



TABULA RASA

Trusted Biometrics under Spoofing Attacks

<http://www.tabularasa-euproject.org/>

Funded under the 7th FP (Seventh Framework Programme)

Theme ICT-2009.1.4

[Trustworthy Information and Communication Technologies]

D7.1: Environmental Scanning Report

Due date: 31/04/2011

Submission date: 29/04/2011

Project start date: 01/12/2010

Duration: 42 months

WP Manager: Holly Ashton

Revision: 1

Author(s): Holly Ashton, Emilio Mordini (CSSC)

**Project funded by the European Commission
in the 7th Framework Programme (2008-2010)**

Dissemination Level

PU	Public	Yes
RE	Restricted to a group specified by the consortium (includes Commission Services)	No
CO	Confidential, only for members of the consortium (includes Commission Services)	No



D7.1: Environmental Scanning Report

Abstract:

Deliverable D7.1 aims to raise awareness of the potential ethical, legal and policy implications raised by systems for biometric spoofing prevention. First we briefly outline spoofing and some common spoofing attacks considered by this project as well as the countermeasures that could be put in place to combat them – some of which are under discussion to be used in the pilots for TABULARASA.

We then provide an ethical discussion of issues relating to spoofing and the countermeasures used to combat it. It must be emphasized that we do not intend to replicate here any work which has previously discussed biometrics in general: the focus, as appropriate to TABULARASA, is specifically on spoofing and spoofing prevention methods.

In the final part of the deliverable, we provide an inventory of existing regulations, reports, working papers and academic articles which address the ethical, legal and policy implications of systems for biometric spoofing prevention. The inventory takes into account existing resources relevant to this theme at the time of writing the deliverable – as appropriate, it must be noted that the inventory is not a definitive and closed resource as it will in all likelihood require updates at a further date to take into account new legislation and changes to work in this field.

Contents

1.	Introduction.....	4
2.	Summary.....	6
3.	Spoofing and Countermeasures	7
3.1	Multiple Biometrics Systems	9
3.2	Liveness Detection	9
4.	Countermeasures to Spoofing: the Ethical Issues.....	11
4.1	Generation of unexpected sensitive, personal information	11
4.2	Function creep	14
4.3	Physical intrusion	16
4.4	Offending human dignity	20
4.5	Legally controversial.....	22
5.	Inventory.....	23
5.1	International Conventions and Declarations	23
5.2	Communications from the European Commission to the Parliament and Council.....	25
5.3	EC Green Papers	27
5.4	Opinions of the European Data Protection Supervisor.....	28
5.5	Opinions of the Article 29 Working Party	29
5.6	ISO Standards.....	31
6.	Conclusion	32

1. Introduction

TABULARASA aims at addressing some of the issues raised by the widely acknowledged fact that biometric systems are vulnerable to attack and that biometric techniques can be spoofed. In a world which is increasingly relying on biometric systems to enhance security measures, researching ways to secure these systems against criminals is of the utmost importance.

It is evident that the using of biometric technologies raises a number of ethical and legal concerns – a simple Google search on ‘biometrics ethical concerns’ raises over a million hits. The issue has been comprehensively covered in the work of a couple of European FP7 projects; BITE¹ and HIDE² which were specifically devoted to considering the ethical and social impact issues relating to biometric technologies. A more recent FP7 project, ActiBio³ included a work package on the ethical, social and legal implications of second generation biometrics (which concern behavioural biometrics and the potential for continuous authentication) in which an Ethical Manual of over 200 pages was produced. This clearly outlined topics such as privacy, incidental medical findings, potential for discrimination and so on. Another project specifically relating to the ethical and legal issues in biometrics is the RISE project⁴, an international initiative for promoting awareness on ethical aspects of biometrics and security technologies.

It is clear then that the need to consider ethical aspects when discussing and researching biometrics is fairly well documented. An area that is less discussed however, concerns the work being carried out to enhance the security of biometric systems. Whilst laudable in its aims, research into biometric spoofing prevention may raise ethical, legal and policy implications of its own that must also be addressed. The countermeasures used to enhance the security of devices must not be assumed to be without problems simply because they are created in a spirit of ‘doing right’.

Current thinking on countermeasures include:

- Combining multiple biometrics in order to create a more robust system (i.e. the idea that the more biometrics you have to convincingly spoof, the harder your task)
- Liveness detection (i.e. exploring ways to ensure that the presented biometric is provided by a real, live, physical being)

TABULARASA will explore these as well as considering the potential of emerging biometrics such as vein, electro-physiological signals and gait.

These approaches to combating spoofing inherently raise a number of ethical, social and legal questions which, to our knowledge, have not previously been explored in depth in the context of

¹ BITE Project - <http://www.biteproject.org/>

² HIDE Project - <http://www.hideproject.org/>

³ ACTIBIO: Unobtrusive Authentication Using ACTivity Related and Soft BIOmetrics, <http://www.actibio.eu>

⁴ RISE: Rising Pan European and International Awareness of Biometrics and Security Ethics, <http://www.riseproject.eu/>

countermeasures for spoofing by any existing projects or research groups.

