

**The Landscape and Isobars of European Values in Relation to Science and
New Technology (ValueIsobars)**

Project number: 230557

Work package: 5

Deliverable 1

**Introductory Overview of
Ethical Issues and Values
Relating to Two Technologies**

Maastricht University (Unimaas)

Introductory Overview of Ethical Issues and Values Relating to Two Technologies

Dr Laurens Landeweerd (with David Townend)

Contents

1. General introduction
2. Value-related issues in biometrics technologies
 - 2.1 Introduction
 - 2.2. Actors and drivers
 - 2.3 Overview of morally relevant distinctions with regard to biometrics technologies
 - 2.4 Values pertaining on biometrics
 - 2.5 Some notions on privacy and security
 - 2.6 Cases
 - 2.7 Questions and issues to be addressed
 - 2.8 Literature
3. Value-related issues in dual use of pathogen research
 - 3.1 Introduction
 - 3.2 Actors and drivers
 - 3.3 Overview of morally relevant distinctions in the dual-use dilemma
 - 3.4 Values pertaining on dual-use
 - 3.5 Two pox cases; small pox and mouse pox
 - 3.6 Questions and issues to be addressed
 - 3.7 Literature

1. General Introduction

Value-informed governance can be regarded as an alternative for more direct participatory approaches in governance. The general aim of Value Isobars therefore consists of identifying what values are, what role(s) they take in public discourse and how they can be translated into advice for governance; This would not only include those issues where there is possible public resistance or unease to the development and introduction of new technologies, but also in the identification of possibly missed opportunities due to lack of knowledge of the values that are in play in the public consciousness.

To provide a practical setting for the findings of the Value Isobars project, Work Package 5 (WP5) prepared introductory overviews of ethical issues and values that focus on two case areas: the current debate on the introduction of various biometrics technologies to society; and, the current debate on dual use problems in pathogen research. To assess the value-related issues emerging from these two areas, we gathered information on three levels:

1. current literature in bioethics
2. newspaper articles and other resources in popular media
3. internet fora, websites and other virtual media

On the basis of this material, we prepared overviews of societal debates on both areas.

WP5's products are informed by the research conducted in WP1, and is informative for WP2, WP3 and WP4. With regard to WP1, we aimed to suggest which issues might be interesting in this area in the Eurobarometer; to WP3, we gathered information on public discourse, value-sensitive issues that are discussed in the public media and we gathered a series of case areas that may serve as starting point for public dialogue; to WP4, we mapped sensitive value-sensitive issues that are relevant for both hard and soft law.

WP5 provides the overview of the two case areas to bind the results of the other WPs together. It will also provide specific test cases in these case areas. These test cases will demonstrate the potential of a value-informed approach to governance and will aid in addressing value-related issues of governance in science and technology.

2. Value-related issues in biometrics technologies

2.1 Introduction

Biometrics technologies are the subject of wide societal debate. For the public, the most obvious example of biometrics technology is the increased use of high-tech instruments in security and immigration procedures at airports and other ports. However, biometrics is an umbrella term for all technologies that identify a person on the basis of his or her biological traits or behavioural characteristics. According to Mordini and Massari:

“[...] any biological or behavioural characteristic [of a person] can be used as a biometric identifier providing it satisfies at least four basic requirements: 1) collectability (the element can be measured); 2) universality (the element exists in all persons); 3) unicity (the element must be distinctive to each person); 4) permanence (the property of the element remains permanent over time). Many body features have been investigated, yet for almost a century only fingerprints satisfied all these conditions.” (Mordini & Massari 2008).

With these four criteria, technologies that can be identified as biometrics technologies are quite diverse. They vary from recognition through fingerprints to genetic data, from automatic facial recognition software to pictures. They include, for example iris scans, hand geometry, face and ear shape recognition, signature dynamics, voice recognition, even computer keystroke dynamics can now be added to this list.

Digitalisation has caused an exponential growth in the number and spread of biometrics technologies. They also rendered the body ‘readable’, in terms of digital codes and ciphers (van der Ploeg, 1999). It adds to Mordini and Massari’s definitions a fifth element - that the biological characteristic is recordable and that the technology is relatively time and financially economic and user-friendly¹. This readability carries several ethical issues, ethical economies alongside time and finance.

The emerging discussion on the harms and benefits of biometrics technologies mostly focuses on the tension between the right to privacy and issues of security². Most importantly, there are concerns over the role of biometrics technologies in the creation of a so called ‘surveillance society’. A ‘surveillance society’ is a society in which governments and other institutions control their subjects through a variety of surveillance technologies.³ In such a society, it is argued, surveillance slips from being a means of keeping track of crime and terrorism to being an end itself. An underlying issue is that data collected for one specific

¹ For example, whereas it is possible to DNA test all the passengers for a commercial passenger flight, the sheer numbers involved make the time and cost prohibitive.

² Although the debate is often seen as either privacy or security in particular circumstances, it can be argued that security is part of privacy.

³ See for example *A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network* (2006)

purpose may unintentionally or without authorisation be used for entirely different purposes within an umbrella aim of, for example, 'war on terror' or on criminality, and from there be used for other 'worthy' purposes of the state, often outside the democratic purpose⁴. This shift of function, also referred to as 'function creep' (Woodward et al. 2001-1), does not merely pose a problem for privacy in security applications of biometrics, but also in commercial applications. In the private sector, uses of personal data that potentially pose a threat for personal privacy include multiple uses of data collected by private companies such as banks, insurance companies and uses of information for marketing purposes. This shows the extraordinarily difficult balance that has to be struck: in order to participate in, for example, modern insurance: should an applicant's genetic information be available to the insurance industry in its risk assessment, for either purposes of identifiability or health assessment? And if the applicant is made aware of genetic conditions through, for example, his or her participation or someone else through his or her close relative's participation in medical research, should that knowledge be required to be disclosed in insurance contracts as an issue of fairness to the insurance company? Should information that is gathered for security purposes be used in the planning of health services or vice versa, both in the public and private sector? Is 'consent' and freedom of contract a sufficient safeguard to the individual's dignity, or is the over enthusiastic protection of the individual an equal assault on his or her dignity? What constitutes a 'misuse of data' and a breach of privacy in these circumstances? Commercial misuse of biometrics data seems to be an equally more widespread problem, although the consequences of misuse of data for security purposes are often seen as more problematic.

It is easy to paint biometrics technologies as necessarily drawing all societies towards bleak Orwellian dystopia. However, biometrics technologies can be useful since they are more reliable forms of identification of the individual, and this could equally be desirable for the protection of privacy for some who fear (or experience) identity theft. The technologies can facilitate a more effective and protected participation in society. More positively still, biometrics may aid in avoiding mistakes or improving access in an increasingly complex health care system. They can facilitate in making access restriction to sensitive research materials more watertight, and help protect the interests of industry and corporate business. Still, all these beneficial applications come at a risk - there are desirable, 'proper purposes' for the technologies in free societies. A problem lies in containing the use to the defined 'proper purposes', and ensuring that the definition of proper purposes is democratic and that the purposes resonate in society, respecting human dignity.

