it would be prudent if she also takes a test that detects early-onset 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 takes the test and discovers that she is also facing the onset of AD. The children of AD patients can suffer physically and emotionally as their parents are no longer able to look after themselves. Laura 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.

However, the insurance company rejects her application form. It gives no reason for rejecting her application. Laura suspects a link between the AD screening service and the insurance company. She contacts Nigel, an investigative journalist, who finds out that an employee of the AD screening service provider has been selling test results to the insurance company.

The national daily newspaper for which Nigel works publishes his "scoop" about undisclosed discriminatory practices in the health insurance market. The story causes widespread public indignation. The newspaper follows up with a front-page leader about biometrics being used as a key to link sensitive personal information from different sources. The government also decries such practices and hastens to 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 health-care sector services.

6.3. Ethical dilemma

The scenario highlights the sensitivity of biometric data, such as DNA, but, acting responsibly, the government, with the support of many companies, sees the damage that illegal use of DNA causes to privacy, such as when insurance companies gather personal data and use it to discriminate against certain individuals (those with Alzheimer's or with a strong possibility of getting the disease). The theme running throughout the scenario is responsibility and the lack thereof. The scenario leads to the purloining and use of sensitive medical data without the consent of those from whom the data came. While some individuals and organisations may act irresponsibly, the government here acts responsibly, assures the electorate that immediate action will be taken to curb this form of discrimination. The National Health agency also acts responsibly and decides to launch a stakeholder consultation on ensuring responsible identity management and the protection of anonymity in healthcare sector services.

7. Dragonfly drones

7.1. Type of scenario: Democratisation of surveillance (Quadrant 4)

This scenario depicts an example of the democratisation of surveillance: 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 wrong-doers.

7.2. The scenario

Police superintendent Max Eggleton is on his way to an interview with a journalist from the *Daily Post*. As he looks out the taxi window, he sees innumerable tiny dots – dragonfly drones – flying above people's heads on the street, streaking over cars and hovering around windows. Eggleton recalls how the US Federal Aviation Authority (FAA) and European Aviation Safety Agency (EASA) relaxed rules in 2015 surrounding the use of unmanned aircraft systems, which resulted in an explosion in the numbers of these tiny aircraft. The Highways Agency began using drones to monitor traffic flows; 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. Increasing numbers of ordinary citizens have been able to afford dragonfly drones, the drop in prices of which has accounted for the biggest proportion in the proliferation of drones.

Many citizens use drones relatively harmlessly to monitor and record their lives and activities. Eggleton has seen wedding photographers using drones to record videos. Sports professionals use small drones 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, other citizens are using these drones for more sinister purposes. 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.

Eggleton meets the journalist in the bar of a hotel just off Journal Square. As expected, she asks why he is calling for better regulation of these devices. Eggleton responds that, "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 the 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 meet such rigorous oversight requirements, with the effect that many citizens are infringing upon one another's privacy and fundamental rights through covert surveillance and protecting criminal networks."

The journalist asks how drones have been protecting criminal networks. Eggleton answers, "Drones are currently being used to monitor the spaces in which crimes are being committed, the properties in which criminals are conducting business and the homes in which they live. 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 in advance of a police raid."

He continues, "The use of dragonfly drones by citizens has another consequence: Criminals are using drones to monitor police activities, procedures and habits. Criminals can judge whether to fight or flee by using intelligence gathered from drones to assess 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."

The journalist says that industry lobbyists point out that it is individuals who are committing these offences, not the drones themselves. In fact, many consumers use drones responsibly for recreational activities. 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.

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 accountable for how their activities may infringe upon privacy and other fundamental rights, and to keep drones out of the hands of those who may be seeking to use them for criminal purposes. We need to have some kind of assessment of the impacts these dragonfly drones are having on our society, some wide discussion or consultation with everyone who has an interest."

7.3. 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 them, because they can use dragonfly drones to surveil and evade the police. While policy-makers want to regulate such technologies, they are facing a lot of pressure from manufacturers and vendors who tell them to "get off the back" of the free market, to stop over-regulating. 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.

8. An analysis of four ethical dilemma scenarios

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.