The main issues of contention largely relate to issues which are problematic to biometrics in general but which may be evident in new ways in relation to countermeasures for spoofing. These shall be discussed in greater depth further into the deliverable but here we list the key issues of concern. Countermeasures to spoofing may:

- 1) allow for the generation of unexpected sensitive, personal information about the data subject, e.g. medical details
- 2) be prone to function creep, e.g. they could store extra data that could be used for purposes different from those strictly related to the prevention of spoofing
- 3) be physically intrusive, e.g. sensors can intrude in people's body intimacy, hurting their feelings of modesty, their cultural convictions, their religious beliefs, or offending people suffering from physical disabilities (both disease and age related) etc.
- 4) offend human dignity, e.g. the amount of details collected can overall become an offense to the necessary respect due to individual's autonomy and privacy
- 5) be legally controversial, e.g. the amount of details collected can be disproportionate in relation to the purpose of the technology

This is the key concept behind the necessity of work package 7 of TABULARASA, 'Ethical, Social and Cultural Factors'. There is a need to take a closer look at the impacts of countermeasures to spoofing and to consider how the securing of biometrics systems can be implemented in the most responsible way possible.

In this first deliverable, we carry out an 'Environmental Scanning' exercise, the aim of which is to highlight the key ethical, legal and policy implications of systems for biometric spoofing prevention in various contexts and applications. We also provide an inventory of existing regulations, reports, working papers and academic articles which provide insights on this theme.

2. Summary

Deliverable D7.1 aims to raise awareness of the potential ethical, legal and policy implications raised by systems for biometric spoofing prevention. First we briefly outline spoofing and some common spoofing attacks considered by this project as well as the countermeasures that could be put in place to combat them – some of which are under discussion to be used in the pilots for TABULARASA.

We then provide an ethical discussion of issues relating to spoofing and the countermeasures used to combat it. It must be emphasized that we do not intend to replicate here any work which has previously discussed biometrics in general: the focus, as appropriate to TABULARASA, is specifically on spoofing and spoofing prevention methods.

In the final part of the deliverable, we provide an inventory of existing regulations, reports, working papers and academic articles which address the ethical, legal and policy implications of systems for biometric spoofing prevention. The inventory takes into account existing resources relevant to this theme at the time of writing the deliverable – as appropriate, it must be noted that the inventory is not a definitive and closed resource as it will in all likelihood require updates at a further date to take into account new legislation and changes to work in this field.

3. Spoofing and Countermeasures

*“Spoofing is an attack performed at a sensor level, outside the digital limits of the system, which consists for the **attacker to masquerade as another** one by falsifying data and thereby gaining an illegitimate advantage. This kind of attack does not require advanced skills, even though knowing how a biometric system works and what the algorithms in it are is a precious advantage. Therefore the potential number of attackers is numerous as anybody can try to perform such an attack.”* – from TABULARASA deliverable D2.1

The concept of masking identity is not new. As described by the Encyclopedia Britannica⁵, a mask is:

“..a form of disguise. It is an object that is frequently worn over or in front of the face to hide the identity of a person and by its own features to establish another being. This essential characteristic of hiding and revealing personalities or moods is common to all masks. As cultural objects they have been used throughout the world in all periods since the Stone Age and have been as varied in appearance as in their use and symbolism.”

Though of course masks in themselves are not all created with wrongdoing in mind, the idea that masking identity can be problematic is not new. An article about the Carnival masks of Venice⁶ notes that “From the early 14th century onwards, new laws were frequently passed in an attempt to stop the relentless moral decline of the Venetian people. Anonymity bred immorality for without recognition there were no consequences for your behaviour and so no need to moderate it”. The first documented legislation on this subject concerned a decree made on 22nd February 1339 which prohibited masquerading around the city at night and in 1448, a decree forbade men from entering convents dressed as women (which some were doing in order to gain entry and commit ‘immoral acts’). The article goes on to state:

“1608 was an important year, the 13th August to be precise, when a decree from the council of 10 was issued declaring that the wearing of the mask throughout the year posed a serious threat to the Republic. To avoid the terrible consequences of this immoral behaviour, every citizen, nobleman and foreigner alike, was obliged to only wear a mask during the days of carnival and at official banquets.”

The threat of a person using the covering up of their identity in order to break acceptable behavior codes can therefore be seen to have been acknowledged many years ago. The use of concealing identity when carrying out criminal acts is still used for example in the donning of balaclavas or masks to evade recognition on closed-circuit television (CCTV). In many countries there is legislation against covering your face in places of higher security such as in banks.