2.2 Actors and drivers

There are three important drivers for the development and introduction of biometrics technologies:

1. National security. After the terrorist attacks in the United States of America of 11th September 2001, the threat of terrorism became a prime motive to boost international

⁴ See Giorgio Agamben's "state of exception" *Stato di Eccezione*. Torino: Bollati Boringhieri. 2003 (translated by K Attwell, University of Chicago Press, 2005).

security measures. This included the further development and introduction of biometrics technologies.

2. Applications for personal identification in industry and corporate business also form an important driver behind innovation of biometrics technologies

3. Biometrics technologies also know numerous commercial applications: it makes it possible to target specific consumer groups.

Actors in these developments can be identified to include a wide population and diverse interest groups: for example, governments, the military, secret services, civil aviation authorities, police forces, private security and investigation companies, researchers/scientists, banks and insurance companies, marketing companies, employers, and, of course, the developers of the technologies themselves.

2.3 Overview of morally relevant distinctions with regard to biometrics technologies

Under this heading, WP5 identified some technically and morally relevant distinctions with regard to diverse biometrics technologies and their purpose.

Technology related distinctions (concepts specifically related to the technologies)

1. All biometrics data contain three elements:
 - a. a device that scans biological, physiological or behavioural traits. These traits need to be:
 - i. common in the population
 - ii. unique per person
 - iii. stable through time
 - b. a device that translates the information gained into digital data
 - c. a databank that enables comparison as well as being open for storage of new data.

2. The nature of the data in question. This depends on the data collected, but also on the translation medium used as well as the user himself, (e.g.):
 - i. Fingerprints
 - ii. Genetic data
 - iii. Keyboard user patterns
 - iv. Voice patterns
 - v. Facial recognition software

The following aspects of biometrics technologies have a specific relevance for the moral analysis

1. The way in which the data was collected as well as where it is stored, and by which parties.
 - a. Known / unknown to the subject in question
 - b. In a public or private setting
2. The purpose of the collected data
 - a. Exclusion and security purposes
 - b. Identification for health purposes
 - c. Identification for commercial purposes

Under some conditions biometrics data could be used for other purposes. Conditions:

- i. A shift of use can be planned or unplanned
 1. by the original user
 2. by secondary users
 - ii. A shift of use can be legitimate or illegitimate?
3. The effectiveness of the technology in question with regard to its purpose:
biometrics aims to reduce fallibilities of subjective, human identification methods by the use of computers. However, all biometrics systems rely on probabilities, and have their own internal fallibilities⁵:

is biometrics technology as reliable as it purports to be?

how should one react when the technology gets it wrong?

In the face of such problems, most proponents of biometrics technologies assume biometrics data and data use is accurate and efficient. This may only lead to an illusion of effectiveness and an illusion of safety, whilst perpetuating or causing serious disadvantages and harms.

- a. Biometrics data aimed at identification in general
 - i. Biometrics data aimed at exclusion, to exclude certain subjects from access (to a building, a factory, a research institutions), but such exclusion can be fair or unfair.
 - ii. Biometrics data are fallible. There can be:
 1. false positives, wrongly allowing access to whatever the biometrics system is designed to protect; or,
 2. false negatives, in which case someone who is entitled to access is denied access.
- b. What systems are in place to deal with challenges to the evidence of the biometrics technology (this is not just at the point of access issue: for example, the use of biometrics technology evidence in court proceedings).

⁵ In for instance the UKPS Biometrics trial, a woman tucked her hair behind her ears between the enrolment and the verification process, which caused the facial recognition system to fail (Wickins 2007; UK Passport Service 2005; pp. 239). Similarly, spectacles (in the case of retinal scans), fringes etc., can pose a problem for biometrics technologies.

4. The user: who uses the data: commercial interest, national security interests, health interests
 - a. What intention does a user have?
 - b. How can he contain that use?
 - i. Issue of responsibility
 - ii. Issue of risk of function creep or unintended use:
 1. by governments (secret service, with an aim to overprotection etc.)
 2. by other parties such as those with commercial interests
 3. by malevolent private parties (psychopaths, sentenced criminals)

2.4 Values pertaining on biometrics

Security and/vs privacy, human dignity, autonomy, liberty, democracy.

- Autonomy
- Human Dignity
- Liberty
- Privacy: can briefly be defined as a right of the individual to have a part of life that does not require accountability to others (be that individuals or the state); it is an interface between the individual and society, defining the point at which others have no right of interference with the life of the individual; the separation between public and private. This can be expressed as a conflict. However, the question arises as to how far the public interest (for example, in security) is in opposition to the individual's privacy, or whether security is part of the privacy of an individual (i.e. that privacy is not breached by security where the security demands from the individual are legitimate, as the right to privacy is not an absolute right for the exclusion of others which the individual chooses to release for his or her own ends - privacy is also about the extent of legitimate social claims to individuality in society, especially where the individual is making demands on society for the protection of his or her interests). There are two problem areas with regard to privacy and the use of biometrics technologies:
 - The use of biometrics technologies may damage the principle of privacy: they may lead, and can in some cases be said to have already led to the creation of a 'surveillance society', in which any citizen may be criminalised. Biometrics technologies have a potential both in their nature and their use to harm the principled right to privacy.
 - Nature: biometrics technologies render the body and the person transparent to the organisation that uses the data in question. The extent of this transparency differs according to the technology or goal.
 - Use: biometrics technologies can be used as a mechanism of control over individuals (depending on the use these can be citizens, illegal aliens, clients, patients, employees, or customers). Without the knowledge or agreement of the subject in question, third parties may

use the information in question for goals the subject in question did not intend or support.

- The severity of such problems may increase through function shift or function creep: the unnoticed and often unintended gradual shift of use of data for one purpose to use of that same data for another purpose.
- The protection of privacy might hamper security measures in the light of terrorism but it might also hamper the prevention of abuse of public service, progress in health service etc. This argument resonates with the privacy vs public interest construction. However, perhaps what is really being said is that the claims regarding the particular activities (in this case in relation to security) are not seen as **legitimate** (for example, because they are not perceived as necessary or effective, or that they serve a different purpose from the published purpose for the activity); this intrusion is not seen as something by the disputant as necessary for his or her interaction with society. (To capture this resonance issue, think about the language described by the participants in on-line social network sites for their privacy when compared to other requests for their similar or less intrusive data - there is an issue of control or the decision to disclose and a desire to participate.)

How to balance these principles and values needs to be further explored.