8.1. Bjork–Schwartz methodology

Drawing on Peter Schwartz, Staffan Björk [21:2] 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.[6]

Several of these points are relevant to ethical dilemma scenarios such as those above, e.g., identifying the focal issue and determining the time frame, key factors, evaluating the

[6] Bjork's list of key points appears to have been adapted from Schwartz [1: 241–247].

focal question. Other points are less relevant – i.e., searching the unknown forces behind the key factors and organising forces in scale of importance and uncertainty.

8.2. SWAMI's deconstruction methodology

Scenarios can be analysed (or deconstructed) according to several criteria, as Schwartz and Björk indicate. The SWAMI methodology is helpful here. The SWAMI consortium[7] 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.[8]

8.2.1. 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 (normative, exploratory) and key assumptions (e.g., intelligent technologies will be embedded everywhere in rich countries, but not in poor countries).

8.2.2. Identifying the technologies and/or devices

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

8.2.3. 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.

8.2.4. 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).[9]

8.2.5. Issues

Next, the major issues raised by the scenarios are identified and explicated. In the SWAMI scenarios, the issues of concern were 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.

8.2.6. 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 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.

8.3. ENISA scenario analysis

The European Network and Information Security Agency (ENISA) built on the SWAMI methodology[10] 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 included:

- *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?

8.4. 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)"].

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

[8] This concise description of the SWAMI methodology has been extracted from Wright [22:481–482].

[9] Schwartz [1: 101], says "The process of building scenarios starts with the 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 the "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).

[10] See, for example, the credit given to the SWAMI methodology in ENISA [23: 26].

8.4.1. Framing the scenario

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

8.4.2. 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).

8.4.3. 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.

8.4.4. 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 five years into the future as demonstrated by the fact that a privacy advocate gets some air time on television and argues his case forcibly, even if it falls on deaf ears in Katherine's case.

8.4.5. The privacy risks

The privacy risks are not something to which she gives any thought. 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, to free will, that free choice is compromised as 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.

8.4.6. 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.

8.4.7. The controls

The scenario seems to suggest that there are few controls in place five 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.

8.4.8. 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 is 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 "brainwashed" that many stakeholders may no longer see the point of an impact assessment.

9. The way forward: Privacy and ethical impact assessment

Until now, scenarios have not been used much (at all) in privacy and ethical impact assessments, although they have been used in other forms of impact assessment. However, the PRESCIENT partners advocate such use. In particular, the project partners advocate "what if" scenarios, such as those set out in this paper, as a useful tool in identifying privacy and ethical issues arising from the development and deployment of new and emerging technologies. Scenarios can help to draw these issues to the attention of policy-makers and decision-makers. They are intended to provoke (stimulate with a sense of urgency)

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.

An important novelty of the approach suggested in this paper is that it differs somewhat from the approach adopted in virtually all privacy and ethical impact assessments – i.e., typically privacy and ethical impact assessments are used with regard to the development of a specific new technology, programme or service. While scenarios can be used to illustrate issues that could arise in connection with a specific technology, the approach suggested here can also be much more forward-looking, i.e., it can also be applied to technology developments that aren't even on the drawing board yet. It can be applied to situations and ethical issues that might arise with prospective technologies that are moving from the realm of science fiction to physical reality or from a class of technologies (e.g., human enhancement).

In many of his documents on risk analysis and management, Ortwin Renn [24: 7] implies that scenario construction is an inherent part of risk governance: "Assessment starts with the respective risk agent or source and tries to both identify potential damage scenarios and their probabilities." Indeed, the whole point of risk governance, or the use of risk as a decision-making modality is foresight. Scenarios are one of the techniques of foresight and, more specifically, part of what we could refer to as societal foresight, or foresight of societal issues (rather than strictly physical risks).