But of course, masking identity is not always as ‘simple’ as hiding who you are. In some cases, it is desirable to take-on the identity of another – to masquerade as someone else. A number of stories exist which relate to a character taking on the identity of someone else in order to achieve

⁵ <http://www.britannica.com/EBchecked/topic/367906/mask>

⁶ http://www.venetianmasquerademasks.co.uk/blog/read_18738/history-and-origins-of-the-venetian-carnival-.html

personal gain. For example, the Greek god Zeus uses disguise to his advantage in one of the ancient Greek myths. The myth relates the story of Zeus disguising himself as Artemis in order to lure the nymph Callisto to a secluded place where he then reveals himself as Zeus and rapes her⁷. From Christianity, the book of Genesis in the Bible includes an account of how Jacob (with the help of his mother and a disguise) tricks his father into bestowing upon him a blessing meant for his older brother Esau (Genesis 27: 5-35) from which he will profit greatly.

In a world where ones personal identity is becoming an ever more valuable tool as a token for ensuring security in travel and day-to-day transactions, it is clear that there are ever more opportunities for people who might seek to profit from using the identities of others. The fast pace of technological developments, and the relative ease for reproducing more conventional identification methods such as identity documents which rely only on photographs and watermarks has led to researchers exploring new ways by which to ascertain someone's identity, including of course, biometrics.

Biometry in general can be defined as; "the automated identification or verification of an individual's identity through measurable physical or behavioural traits"⁸. Given the fact that the physical attributes and behavioural patterns of individuals tend to be unique, biometrics were initially welcomed as the new, high secure way of proving identity. However, inevitably, it did not take long for people to seek dents in the armour of these new technologies. Various methods for bypassing and tricking (or, 'spoofing') biometric systems have been devised. Of course these require the faking or taking on of another's attributes; a modern form of 'masquerading' if you will. And unlike in the Venice of yore, the 'masks' being used are not as visible but rather, they have become subtle and ever more realistic copies of the original.

In the TABULARASA deliverable D2.1, 'Definition of use cases', a number of possible spoofing methods are listed, including for example:

Ways to spoof a fingerprint;

- Use of latent marks on dust or any material
- Use of a printed fingerprint
- Use of an artificial finger (silicone finger, gummy finger...)
- Use of a cut finger⁹

Ways to spoof someone's face;

- Use of a picture
- Use of a photo on a T-shirt
- Use of a mannequin
- Use of a cast

⁷ "Callisto." *Encyclopedia Mythica* from Encyclopedia Mythica Online.

<<http://www.pantheon.org/articles/c/callisto.html>> [Accessed April 4, 2011].

⁸ TERMIUM Plus, Canadian Translation Bureau, online;

<http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=&index=frt&srchtxt=BIOMETRIE>

⁹ Whilst this may sound somewhat sensationalist, there have already been instances of criminals acquiring a persons' finger by force in order to use the biometric data from their fingerprint. For instance, as far back as 2005, there was a report of Malaysian car thieves carrying out this crime, cutting off a Mercedes owners' finger using a machete in order to bypass the cars immobilizer (see: <http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm>).

- Use of make-up
- Use of natural similarity
- Use of plastic surgery
- Use of a cut head¹⁰

Ways to spoof speaker recognition:

- A speaker could be recorded and their speech replayed to the system

Other biometrics can also be potentially spoofed in various ways (see deliverable D2.1 for more details).

Laws banning the donning of masks after sunset are obviously not sufficient to deal with the threats posed by such spoofs. Thus, in order to defend a system from a spoofing attack, a more up-to-date approach is required. In particular, various countermeasures can be put in place, the aim of which is to strengthen the biometric system which may come under attack. As noted in the introduction, current methods for detecting or preventing an attack of a biometric system follow two major themes:

- 1) Combining multiple biometrics in order to create a more robust system
- 2) Liveness detection

A number of different anti-spoofing methods can be applied which fit under these two headings. During TABULARASA some of these will be explored for feasibility through the carrying out of pilot tests. Furthermore, emerging biometrics will also be explored for their potential in strengthening biometrics systems. Here we provide a description of the two major countermeasure approaches.

3.1 Multiple Biometrics Systems

The concept behind using a system that incorporates many biometrics is that it should be harder for someone to correctly spoof a system if they have to attack a number of different modalities at once. Thus, creating an adequate fake fingerprint as well as obtaining a suitable fake iris should be harder than obtaining either of those in isolation. Furthermore, if someone were to attack a system whose fingerprint scanner was vulnerable but which had an excellent iris reader, the system should, in theory, be less vulnerable on the whole to a spoofing attempt than a system relying on just one of those elements.

3.2 Liveness Detection

Liveness detection involves methods to ascertain whether a presented biometric originates from a live person or whether it is fake. A number of measures can be used to assist with liveness detection, including¹¹;

- *Procedural solutions*

For instance, a human operator could be in place to examine people and detect any abnormality

¹⁰ Though an extreme and disturbing measure it is non-the-less a potential way of spoofing a system.

¹¹ Taken from D2.1 of TABULARASA.

relating to the biometric in use. In the case that the biometric measure in place was a fingerprint reader for example, the operator might check everyone's hands/fingers.