- Security & safety: with biometrics technology, it will be much easier to identify a person. Anonymity and invisibility are increasingly perceived to be potential threatening in modern society. The ability to identify individuals more easily may aid in reducing the risk of a terrorist attack (but arguably, the constant sense of the state against the individual may be counter productive in this regard). However, there are questions about the assumption of the benefit of biometrics to security and safety:
 - Effectiveness: although biometrics technologies, due to their technological and digital nature, appear to be highly effective when compared to non-technological strategies, they may only lead to an illusion of safety, whilst carrying along serious harms to privacy and personal freedom. There is a need for a proper assessment of the effectiveness of the technologies involved and an assessment of possible unexpected or less predictable harmful side effects. States should go further in explaining the possible harms involved, there should be a positive assessment of what benefits are served and clarity in explaining how the harmful aspects are controlled and reduced.
 - Means going beyond the original goal (function creep): the goal of countering terrorism may be overreached when the means to achieve security go beyond this and the function of biometrics technologies shift to general control over citizens in modern society.
 - The problem is that the protection of national security has enjoyed a special legal position: it is almost a trump card that reduces the need to justify the activity within the normal safeguards of democratic society (the scrutiny or

parliament and open court)⁶. This lack of accountability may lead to uses without explicit purpose, and without consent. In the extreme, these uses might lead to a criminalisation of innocent citizens and damage principles such as:

- liberty
 - personal freedom
 - privacy
- Proportionality: closely linked to the questions of effectiveness and function creep, and central to the issue of legitimacy, is whether the measures undertaken in biometrics technologies are proportional to the threats they seek to remove or reduce, especially if the technologies' claims to efficiency are questionable.
 - Democracy: this again points to the problem that much of the move towards 'national security' is conducted outside the normal mechanisms of democratic safeguards. This also goes to the effectiveness of the mechanisms; resonance with the citizens, the heart of democracy, is lost when the measures are conducted in a secrecy that is not within the trust of the citizens.
 - Commercial interests: biometrics data is powerful in commerce. At the least intrusive end, it may serve to target products to specific groups of customers; at the more difficult end, it can be used in decision-making about the access of specific individuals to goods and services within society (e.g. insurance, and health care).
 - The problem here is that commercial gain may run counter to the right to privacy.

2.5 Some notions on privacy and security

Biometrics is only one form of surveillance-enabling technology. Other technologies include surveillance cameras, databases, sensors, implantable microchips, GPS, and wireless networks. Some of these can be combined with biometrics (facial recognition software and surveillance cameras; databases and information such as DNA-profiles or fingerprints; sensors and keyboard recognition patterns etc.) The threat of terrorism or criminality has been taken up as a reason to increase the application of biometrics technology and other forms of surveillance. Four standard arguments are used against the idea that biometrics data pose a problem to privacy (Alterman 2003; pp. 141):

(1) The "technical limits" argument: in a large population the technology has limited capability to identify a particular individual.

(2) The "balkanization" argument: information remains local and restricted because no interoperability standards exist (i.e. systems cannot talk to each other to allow the effective transfer of data). [However, this belief may express a false sense of security with regard to function shift or function creep]

⁶ See Agamben (2003) to consider the possibility that these 'exceptional' measures and procedures become assimilated into the normal fabric of society.

(3) The “cooperation” argument: the technology cannot easily be abused because identification requires cooperation.

(4) The “security” argument: the template algorithms are secure because biometrics vendors have a proprietary interest in keeping them confidential.

These four arguments are highly contestable. Although the threats of terrorism or criminality is not to be taken lightly, the strategies to counter these threats may not be as effective as they purport to be, and they may find other uses that are not connected to these original goals. This danger of ‘function creep’ has been considered by *Privacy International* and its work is worth considering at this point in the discussion:

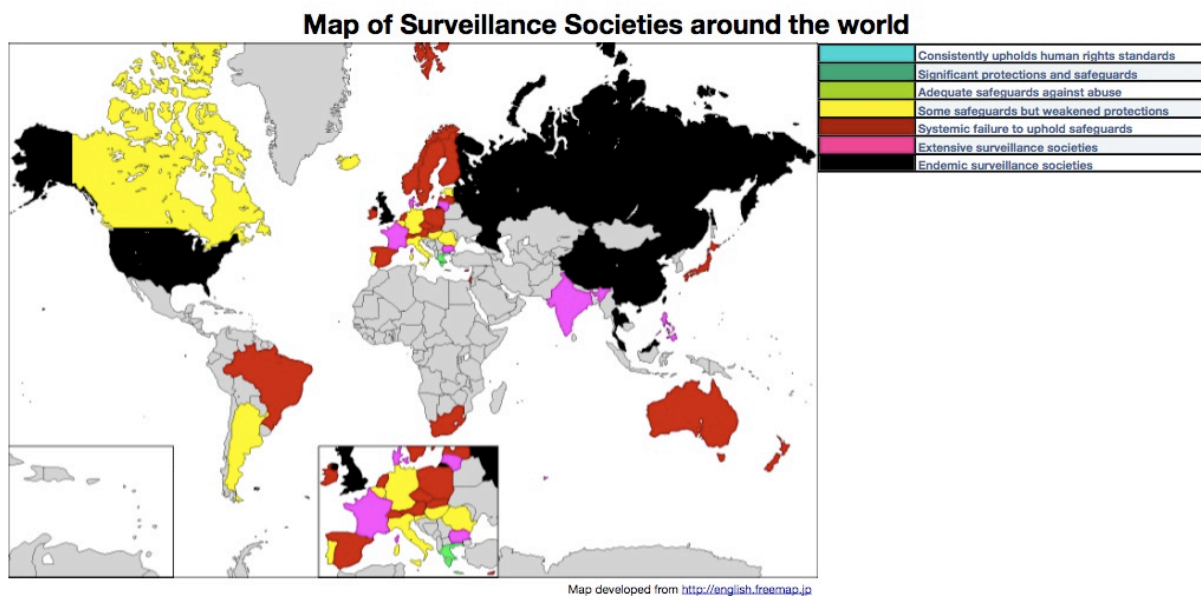


Figure 1: *Privacy International's* Map showing different countries' levels of security and privacy protection⁷.

Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London, England, and has an office in Washington, D.C.

On their 2007 findings, PI point to the following issues:

- The 2007 rankings indicate an overall worsening of privacy protection across the world, reflecting an increase in surveillance and a declining performance of privacy safeguards.
- Concern over immigration and border control dominated the world agenda in 2007. Countries have moved swiftly to implement database, identity and fingerprinting systems, often without regard to the privacy implications for their own citizens

⁷ Privacy international: <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597> (last visited on 16th August 2010).