The PRESCIENT scenarios are not probabilistic, trying to figure out causalities, rather they are narrative scenarios sketching some broad ethical issues that might arise from the use of ICTs. In that sense, they are modelling exercises of novel societal issues that arise from the use of ICTs. Ethical dilemma scenarios used in conjunction with privacy and ethical impact assessment help to overcome a particular problem with the development of many complex technologies. Many people may be involved in technology development today so that an involved individual might see herself as responsible for only a part of the technology development (and perhaps only partly responsible for particular consequences), but not for the whole process. This raises issues of responsibility and accountability, which need to be discussed by those stakeholders who have an interest in or are affected by the new technologies. A privacy and/or ethical impact assessment can be used to address these issues in a holistic way.[11]

In most, but not all of the scenarios, a privacy and ethical impact assessment 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 remains an important instrument. Similarly, when Laura (in the DNA scenario) finds out that she has been refused insurance because the insurance company discovered she had incipient Alzheimer's disease, she goes to a journalist to spell out her suspicions about the illegal use of 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 combating discriminatory practices. And, as just mentioned, a responsive government is also important.

The authors believe this paper to be timely in the context of the debates surrounding the General Data Protection Regulation proposed by the European Commission in January 2012. Article 33 proposes a mandatory "data protection impact assessment" where data processing presents risks to data subjects (individuals). However, the authors believe that new technologies raise ethical issues beyond simply privacy and data protection and commend the use of scenarios and ethical impact assessments to highlight these issues and, in consultation with stakeholders, to identify possible solutions.

[11] A description of the PRESCIENT-proposed privacy and ethical impact assessment methodology can be found in PRESCIENT Deliverable 4 at http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT_deliverable_4_final.pdf./

Acknowledgement

This paper is based in part on work undertaken by the authors in a European Commission-funded project, called PRESCIENT (Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment, grant agreement no. 244779). The views in this paper are those of the authors alone and are in no way intended to reflect those of the European Commission.

References

[1] P. Schwartz, The Art of the Long View, John Wiley & Sons, Chichester, 1998. (first published 1991).
[2] M. Godet, The art of scenario and strategic planning: tools and pitfalls, Technol. Forecast. Soc. Chang. 65 (2000) 3–22.
[3] J.P. Gavigan, F. Scapolo, M. Keeanan, I. Miles, F. Farhi, D. Lecoq, M. Capriati, T.D. Bartolomeo, A Practical Guide to Regional Foresight, IPTS, Seville, 2001.
[4] In: D. Wright, S. Gutwirth, M. Friedewald, et al., (Eds.), Safeguards in a World of Ambient Intelligence, Springer, Dordrecht, 2008.
[5] B. Masini, J.M. Vasquez, Scenarios as seen from a human and social perspective, Technol. Forecast. Soc. Chang. 65 (2000) 49–66.
[6] H. Kahn, A.J. Wiener, The Year 2000: A Framework for Speculations on the next Thirty-Three Years, Collier Macmillan, London and New York, 1971.
[7] J.C. Glenn, The Futures Group International, Scenarios, Futures Research Methodology Version 3.0, in: J.C. Glenn, T.J. Gordon (Eds.), The Futures Group International, Washington, D.C, 2009, (http://www.millennium-project.org/millennium/FRM-V3.html).
[8] O. Da Costa, M. Boden, M. Friedewald, Science and technology roadmapping for policy intelligence: lessons for future projects, in: M. Potůček, B. Slintáková (Eds.), The Second Prague Workshop on Futures Studies Methodology, CESES FSV UK, Prague, 2005, pp. 146–161.