- *Challenge-response approaches*

This involves the requirement of users to provide certain specific required actions when asked and as a measure to combat spoofing it appears fairly promising. Potential uses of challenge response could include: asking a passenger to position his finger with a specific random rotation at each acquisition or to present a bunch of fingers on the multiple-fingerprints sensor; asking the user to move his head, smile, open his mouth, blink his eyes; text prompted speech recognition, and so on.

- *Technical solutions*

Liveness detection tools could be included in the sensor. These could include: electro-optic sensors, temperature measurement, conductivity measurement, blood pressure measurement, light propagation analysis, response to an electric stimulus, pulse oxymetry, detection of genuine skin, active lighting, multi-camera face analysis or multi-spectral face image device

- *Software solutions*

Dedicated algorithms may also be considered as an aid to spoofing detection. This could include such software solutions as: bubbles detection, pore detection, wavelet analysis, bleach detection of the finger while pressing on the sensor, detection of 2D faces/3D faces, volume computation, measurements of skin reflectance, skin texture analysis, skin spectroscopy analysis and so on.

The usage of countermeasures to guarantee the enhanced security of biometric authentication systems against spoofing attacks is of vital importance. However, it must be clear that any such countermeasures are implemented in an ethically and legally responsible manner. In the next section we explain the importance of this by highlighting the topics of ethical concern relating to the implementing of countermeasures to spoofing.

4. Countermeasures to Spoofing: the Ethical Issues¹²

Whilst the need for strong security measures surrounding the use of biometrics is indisputable, the way in which any such measures are implemented requires careful consideration as they may in themselves raise issues of ethical concern.

“The mere act of using biometric technologies to capture sensitive biometric data constitutes an immense privacy concern if security is jeopardised, whereas in a scenario where security remains intact, privacy is enhanced and identity theft becomes significantly more difficult. However, as experience shows, there is no such thing as perfect security and hence biometric implementations are likely to see trade-offs between the two ends of the privacy spectrum”

Andronikou, Demetis and Varvarigou (2007)¹³

Using countermeasures to prevent/detect spoofing is a way of securing systems against identity theft, however, as stated in the quotation above, there is no such thing as perfect security. In the introduction we listed the key issues of ethical/legal concern that could relate to countermeasures for spoofing. It must be noted that the concerns mentioned here are also obviously concerns given for the use of biometrics in general. Here we present the way in which the concerns might be specifically related to countermeasures for spoofing.

4.1 Generation of unexpected sensitive, personal information


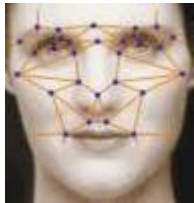

It is fully acknowledged that biometrics can generate or reveal sensitive personal information about an individual and it follows that measures to check that a presented biometric is genuine may also lead to the revelation of information that a person may not wish to disclose. In particular, countermeasures involving liveness detection may potentially allow for the disclosure of medical information if not carefully implemented with appropriate measures in place. For instance, a liveness detection sensor checking for pulse could potentially detect an irregular heartbeat. Checking the veracity of fingerprints could also potentially reveal drug-use¹⁴. In Table 1 we reveal some of the key concerns relating to the countermeasures for various biometrics which are foreseen to be used in TABULARASA.

¹² Please note that the ethical concerns, as well as guidelines on how to deal with these responsibly will be covered in more depth in other deliverables of the ‘Ethical, Social and Cultural Factors’ work package. Here they serve as a backdrop to the inventory which we have compiled.





¹³ Andronikou, V., Demetis, D., Varvarigou, Th., ‘Biometric Implementations and the Implications for Security and Privacy’, 1st in-house FIDIS Journal Issue, 1-2007, available at http://journal.fidis.net/fileadmin/journal/issues/1-2007/Biometric_Implementations_and_the_Implications_for_Security_and_Privacy.pdf.


¹⁴ Everts, Sarah (2008). *Fingerprints Reveal Drug Use*. Chemical & Engineering News 86 (51): 34.