- The 2007 rankings show an increasing trend amongst governments to archive data on the geographic, communications and financial records of all their citizens and residents. This trend leads to the conclusion that all citizens, regardless of legal status, are under suspicion.
- The privacy trends have been fuelled by the emergence of a profitable surveillance industry dominated by global IT companies and the creation of numerous international treaties that frequently operate outside judicial or democratic processes.
- Despite political shifts in the US Congress, surveillance initiatives in the US continue to expand, affecting visitors and citizens alike.
- Surveillance initiatives initiated by Brussels have caused a substantial decline in privacy across Europe, eroding protections even in those countries that have shown a traditionally high regard for privacy.
- The privacy performance of older democracies in Europe is generally failing, while the performance of newer democracies is becoming generally stronger.
- The lowest ranking countries in the survey continue to be Malaysia, Russia and China. The highest-ranking countries in 2007 are Greece, Romania and Canada.
- The 2006 leader, Germany, slipped significantly in the 2007 rankings, dropping from 1st to 7th place behind Portugal and Slovenia.
- In terms of statutory protections and privacy enforcement, the US is the worst ranking country in the democratic world. In terms of overall privacy protection the United States has performed very poorly, being out-ranked by both India and the Philippines and falling into the "black" category, denoting endemic surveillance.
- The worst ranking EU country is the United Kingdom, which again fell into the "black" category along with Russia and Singapore. However for the first time Scotland has been given its own ranking score and performed significantly better than England & Wales.
- Argentina scored higher than 18 of the 27 EU countries.
- Australia ranks higher than Slovakia but lower than South Africa and New Zealand.

2.6 Cases

Case 1: Marketing and biometrics data

Biometrics technologies may be on a par with data privacy. Simon's *NetPolicy.Com* presents a useful example of the problems that may be caused:

“Consider the case of the Texas factory worker who began to receive threatening letters filled with details of her personal life. IT turned out that a direct marketing company was using state prison inmates to process computer tapes containing detailed personal information on more than 90 percent of American households. A convicted rapist and burglar had viewed her file” (Simon 2000; also quoted in Alterman (2003)).

Alterman mentions two connected concerns: 1) there is a problem in that any party, be it the secret service or a private person with bad intentions may legitimately or illegitimately gain access to personal information, and use this to cause harm or generally tread one's right to privacy or to be left in peace; 2) there is a problem that data collected for one purpose may be used, legitimately or illegitimately, for a completely different purpose, unforeseen by the person who originally collected the data, who didn't handle the data responsibly, and that the person whose data it concerns in any case did not expect or agree to (Alterman 2003; pp. 140; Garfinkel 2000; pp 154ff; 274-275). In respect of the first part of this case, the disclosure of information about an individual for one purpose will inevitably mean that the processor of the data gains knowledge about the individual. Despite the validity of the primary purpose that requires the processor to be made aware of the individual's information, it is necessarily judged in the mind of the processor, or (in the mind of the individual who is under surveillance) his or her life is potentially being judged by the processor of the data. Even when the primary purpose is legitimate, there is a secondary, inevitable intrusion that makes some feel vulnerable. In respect of the second part, dealing with the unforeseen purpose that presents a purpose beyond the consent or knowledge of the donor subject is an enduring conundrum in data protection.

- Which norms are at play in this case scenario?
- Which ethical principles are at play in this case scenario?
- Which values conflict in this case scenario?

Case 2:

This is a composite from a number of thinkers. The US government's organisation DARPA (Defense Advanced Research Projects Agency) initiated a \$50 million program under the title "Human ID at a Distance" (Alterman 2003). Its main target is the development of biometrics technologies to "identify a known terrorist before he closes on his target" (Woodward 2001-II, pp. 10). Woodward's essay discusses the 2001 Superbowl game where Tampa police chose to use face recognition technology to compare images of the members of the crowd with those of convicted criminals - a classic presentation of the enduring case of being investigated for a crime only on the basis of suspicion rather than a presumption of potential criminality (the case being extended through the potential of biometrics technologies). As *WiredNews* notes, "fans may have resented being . . . made part of a digital line-up, but Tampa Police say the technology allowed them to pinpoint 19 people with criminal records in a crowd of over 100,000" (Scheeres 2001). "Of course, the Tampa police probably overestimated the current capabilities of the technology, and the 19 putative matches may well include false ones. This again shows that potentially intrusive uses of biometrics exist even if the "technical limits" argument is sound. Imagine, for instance, some mismatched individuals being hauled in for questioning: it would be little solace to know that the privacy of the people on the "watch list" was protected by the technical limitations of the software." (Alterman 2003).

- Which norms are at play in this case scenario?
- Which ethical principles are at play in this case scenario?
- Which values conflict in this case scenario?

Case 3:

A student from the city of Utrecht went to court because he didn't want his fingerprints to be stored on a governmental database⁸. Aaron Boudewijn applied for a new passport but refused to provide for his fingerprints. He was therefore refused a new passport. He appealed the decision to the court: "they may use my fingerprints for my passport but I don't want them to store them in a central database", he told a national paper. He claimed that this constituted a breach of his right to privacy. Furthermore, his fingerprints would become easy to reproduce, with all attached risks and consequences.

- Which norms are at play in this case scenario?
- Which ethical principles are at play in this case scenario?
- Which values conflict in this case scenario?

Case 4:

This is a hypothetical case devised by the WP5 group. The gathering of genetic information about individuals has produced increasing understanding about certain diseases in the population. The systematic gathering of genetic information through a simple saliva test at the point of application for an identity card could provide not only biometric information for the identification of individuals, but could provide an extraordinarily rich medical research database and, by extension, to the understanding of the prevalence of certain genetic conditions in the population generally. Equally, these identification and medical benefit ends could be achieved through the storing of data contained in blood samples taken from newborn children.

- Which norms are at play in this case scenario?
- Which ethical principles are at play in this case scenario?
- Which values conflict in this case scenario?

⁸ <http://www.nu.nl/binnenland/2185458/student-rechter-privacy-paspoort.html> (last visited 16th August 2010)

2.7 Fundamental questions and issues in biometric technologies that need to be addressed

What is the relationship between privacy and public interests in security and safety?

How far are the current biometric technologies effective and efficient?

What is a legitimate use of such technology, and by whom is 'legitimate' defined?

How can effective safeguards against the unauthorised use of the technologies and data gained therefrom be created and enforced such that there is trust and confidence in the public?

2.8 Literature

Agamben, G. (2003) *Stato di Eccezione*. Torino: Bollati Boringhieri. English translation: K Attwell, University of Chicago Press, 2005.

Alterman, A. (2003) "A piece of yourself: Ethical issues in biometric identification.": *Ethics and Information Technology* 5: 139–150.

Garfinkel, S (2000). *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly & Associates, Sebastopol, CA, 2000.

Mordini, E., and Massari, S. (2008). "Body, biometrics and identity". *Bioethics* 22(9): 488-98.