[9] S. Venier, E. Mordini, M. Friedewald, P. Schütz, D. Hallinan, D. Wright, R.L. Finn, S. Gutwirth, R. Gellert, B. Turnheim, A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies, Deliverable D4, Final Report of the PRESCIENT consortium to the European Commission, 25, Mar 2013. (http://www.prescient-project.eu/prescient/inhalte/documents/deliverables.php);
E. Kenneally, M. Bailey, D. Maughan, A framework for understanding and applying ethical principles in network and security research, in: R. Sion, et al., (Eds.), Proceedings of the 14th International Conference on Financial Cryptography and Data Security, Springer-Verlag, Berlin, 2010, pp. 240–246.
[10] D. Dittrich, E. Kenneally, M. Bailey, A. Burstein, K.C. Claffy, S. Clayman, J. Heidemann, D. Maughan, J. McNeill, P. Neumann, C. Scheper, L. Tien, C. Papadopoulos, W. Visscher, J. Westby, The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, Cyber Security R&D Center, Menlo Park, CA, 2011.
[11] M. Dreyer, O. Renn, S. Cope, L.J. Frewer, Food Control 21 (12) (December 2010) 1620–1628(http://www.sciencedirect.com/science/article/pii/S0956713509001509).
[12] D. Wright, A framework for the ethical impact assessment of information technology, Ethics Inf. Technol. 13 (3) (2011) 199–226(First published, online 7 July 2010).
[13] J. Kuzma, J. Paradise, G. Ramachandran, J.-A. Kim, A. Kokotovich, S.M. Wolf, An Integrated Approach to Oversight Assessment for Emerging Technologies, Risk Analysis 28(5), 2008.
[14] B. Hofmann, On value-judgements and ethics in health technology assessment, Poiesis Prax. 3 (4) (December 2005) 277–295(Published online: 14 April 2005).
[15] M.A. Weingarten, M. Paul, L. Leibovici, Assessing ethics of trials in systematic reviews, BMJ 328 (Apr 24 2004) 1013–1014.
[16] M. Decker, Interdisciplinarity in technology assessment: implementation and its chances and limits, in: C.F. Gethmann (Ed.), Wissenschaftsethik und Technikfolgenbeurteilung, Springer, Berlin, 2001.
[17] C.F. Gethmann, Participatory technology assessment: some critical questions, Poiesis Prax. 1 (2002) 151–159.
[18] E. Palm, S.O. Hansson, The case for Ethical Technology Assessment (eTA), Technol. Forecast. Soc. Chang. 73 (2006) 543–558.
[19] I. Székely, M.D. Szabó, B. Vissy, Regulating the future? Law, ethics, and emerging technologies, J. Inf. Commun. Ethics Soc. (JICES) 9 (3) (2011) 180–194.
[20] S. Livingstone, P. Lunt, L. Miller, Citizens, consumers and the citizen-consumer: articulating the citizen interest in media and communications regulation, Discourse Commun. 1 (1) (2007) 63–89.
[21] S. Björk, Designing Mobile Ad Hoc Collaborative Applications: Scenario experiences with Smart-Its, Position paper at the Mobile Ad Hoc Collaboration Workshop at CHI, 2002.
[22] D. Wright, Alternative futures: AmI scenarios and minority report, Futures 40 (5) (2008) 473–488.
[23] ENISA, Being Diabetic in 2011: Identifying Emerging and Future Risks in Remote Health Monitoring and Treatment, European Network and Information Security Agency, Heraklion, 2009.
[24] O. Renn, Risk Governance – Coping with Uncertainty in a Complex World, Earthscan, London, 2008.

David Wright (david.wright@trilateralresearch.com) is Managing Partner of Trilateral Research & Consulting, London.

Rachel Finn (rachel.finn@trilateralresearch.com) is an Associate Partner at Trilateral.

Raphael Gellert (raphael.gellert@vub.ac.be) is a PhD candidate and member of the interdisciplinary Research Group on Law Science Technology & Society (LSTS) at the Vrije Universiteit Brussel (VUB).

Michael Friedewald (Michael.friedewald@isi.fraunhofer.de) is the Head of the ICT Research Unit at Fraunhofer Institute for Systems and Innovation Research in Karlsruhe, Germany.

Philip Schütz (philip.schuetz@isi.fraunhofer.de) is a PhD candidate and researcher in the ICT Research Unit at Fraunhofer Institute for Systems and Innovation Research in Karlsruhe.

Serge Gutwirth (serge.gutwirth@vub.ac.be) is a Professor of Law and Director of the Research Group on Law Science Technology & Society (LSTS) at the Vrije Universiteit Brussel (VUB).

Silvia Venier (silvia.venier@cssc.eu) is a researcher at the Centre for Science Society and Citizenship (CSSC), Rome.

Emilio Mordini (emilio.mordini@cssc.eu) is the Founder and Director of the Centre for Science Society and Citizenship (CSSC), Rome.