Table 1 - Countermeasures and Ethical Concerns

BIOMETRIC	POSSIBLE SPOOFING ATTACKS	FORESEEN COUNTERMEASURES	ETHICAL CONCERNS
<p>Fingerprint</p> 	<p>Printed fingerprint</p> <p>Artificial fingers</p> <p>Cut fingers</p>	<p>Show hands to the operator</p> <p>Liveness detection tool</p> <p>Software solutions</p> <p>Challenge-response</p> <p>Multi-biometrics</p>	<p>Liveness detection methods may potentially reveal medical information – for instance, blood pressure measurement could reveal hypertension.</p> <p>Analysis of fingerprints can disclose information about drug habits and potentially medical history of the individual (Everts, 2008)</p> <p>Methods may not be sensitive to the desires of certain cultural or religious groups (for instance touching a sensor that has been touched by others)</p> <p>Use of multibiometrics may cause concern due to the greater amount of data captured and processed.</p>
<p>Face</p> 	<p>Use of a picture</p> <p>Use of a photo on a T-shirt</p> <p>Use of a mannequin</p> <p>Use of a cast</p> <p>Use of make-up</p> <p>Use of natural similarity</p> <p>Use of plastic surgery</p> <p>Use of a cut head</p>	<p>Monitoring people who pass</p> <p>Challenge-response (e.g. asking the user to move his head, smile, open his mouth, blink his eyes, etc.)</p> <p>Liveness detection</p> <p>Software solutions</p> <p>Multi-biometrics</p>	<p>Challenge-response methods may be uncomfortable for some groups (for instance people on the Autistic spectrum¹⁵)</p> <p>Liveness detection such as checking for genuine skin may be problematic for certain people (for instance someone with bad burns)</p> <p>Use of multibiometrics may cause concern due to the greater amount of data captured and processed.</p>
<p>Iris</p> 	<p>Printed image</p> <p>High resolution display of an iris</p>	<p>Liveness detection tool</p> <p>Software solutions</p> <p>Multi-biometrics</p>	<p>Tools to determine the veracity of an iris could potentially gather information which might disclose medical issues such as albinism, jaundice,</p>

¹⁵ Browndyke, J. N. (2002) *Autistic Behaviour: Etiology and Evaluation*. Accessed online: http://www.neuropsychologycentral.com/interface/content/resources/page_material/resources_general_materials_pages/resources_document_pages/autistic_behavior_etiology_and_evaluation.pdf

			<p>Kayser-Fleischer rings (due to copper deposition as a result of particular liver diseases)</p> <p>Use of multibiometrics – as above.</p>
<p>Vein</p> 	<p>Use of a printing of features from a stolen venous network</p> <p>Use of a vascular pattern print-out</p> <p>Use of a video of a moving hand</p>	<p>Liveness detection tool</p> <p>Software solutions</p> <p>Multi-biometrics</p>	<p>As for the other modalities, methods used to check for liveness could potentially disclose medical information on a subject.</p> <p>Use of multibiometrics – as above.</p>
<p>Gait</p> 	<p>Mimic the way someone walks</p> <p>Disguise</p>	<p>Monitoring people who pass for unusual behavior</p> <p>Multi-biometrics</p>	<p>Abnormal or unusual gait can be a symptom or result of various medical problems including neurodegenerative and musculo-skeletal disorders (e.g. Parkinson’s Disease) and psychiatric conditions (such as depression).</p> <p>Use of multibiometrics – as above.</p>
<p>Speaker/speech recognition</p> 	<p>Record and replay</p> <p>Mimic someone’s voice</p>	<p>Monitor use of the system</p> <p>Challenge-response</p> <p>Multi-biometrics</p>	<p>Some people may have problems with their voice for medical reasons (for instance throat cancer, having a laryngoplasty or temporarily ill with a cold) which could cause them to have problems passing countermeasure checks.</p> <p>Asking someone to read a particular text could be embarrassing for people with learning difficulties/illiteracy who may be self-conscious and have problems carrying out the task.</p> <p>Use of multibiometrics – as above.</p>
<p>ECG / EEG</p> 	<p>A replica of the signal of the subject provided to sensor’s electrodes</p>	<p>Presence of a supervisor</p>	<p>Whilst the sensors used for biometrics are not of the standard to allow medical diagnoses, signals may non-the-less show up an abnormality (such as a</p>

			cardiac irregularity) that supervisor could pick up on. There are also concerns that ECG could be covertly combined with lie-detectors ¹⁶ which a supervisor of the system could use.
<p>Multi-modal biometrics</p> 	Use various attacks as relevant to the modalities included in the multi-modal system (e.g. fake fingerprint used with a picture/mask of a face)	<p>Monitoring people who pass</p> <p>Liveness detection tool</p> <p>Software solutions</p> <p>Challenge-response</p>	<p>Use of multibiometrics may cause concern due to the greater amount of data captured and processed.</p> <p>Any concerns about the individual modalities are relevant to a multi-modal system.</p>

4.2 Function creep

Function creep relates to the concept of a technology that was designed for one purpose being used for a completely different purpose. Where countermeasures for spoofing are concerned, function creep would need to be guarded against to ensure that the methods adopted could not be used in controversial alternative ways. For instance, it should not be possible for the technical and software solutions used to detect a faked modality, to be used to categorise groups of people (e.g. based on skin colour, age, blood pressure or any other category which the countermeasure device could potentially identify someone by). Furthermore, any data stored by the system to assist with identifying spoofs would need to have strict controls in place concerning its' use. It should not be possible to use data for purposes separate to those directly concerning the prevention of spoofing.