Murakami Wood, D. (ed.) (2006) *A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network*. Information Commissioner's Office, UK. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (last visited 16th August 2010)

Ploeg, van der, I. (1999). "The illegal body: 'Eurodac' and the politics of biometric identification". *Ethics and Information Technology* 1: 295–302.

Privacy International 2007:

<http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597> (last visited 16th August 2010)

Scheeres, J., (2001) "When Your Mole Betrays You", *Wired News*, 3/14/2001
<http://www.wired.com/politics/law/news/2001/03/42353> (last visited 16th August 2010)

Simon, L. D. (2000), *NetPolicy.Com: Public Agenda for a Digital World*. Washington, DC: The Woodrow Wilson Center Press, 2000, p. 136.

UK Passport Service (2005). Biometrics Enrolment Trial Report, May 2005.

http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec3extra/UKPSBiometrics_Enrolment_Trial_Report.pdf (last visited 16th August 2010)

Warren, S., and Brandeis, L. (1890). "The Right to Privacy" 4 *Harvard Law Review* 193/1890.

Wickins, J. (2007) "The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification". *Science and Engineering Ethics* 13(1)

Woodward, J. D. et al. (2001-I). Army Biometric Applications, Identifying and Addressing Sociocultural Concerns. Document Number: MR-1237-A.

http://www.rand.org/pubs/monograph_reports/MR1237/ (last visited 16th August 2010)

Woodward, J. D. (2001-II) *Superbowl Surveillance: Facing Up to Biometrics*. Rand Arroyo Center. http://www.rand.org/pubs/issue_papers/IP209/ (last visited 16th August 2010)

3. Value-related issues in dual use of pathogen research

3.1 Introduction

The dual-use dilemma originally described the potential of a technology for both military and non-military uses: i.e. technologies developed for non-military uses shift in function to military applications and vice versa. After the terrorist attacks in the United States of America on 11th September 2001, 'dual use' was no longer used merely to refer to this descriptive distinction between military or non-military use - which stands separate from the question of whether either is a justified use - but it increasingly became associated with the dilemma that a piece of scientific research sometimes has the potential to be used for 'bad' as well as 'good' ends (e.g. see Selgelid 2007; Selgelid 2009). Here, we include this latter aspect⁹. Miller and Selgelid state the main dilemma of dual use is how to prevent misuse without foregoing beneficial applications (Miller & Selgelid 2007). Unintended harmful consequences of some forms of research may also be included under the dual-use dilemma, since they may become the harmful intended consequences of third parties. Sometimes definitions of dual-use also include conflicts over use between researchers and governments, for example, when research aimed at health benefits can also be used for military purposes.

Research with a potential of dual-use aims to provide benefits but comes at a risk of misuse by rogue states, terrorists groups or criminal groups. One specific area of research with a dual-use potential is research aimed at the protection of human life and physical health against diseases (including novel diseases and pathogens such as those that may be developed through synthetic biology) which may lead to use to cause death and sickness through biological agents as weapons in the hands of malevolent groups or individuals. The implied trade-off's are not easily translated into probabilities. Research with a high risk that it will be abused but only offering a small gain in terms of benefits would be unjustified and vice versa, although the potential of strategies to reduce the risk of abuse should be included in the risk calculation, but dual-use issues hold are not easy to predict or place values upon given that the actors are outside the law and are, in many senses, invisible when making risk assessments. It's not an issue of probabilities but of risks and known unknowns as well as

⁹ For this broader definition, a paradigmatic example is the use of pathogens to derive a vaccine as the same or related knowledge can also be used to spread a disease or to enhance it. Another example is the use of the anthrax virus, sent in envelopes through the postal system to cause harm.

unknown unknowns. With regard to known and unknown unknowns the precautionary principle must apply¹⁰.

Scientific research has the potential to produce results that can be used to cause harm even though it intends to promote good. This does not necessarily mean that all technology is neutral and that good or bad intent demonstrated is only demonstrated in technology's use or application. Some technologies may be rigged for a specific use, the use being implicit in their design; some technologies may lend themselves more easily to what is considered a bad use than others, regardless of the intentions of the researchers in question.

Current discussion of the dual-use dilemma focuses very much on preventing bioterrorism, but science may also be misused in other settings, including warfare, agriculture and law enforcement. Strategies to prevent misuse are not merely to be found in stricter regulation but could also be operationalised at the level of scientific practice, information dissemination or technology applications, and the scientific community is concerned that preventive strategies will cause more harm than good, by impeding scientific progress (Miller and Selgelid 2007). The implementation of more regulations has often proved to be counterproductive and it appears to be more sensible to embed risk-reducing policies in practice than to implement regulations to that aim from outside. The question is how to do this.

3.2 Actors and drivers

With regard to current problems and policy in relation to dual-use, questions about who the most important actors and drivers are is, of course, dependent on the particular technology. We can identify several general actors and drivers, for example, when considering retention of pathogens by governments for defensive as well as offensive purposes. Here governments and the researchers themselves (individually and institutionally) are concerned with safety and security issues. Dual-use also refers to abuse of technologies to blackmail individual actors or governments, so malevolent parties can also have financial interests in the abuse of novel technologies. For other parties generally considered to be malevolent, either religious zeal or environmental zeal can be a strong driver for offensive use of certain biotechnologies. Readily obtainable animal, plant and human pathogens can be used by malevolent parties varying from rogue researchers to terrorist cells or rogue states with minimal microbiological training. More advanced techniques of genetic engineering that can enhance the virulence and transmissibility naturally occurring pathogens. Developments in

¹⁰ The articulation of the difficulty of foreseeability using the terms known knowns and unknown unknowns was famously made by Donald Rumsfeld, then US Secretary of Defense, at a press briefing on 12th February 2002. A formulation of the precautionary approach (a term often used as alternative for 'precautionary principle', see a.o. Peel, 2004): "Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation". The precautionary principle seems to be applicable mainly to issues of risk, rather than use with a bad intent. Indeed, precaution seems to be an issue of harm that occur due to unintentional accidental risks. But precaution should also include the unintentional leaking of know how to parties with bad intent. Therefore, the precautionary principle also applies to those cases in which it is uncertain whether parties with bad intentions could get their hands on certain technologies and use them to their own aims. The specific application of a precautionary approach to dual-use would involve finding out what instruments can be put to practice to safeguard good uses of certain technologies without risking bad uses.

synthetic genomics that make it possible to create pathogens from scratch. This points to the difficulty of setting policy to reduce the risks of dual use: whilst many of the actors operate within the established norms of social control and expectation, the core of the dual use problem is that other actors are willing to step outside the generally accepted norms to assert different norms and expectations in order to shift the social order to a new ground. Thus it becomes difficult to predict actions and apply dominant behavioural logic in establishing the security and safety risks. For example, the pursuit of a cause may remove a common assumption of avoiding death, either to others or self, in the mind of the actor; the actors may be invisible, placing the construction of the risk equation into the realm of shadows.

Two questions emerge in the question of the construction of norms around how to deal with possible dual uses of otherwise individually and socially valuable technologies: first, how far should the fears of the unknown influence the way a society lives with the known potentials and needs of its members? and, second how far can we assume that the dominant norms in society are the only norms in play (i.e. is it constructive to see the aims and objectives of those with 'bad' intent as immoral, or indeed 'bad' simply because it differs from the dominant norms of the society)?

3.3 Overview of morally relevant distinctions in the dual-use dilemma

Under this heading, WP5 identified (and/or collected) some technically and morally relevant distinctions with regard to dual-use.

1. The ends of the user: it depends on what the ends of the user are, but also from whose perspective we regard the use in question.
 - a. Beneficial or harmful use: researching pathogens to find a cure for specific diseases is mostly regarded as a good use but to spread a disease amongst an enemy is (now) often seen as a bad use.
 - b. Justified and non-justified use: depends on who is the group that sets the norms. What if violence is the only resource those who feel oppressed are left with? For example, whereas the language of the 'war against terror' sets certain individuals and causes as 'evil', there are many historical examples of conflicts where the aims and methods of those previously labelled 'terrorists' are re-evaluated and re-labelled as virtuous struggles.
 - c. Military or non-military use: research on pathogens for military purposes is another type of use than research on the same to cure diseases. This is sometimes also subsumed under the heading of dual-use.
 - i. Offensive or defensive military use: research on pathogens to prevent use of a rogue state to spread diseases would be defensive, research to pathogens to spread a certain disease amongst an enemy is offensive use.
 1. Offensive military use by 'the good guys' vs. use by 'the bad guys': this must be one of the most controversial uses of dual use, since any offensive use of biotechnologies for military purposes is to be considered malevolent. Still, covertly stated examples of this type of reasoning can be found.

2. The researcher: it depends on the user whether we consider something to be a bad use or not (and a central question is how far the researcher should temper his or her work to accommodate the potential of unacceptable use by others in the future):
 - a. Use intended or not intended by the researcher: a researcher may aim at curing diseases whilst someone else uses his research for terrorist purposes.
 - b. Intended application (e.g. military) but by not intended users (e.g. rogue states)

3. Perspective: it differs per person or community whether the use of pathogens to combat an enemy is justified or not:
 - a. Use by terrorists
 - b. Use by the military
 - c. Use by criminals

4. The design in question: the type of use may be implicit in the design or not. Viral strains can be produced in such a way that they will pose harm, some in such a way that they never can. Here the issue of function shift or function creep should be central.

5. The issue of 'plural-use' as distinct from 'Dual-use'

6. Forseeability
 - a. Unintended use that could have been foreseen
 - b. Unintended use that could not have been foreseen

3.4 Values pertaining on dual-use

Resolving the discussion on how to deal with dual-use is not merely a question of disentangling the information knots involved, exposing issues where insufficient information is available, and then making rational choices based on good information on any risk of bad intended use of technology. What is valued in society also plays an important role in this respect; does one value liberty in scientific research more than safety? Do these two necessarily exclude each other? Should a risk to dual-use lead to a closed mentality in scientific research or can openness of scientific research also be a means to solve these issues? Is the dual-use question a problem about the dual-use or about effective conflict resolution in society and internationally?

The following value-related areas are in play in the dual-use dilemma:

- Right to life versus risk to life: we conduct research to health benefits because people believe value the concept of a right to life highly. We have a duty to try and save lives by curing illnesses where possible. However, if the technological means to save these lives can also be used for the opposite effect, where do the duties lie?

- Research values: we attach certain values to scientific research, both with regard to its intended goals and as a field with its own intrinsic value. Scientific research has a strong independent claim against external restriction through claims to
 - freedom of inquiry
 - free speech
 - free dissemination and transparency of results

However, these are not absolute rights; the question of how to balance the science claim against other competing claims is simply another manifestation of the dual-use dilemma - how, where and by whom are competing rights claims evaluated in society and how are the decisions enforced?

- Good and bad intent; a question of perspective? Different parties in the world hold different ideas over what is good. Some parties feel they have to resort to threats and violence to reach their goals, perhaps even accepting such threats and actions as good and acceptable or necessary in themselves. Those parties that are traditionally (or perhaps more accurately, currently) considered to be 'good' from the Western capitalist perspective resorted to such means in the past as well, and in some cases still do in their present activities. Can we always make definitive and authoritative judgments of which uses and intentions are 'good', and which aren't? Who sets the norm, and sanctions certain uses and users whilst excluding others?
- Is the 'Dual-Use' debate a mechanism in modern society for enforcing the dominant social paradigms and social order? Are external, independent claims to overarching norms available that base the argument against the development of technologies that have a potentially harmful use on a universally acceptable idea of 'good' or 'bad' rather than a culturally specific claim? If there is no such universal available, then the issue moves away from the restriction of science and technologies to the construction of effective alternative dispute resolution and inclusion of diverse and conflicting cultures in the modern world.
- Prudence, precaution and issues of risk and risk perception; the dual-use dilemma is related to issues of risk of use with a bad intent. Although parties with a bad intent perhaps would not perceive their goals as a 'hazard', how far is it then incumbent upon parties responsible for research and development of novel technologies to take precautionary measures? How far should this be in proportion to the potential for technologies and products widely available through modern commerce to be sold and available largely unrestricted?
 - The precautionary principle: what are the chances of use to bad purposes? What measures should be taken to prevent use for bad intentions? How far should this be measured against other, already socially accepted risks?
- Neutral or normative nature of a technology. Common opinion is that technologies, as any instrument, are neutral, and that it is the user that renders it an instrument to either good or bad. There always was an opposing thought that some instruments are geared or rigged for specific purposes, that this includes whether they are used for a specific political goal, and that they should therefore be restricted or outlawed.

- Is the creation of an atomic bomb, land mine, etc. so necessarily linked to the destruction it would cause if it was used that those involved with the production cannot make a defensive claim that they did not pull the trigger or sanction the use? And at what point does a balance of different uses absolve the inventor and manufacturers of multi-purpose devices: is dynamite, on balance, on the absolution list? are bullets? are tanks, knives, four-wheel drive vehicles and aeroplanes? But equally, is the clothing manufacturer who exploits developing country workers, the international seed producer, or international banking system absolved from its effects upon the starving people of the developing world? And are we who participate in such trading practices by buying financial products or cheap clothing or food, absolved because the system produces good as well as bad results. Again, is the compartmentalisation of certain practices as 'dual use' simply a way of shielding other unacceptable practices from appropriate scrutiny when one tries to understand the value judgements involved in the debate?