Function creep in the field of automated personal recognition may be motivated by several reasons (from State intelligence, to commercial purposes) and it is not limited to biometric identification. Most examples of function creep are indeed rather innocuous. The “Social Security Number” in the US is an often cited example of function creep. Although the original social security cards bore the warning that the SSN could not be used for identification, in the 1960s the Internal Revenue Service started using the SSN for tax payer identification and today the SSN has been the main identity document used by most US citizens. Function creep usually involves three elements: 1) a policy vacuum; 2) an unsatisfied demand for a given function; 3) a slippery slope effect, or a covert application. A policy vacuum is probably the most important element to determine the risk of function creep. When organisations (be it small companies, large industries, or governmental agencies) adopt new information technologies, or new information schemes, failing to create specific policies, these technologies end up being driven only by the different

¹⁶ Mordini, E. & Ashton, H. (2011 - in press), *The Potential for Disclosure of Personal Medical Information*, in Mordini E, Tzovaras D (eds), *Second Generation Biometrics: the Ethical and Social Context*, Springer, The International Library of Ethics, Law and Technology

interests of various stakeholders. As a result, the new scheme may develop in a quite different sense – sometimes even opposite - from that primarily intended. Civil liberties advocates have the tendency to implicitly blame people because they adopt new technologies without considering the downside. Yet it is evident that the main responsibility rests with policy makers who should create the opportune policy frame for innovations.

An unsatisfied demand for a given function is the second important element that has the potential for creating a function creep. Information collected for one purpose is used for another when there is a need that is not properly met. In the example of the SSN, it is evident that the lack of a suitable tax payer identifier was the main driver for the SSN's mission change.

Finally, function creep must develop almost unnoticed. Usually, function creep happens for one of two reasons: either the new function(s) develop little by little, quite innocently, because of the incremental effect of several minor changes of mission/technology misuse, or the new functions are the result of a hidden agenda or, of various undisclosed purposes. Warrantless cell-phone tracking by law enforcement is a good example of this latter kind of function creep, which is obviously the most ethically and politically worrisome.

Analysing function creep more in depth, and in the context of biometric applications, one should distinguish between two different situations: the first being when biometric identification is used beyond the limits for which the system was officially adopted, the second being when biometric identification is used to generate extra information which is not per se relevant to identification.

As per the first point, it is evident that any identification scheme can be carried out with a hidden agenda (e.g., sorting out some social groups, collecting extra information about people, eliciting the feeling of being under observation, etc.) and biometrics do not make an exception. For instance a security agency could decide to carry out a covert screening programme parasitic to a standard identification/verification programme. People enrolled for identification or verification purposes could also be covertly screened against, say, a database of terrorists. In such a case, biometrics would still be used for identification purposes, but these purposes would be partly different from those officially claimed. More correctly, in these cases one should refer to a “subversive use” of a biometric system, say, to an attempt to subvert the correct and intended system policy (ISO SC37 Harmonized Biometric Vocabulary - Standing Document 2 Version 8 - dated 2007-08-22 ¹⁷).

There is however also the possibility that biometric systems are used to generate details which are not relevant to personal recognition, which is a proper case of function creep. To date, there is no evidence that any biometric application has ever been systematically used to reveal a subject's personal details beyond those necessary for personal recognition (of course one could argue that some ID schemes adopted in countries such as Pakistan or Malaysia have been inherently designed in order to produce extra information and to track citizens, but this is a rather different issue because it involves the whole policy of a state rather than specific technology misuse). No one doubts that biometrics can be used to generate extra information, but until now details that could be elicited by biometrics could also be obtained in easier ways. Consequently, there is no point in obtaining such information through the use of biometric applications. In practice, biometrics have the potential for being misused, but the cost/benefit ratio of such a misuse is still discouraging to any Big Brother candidate. Yet, this is likely to change in the near future with

¹⁷ <http://isotc.iso.org/livelink/livelink?func=ll&objId=2299739&objAction=browse>

second generation biometrics and large scale adoption of multimodal systems. One of the possible variants of Murphy's law states that if any technology can be misused, it will be, and there is no reason to assume that biometrics might escape this rule.

Function creep is facilitated by a surplus of information. The principle of data minimization, or limitation, should then be the cornerstone of any biometric policy, which is respectful of privacy tenets. Unfortunately, this is not the case with most biometric systems, which are redundant and end up generating more data than necessary.

To conclude it seems that the general tenets to be considered addressing the issue of function creep and anti-spoofing measures are:

1) **Effective and focused regulation:** as far as anti-spoofing measures become standards and are commercialized it is paramount that their usage is framed by a clear and unambiguous regulatory framework which establishes criteria to minimize data collection and retention. This should imply both self-regulatory measures (e.g., company ethical codes, international standards, best practices) and the development of specific technological approaches (privacy by design). The need to develop also specific statutory legislation is questionable, provided that it were possible in this very nuanced field.

2) **Understanding user requests in context:** one of the main reason why technology is misused is the failure to understand user requirements in different contexts. This unavoidably generates unexpected usage, which are always at risk to become misuse. It is consequently paramount to develop a anti-spoofing measures on the basis of a careful analysis of user requirements and specific use cases.