- Medical versus military good intent: medicine has its own internal values such as alleviating suffering, saving life, curing diseases. Research conducted in this context will often be conducted by people who specifically adhered to such values (the traditional goals of medicine). The products that are developed on the basis of such research can sometimes also be used for either defensive or offensive military purposes. Who is to hold responsibility over the use of such technologies? Does the inventor hold some moral copyright on the use of his ideas?

- Distributive justice: issues of a just distribution of the risks, burdens and benefits of certain types of research. Suppose a certain important innovation in research makes it possible to cure AIDS but at the same time has a potential to release a deadly airborne variant of the virus. How high may a risk for bad intent be to restrict specific types of research? How can one weigh risks, benefits and burdens?

- The issue of rights and responsibilities: who is responsible for the dual-use dilemma? The following parties are involved and should be taken into consideration:
 - Individual researchers / research groups
 - Research institutes and funding institutes
 - Governments
 - The military
 - Etc.

- Given that some of the actors involved in dual use are claiming an exemption from social norms and mechanisms for dispute resolution, how are the norms and values in play in dual use negotiated or discussed?

3.5 Two pox cases; small pox and mouse pox

Case 1:!

The first means to prevent smallpox was a process known as 'variolation'. Healthy individuals were exposed to small samples of smallpox, giving the individual a mild form of the disease, and as a result enabling the individual to develop immunity. An early 11th Century record mentions a Buddhist nun who ground smallpox scabs into a powder which was then inhaled by a healthy subject to produce immunity. This practice spread throughout China, India, and Turkey by the 18th century. It is known that variolation was practiced in the Ottoman court. In 1796, Edward Jenner discovered that milkmaids who contracted cowpox, a milder pox virus, did not contract smallpox. He inoculated an 8 year old boy, James Phipps, with the virus, and as a result Phipps did not contract smallpox when he was exposed to it. Despite initial doubts, the practice of **variolation** spread over Europe and the United States during the **18th** century. Famous advocates of inoculation included Thomas Jefferson and Napoleon Bonaparte.

At this time, the greater understanding of the smallpox virus also led to its use as a bioweapon. In one of the first documented cases of biological warfare, in the 18th century, contaminated blankets used by smallpox patients were distributed among Native American Indians by the British with the intent of initiating outbreaks. This happened during the French and Indian Wars (1754–63), which was conducted against the French and their Native American allies (Peckham 1947; Anderson 2000). In June 1763, General Jeffrey Amherst wrote a letter to a subordinate outlining a plan to "extirpate this execrable race" by the dispensation of smallpox-infected blankets. The British gave two blankets and a handkerchief to representatives of the Delaware Indians. These had previously been exposed to the smallpox virus (Anderson 2000). It is not clear whether this attempt at biological warfare was successful (Anderson 2000; 541) but according to some sources a smallpox epidemic with a high mortality rate took hold amongst the tribes and this was attributed to the infected blankets and handkerchief. Some tribal groups virtually vanished, and the rest suffered severe population losses¹¹.

Today the smallpox virus has been eradicated except for those strains residing in laboratories. Due to this fact and past use of the virus as a bioweapon, there is heightened concern of terrorist use of the variola virus. If a terrorist group acquired a strain of the virus, a weapon could be easily manufactured and disseminated. This could result in a catastrophic global epidemic. As 'Global Security', a popular website on that issue, provides information on the history of the US - Iraq confrontations, the military forces on both sides and on possible targets puts it:

“the variola virus remains a hazardous, Category A (CDC category) biological warfare agent, meaning it has been given high priority due to its potential threat to national security. During World War II, the US and UK considered using smallpox as a weapon, but with smallpox vaccines readily available, decided smallpox would be ineffective as

¹¹ <http://www.zkea.com/archives/archive01002.html> (last visited 16th August 2010).

a weapon. During the Cold War, in 1974, the Soviet Union initiated *Biopreparat*, a civilian pharmaceutical company, as a front for the Soviet biological weapons program. Vladimir Pasechnik, a Soviet microbiologist who defected in 1989, provided information on the Soviet development of India 67 or India 1, a particularly virulent strain of smallpox, as a biological weapon. Scientists used embryonic chicken eggs to cultivate large amounts of smallpox virus. In addition, Dr. Ken Alibek (formerly Kanatjan Alikbekov), the former First Deputy Director of Biopreparat, reported the Soviet development of chimera viruses by inserting genetic material from other viruses into smallpox. Reports suggested that the North Korean biological weapons program conducted research on smallpox as a possible biological agent. Widespread fears remain that the smallpox virus can be used as a weapon of bioterrorism as populations are no longer vaccinated against the virus".¹²

- Which norms are at play in this case scenario?
- Which ethical principles are at play in this case scenario?
- Which values conflict in this case scenario?

Case 2:

In the late 1980s, Australian researchers unintentionally developed a lethal mousepox virus. The researchers in question inserted the gene for interleukin-4 (IL-4) into a mousepox virus. They hoped that the altered virus would induce infertility in mice to combat mice pests in Australia. The altered virus unexpectedly killed both naturally resistant and vaccinated mice. The researchers published the results of their research in the *Journal of Virology* in 2001 (Jackson *et al.* 2001). In this journal, they also described what materials and what methodology they had used. Open publication of research, along with methodology and materials used is considered to be an essential part of conducting science. Exceptions are, amongst others, research sensitive to industrial espionage and research for military purposes, but this research had been conducted to find a novel pest control against mice in Australia. Critics stated the open publication of their research might lead terrorist groups to develop new biological weapons: it was argued that there was only a small, technical step from research on mousepox to research on smallpox. Malevolent parties would be able to create a smallpox variant that would be resistant to any known vaccine. The original strain of smallpox was eradicated in the 1980s but there are still stockpiles in labs across the world, and one could reconstitute new versions of the virus (Selgelid 2009). The researchers acknowledged the dangerous nature of their research at an early stage. They also considered the original intent of their research to have a dual-use aspect. Sterilizing the world population might after all become a technological possibility on that basis. Terry Gilliam's dystopic scenario of an eradication of the world population in his novel *Twelve Monkeys* seems only around the corner.

¹² Weapons of mass destruction: http://www.globalsecurity.org/wmd/intro/bio_smallpox.htm (last visited 16th August 2010).

Dual use is a problem of promoting good in the context of a potential use for harm. In this case, there is a dual-use tension between promoting health and protecting food and feed production, whilst the research that aims at this may also potentially be used to kill thousands of innocents. The dilemma arises not because of the intentions of the researchers but because of possible intentions other parties may have to use their ideas to develop weapons out of dangerous biological agents to cause harm. Such parties may include other researchers. The purposes can vary from criminal use to blackmail governments or other parties, to terrorist groups using biological agents for bioterrorism, or to rogue states. But with the broader definition of dual use, military use of similar research for biowarfare may also be included (Miller & Selgelid 2007)¹³.

There are two types of potential threat with regard to research with dual-use aspects: internal threats and external threats (Miller & Selgelid 2007). Internal threats involve researchers. They may want either to use or sell dangerous agents out of resentment over being reprimanded or passed over for promotion, financial pressures, blackmail threats, psychological or personal problems, recruitment by a terrorist organization etc. External threats include criminal gains, terrorist organisations, rogue states etc. Seen the potential malevolent use of the accidental outcome of the Australian mousepox research, should the researchers have refrained from publication, and if yes, at which stage? Should the government have impeded their research? Would such measures reduce the possible insider-threat? And if the government had absorbed their research within state secrecy, how would it proceed as 'good science' (i.e. science that is scrutinized by independent peers to judge its veracity)?

- Which norms are at play in this case scenario?
- Which ethical principles are at play in this case scenario?
- Which values conflict in this case scenario?

Case 3:

The dual use nature of biological weapons makes it a difficult task to detect and stop a country that wants to develop bioweapons. In most cases, bioweapon agents are self-replicating, and even the smallest amounts can quickly generate sufficient quantities for weapon production. That a biological agent is dangerous is not in itself reason to forbid research. Dangerous agents can be used for both beneficial and harmful. Discerning the end-use of dual-use technology can be difficult. And not all agents are complex or hard to find and acquire.

The website 'Global Security' describes the situation in the following way:

"Generation of biological agents requires fermenters or single cell production capabilities. These can be used in making vaccines but that may also be effective for manufacturing biological weapons. The most technologically advanced and best-tooled fermenters are safest and most efficient – qualities that any user would desire - and may be equally desirable for weapon making and health programs. The primary

¹³ Miller & Selgelid (2007).

difference between the production requirements for biological weapons and non-military commercial purposes lies in containment and contamination. During biological agent production, efforts are generally made to avoid contaminating the environment with the organism. Less concern arises about the contamination of the product. Conversely, the pharmaceutical, brewing, and biotechnology industries are most concerned about protecting the purity and quality of the product. This concern is reflected in the nature of the sealing joints, positive or negative pressure chambers, and containment of venting systems.”¹⁴

How can one discern the ends of another user? Isn't distrust a major factor in fear for malevolent use of fermenters.

- Which norms are at play in this case scenario?
- Which ethical principles are at play in this case scenario?
- Which values conflict in this case scenario?

3.5 Questions and issues to be addressed

What instruments can one apply to safeguard the good use without risking the bad uses.

This question cannot be answered self-evidently. One can distinguish several questions and issues that need to be resolved:

Publication of scientific research is crucial for scientific progress and technological innovation. But if publication in publicly available scientific journals poses a danger, should this open publication be restricted? And are there other ways to have scientists and society reciprocally enjoy the fruits of each others labours?

Not only open publication but also access to certain facilities or instruments may be instrumental to malevolent use of certain technologies. In how far can these be restricted.

In some a restriction of access and use to specific facilities and instruments may be a reason to put less burden on restricting open publication of results. When might this be the case?

Is it the safety “culture” and the mindset of those working with the topic that is problematic? Are they too much rigged to only see issues of risk and safety as relevant, ignoring issues of dual-use and security?

Could international openness on research with a dual-use aspect to it help, or would it do the opposite? Should national interests always be the basis for action? How can national

¹⁴ Global security: http://www.globalsecurity.org/wmd/intro/bio_production.htm (last visited 16th August 2010)

interests be wed to international cooperation. How can such a cooperation render malevolent use less attractive?

Where should the responsibility reside for the problem of possible military use or terrorist use of specific technologies? Should it be the responsibility of scientists, companies and laboratories or governmental institutions? On what basis are they to decide which types of research should be under strict control, or even under 'embargo'?

Emphasising the dual-use dilemma may lead to further polarisation between different parties. What the one party considers to be national security or 'preventive warfare' the other may consider to be unjust warfare, what one party considers to be legitimate use of weapons against a far more powerful foe, the other may consider to be terrorism. It is unclear which parties are truly under threat. Should 'we' fear 'them' or should 'they' fear 'us'? Shouldn't we try to create a basis for dialogue rather than further polarisation? Which conditions can one create to this aim? When can one no longer pursue this route?

3.7 Literature

Anderson, F. (2000) *Crucible of War: The Seven Years' War and the Fate of Empire in British North America, 1754-1766*. pp. 542, 809n

Fenn, E. A. (2000) "Biological Warfare in Eighteenth-Century North America: Beyond Jeffrey Amherst". *The Journal of American History*, Vol. 86, No. 4 (Mar., 2000), pp. 1552–1580.

Global Security "Weapons of Mass Destruction: smallpox" http://www.globalsecurity.org/wmd/intro/bio_smallpox.htm (last visited on 16th August 2010)

Jackson, R. J., Ramsay, A. J., Christensen, C., D., Beaton, S., Hall, D., F., Ramshaw, I., A. (2001) "Expression of mouse interleukin-4 by a recombinant ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox". *J Virol* **75**: 1205–1210

Miller S and Selgelid M, (2007) "Ethical and Philosophical Consideration of the Dual-Use Dilemma in the Biological Sciences" *Science and Engineering Ethics* 13:523-580

NativeWeb "Jeffrey Amherst and Smallpox Blankets: Lord Jeffrey Amherst's letters discussing germ warfare against American Indians" http://www.nativeweb.org/pages/legal/amherst/lord_jeff.html (last visited 16th August 2010).

Peckham, H. H. (1947) *Pontiac and the Indian Uprising*. Princeton University Press.

Peel, J. (2004). "Precaution - A Matter of Principle, Approach or Process". *Environmental Policy*, 2004: pp. 1444-8602

Selgelid, M. J., Weir, L. (2009) "The mousepox experience; an Interview with Ronald Jackson and Ian Ramshaw on Dual-use Research". *EMBO Reports* 2009 **11**, pp. 18 – 24.

United States Department of Labor Occupational Safety and Health Administration "Smallpox as a Bioweapon" <http://www.osha.gov/SLTC/smallpox/evaluation.html> (last visited 16th August 2010)

Conclusion: Future Work

We will keep updating WP5 working documents in the duration of the project. We will develop the case scenarios for both case areas. With regard to dual use problems we will look at research on malaria prevention for the military since measures to prevent malaria contamination for soldiers may become useful for health measures in developing countries. A problem is that most research to prevent malaria is publicly funded, not by private companies, and that there seems to be only limited research. Military research to prevent malaria might therefore boost the search for a solution for this grave problem. Additionally, we will look at commercial applications of biometrics technologies.

Overall, the next step for this work package is to get clarity on the relation between principles and values, and to functionalise the other work packages in these two case areas as a test case. This was discussed in Lisbon. We will also provide for a more concrete description of what the role of case scenarios can be for value dialogue.