3) **Transparency:** the main countermeasure to prevent malicious misuse of any technology is transparency, anti-spoofing technology does not escape this general rule. It is paramount to make all anti-spoofing technologies transparent and public. Of course this could create some puzzling problems, given that one runs the risk to facilitate further attacks. Finding the right balance between transparency and secrecy is consequently one of the main policy challenges that one is going to meet in this field.

4.3 Physical intrusion

Sensors can intrude on people's body intimacy in a number of ways. In the most basic sense, sensors may hurt a person's feelings of modesty. Whilst this is an area of delicacy for biometrics in general, it is particularly relevant to countermeasures which aim to confirm that a person is presenting a genuine biometric. Countermeasures to spoofing, by their nature are probing the veracity of a person's most private domain – their body. Some countermeasures may be problematic for certain groups of people – for instance, cultural convictions may make certain groups reluctant to engage with some types of sensors¹⁸. Furthermore, people with physical

¹⁸ For example, it is known that Japanese people prefer to use fingerprint scanners that don't involve touching a sensor (study). This could make them reluctant to engage with countermeasures where touch was required in order to assess skin, heat or pulse.

disabilities (either disease or age-related) may find it difficult to engage with certain sensors which could make them feel embarrassed or awkward and could make it difficult to pass through security zones easily without causing problems.

For instance, Sickler and Elliot (2004)¹⁹ comment:

“In all of our trials to date, each biometric system has performed better with the younger population than with the older half, though the differences were not necessarily statistically significant (n.p.)”.

Moreover certain countermeasures may generate details on people’s emotional and mental status. For instance, challenge response methods could be difficult and embarrassing for people with dyslexia or people who were illiterate who might have difficulties in reading out a text used to prompt them. Other challenge-response methods might be uncomfortable for some people (for instance someone with Asperger’s or Autism who might prefer to do things according to a specific familiar behaviour pattern). Other factors such as being depressed, drunk or on drugs might also affect how a person relates to the presented anti-spoofing measure.

All these examples concern the notion of integrity. The word integrity literally means “the quality or state of being complete or undivided”. Physical and mental integrity thus refers to the inviolability of a person's body and mind, say, it refers to the right against being touched (in physical and metaphorical senses) without consent. Historically, the notion of body integrity comes from the legal conception of *Habeas Corpus* (Latin: you shall have the body), originally the legal action through which a person can seek protection against an unlawful detention. The *Habeas Corpus* affirms the right not to be imprisoned arbitrarily and to not have the body violated in any other way (e.g. physical inspection, torture, abusive treatments, and so on). “The violation of the right to physical and psychological integrity of person is a category of violation that has several gradations and embraces treatment ranging from torture to other types of humiliation or cruel, inhuman or degrading treatment with varying degrees of physical and psychological effects caused by endogenous and exogenous factors which must be proven in each specific case”²⁰. Body integrity is threatened by physical pain, injuries, sexual assaults, rape, physical inspections, and the like. Mental integrity is violated any time when emotional and cognitive processes are brutally invaded, abused and/or disrupted.

We all have an interest in protecting our physical and mental integrity. This is clearly expressed by the *Universal Declaration of Human Rights* (art.3) which states that everyone has a right to the inviolability of his or her person, and by the *Convention on Human Rights and Biomedicine*²¹ (art.1), which states that "Parties to this Convention shall protect the dignity and identity of all human beings and guarantee everyone, without discrimination, respect for their integrity and other rights and fundamental freedoms with regard to the application of biology and

¹⁹ Sickler, N. C., & Elliot, S. J. (2004). An evaluation of fingerprint quality across an elderly population vs. 18-25 year olds. *Biometric Consortium 2004 Conference*, Purdue University.

²⁰ Inter-American Court of Human Rights, *Loayza Tamayo Case*, Judgment of Sept. 17, 1997 (Ser. C) No. 33, para. 57, <http://www1.umn.edu/humanrts/iachr/C/42-ing.html>

²¹ The concept of body integrity has important applications in the biomedical sphere, where *inter alia* it requires that invasive actions cannot be lifted without the informed consent of the patient.

medicine". The principle of body integrity does not concern only violations of the body resulting in suffering or in adverse health conditions, but it also deals with intrusions without harmful effects. This leads to an additional issue, which is particularly relevant to debates concerning countermeasures for spoofing. Does a bodily or psychological intrusion constitute a violation of integrity only if it is perceived as such? Or, on the contrary, are there objective criteria to establish when a violation infringes the right to integrity? Indeed the principle of the "inviolability of the body" includes two cognate, but different,²² concepts: 1) the view "that the body is a 'sacredness' in the biological order"²³; and 2) the view of the body as personal property, whose borders cannot be trespassed without the owner's consent. There are then two diverse perspectives about body integrity, the former contends that the right to be free from bodily (and mental) intrusion is inherently part of the notion of human dignity²⁴, the latter maintains that bodily integrity is the right of "every human being ... to determine what shall be done with his own body"²⁵ and to protect his physical privacy. While the dignitarian approach usually contends that body integrity is – at least in part – an objective concept, the privacy approach emphasises the subjective aspect of body integrity, which always implies the notion of consent (or lack of) to the intrusion.

The tension between dignitarian and privacy interpretations of body integrity is well illustrated by the Dutch Constitution (art.11) which states "everyone has a right to untouchability of his body, except for restrictions provided by or valid because of the law". Then, according to Dutch criminal law (art.56), arrested people can be "examined on body and clothes" but only if the examination limits itself to the surface of the body (including natural orifices), while "cutting or pulling hair, drawing blood and obtaining sperm, and taking x-rays are not warranted".²⁶ The law then prohibits the use of any instrument which can penetrate the body surface, conceptualised as a moral and legal border not to be trespassed. It is evident that here there is a tension related to the word "untouchability", which could refer either to the dignity, the sacredness, of the whole body, or to the notion of 'body' as a private property, which is touchable only to the extent that its owner consents.²⁷

²² Actually, together with Giorgio Agamben, one could argue that these two concepts are anything but the two sides of the same coin, being the notion of sacred body only the other side of the notion of body as a property. In his analysis of the *habeas corpus*, Agamben argues that "the root of modern democracy's secret biopolitical calling lies here: he who will appear later as the bearer of rights and, according to a curious oxymoron, as the new sovereign subject (*subiectus superaneus*, in other words, what is below and, at the same time, most elevated) can only be constituted as such through the repetition of the sovereign exception and the isolation of *corpus*, bare life, in himself. If it is true that law needs a body in order to be in force, and if one can speak, in this sense, of "law's desire to have a body," democracy responds to this desire by compelling law to assume the care of this body. This ambiguous (or polar) character of democracy appears even more clearly in the *habeas corpus* if one considers the fact that the same legal procedure that was originally intended to assure the presence of the accused at the trial and, therefore, to keep the accused from avoiding judgment, turns -- in its new and definitive form -- into grounds for the sheriff to detain and exhibit the body of the accused. *Corpus is a two-faced being, the bearer both of subjection to sovereign power and of individual liberties*" (Agamben G, 1988, *Homo Sacer: Sovereign Power and Bare Life*. Stanford UP, Stanford, CA. P 124-125)

²³ Murray TH, (1987), On the Human Body as Property: the Meaning of Embodiment, Markets, and The Need of Strangers, *Journal of Law Reform* 20, 4:1055-1089

²⁴ See for instance, Maschke KJ, (2003), Proxy Research Consent and the Decisionally Impaired: Science, the Common Good, and Bodily Integrity, *Journal of Disability Policy Studies* 13, 4

²⁵ Schloendorff v. Society of New York Hospital, 1914, quoted by Maschke KJ, (2003).

²⁶ Ten Have HA, Welie JW, (1998) Ownership of the Human Body Philosophical Considerations, Springer, p.102

²⁷ The notion of sacredness implies etymologically that something is untouchable because it belongs to the god. The two notions of dignity and privacy eventually differ only in defining who is the owner of the body, whether the god or

A dignitarian interpretation of the notion of body integrity is endorsed by the *Charter of Fundamental Rights of the European Union*, which has an article (art.3), specifically focusing on the *Right to the integrity of the person*, in the first Chapter devoted to Dignity:

1. Everyone has the right to respect for his or her physical and mental integrity.
2. In the fields of medicine and biology, the following must be respected in particular: the free and informed consent of the person concerned, according to the procedures laid down by law [...]

The context in which art.3 is collocated points out that “the dignity principle should be regarded as a tool to identify the cases in which the body should be absolutely *inviolable*”²⁸ and that consequently “the principle of inviolability of the body and physical and psychological integrity set out in Article 3 of the Charter of Fundamental Rights rules out any activity that may jeopardise integrity in whole or in part - even with the data subject’s consent.”²⁹ The respect for body integrity demands that body inviolability is considered – at least in part – a non-negotiable principle. Body integrity is violated any time that an undue and unsolicited intrusion “penetrates” the individual’s personal sphere, independently from whether such an intrusion is tactile, visual, acoustic, psychological, etc. or whether it produces injuries.

In the US bodily integrity is protected by the Fourth Amendment of the Constitution, which protects physical privacy:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

In order to be reasonable a search should meet people’s rational expectations about their right to privacy.³⁰ Intrusive searches demand specific reasons, might need a warrant, and cannot be a routine procedure. In 2008 the New York State Court of Appeals (New York State’s highest court) discussed the case of Azim Hall, a drug dealer who was stripped and searched by the police and was found to have a string hanging from his anus. The police pulled the string and found a baggie of cocaine inside his rectum. Azim Hall complained that his Fourth Amendment right was violated. The Court ruled that

There are three distinct and increasingly intrusive types of bodily examinations undertaken by law enforcement after certain arrests and it is critical to differentiate between these categories of searches. A “strip search” requires the arrestee to disrobe so that a police officer can visually inspect the person’s body. The second type of examination — a “visual body cavity inspection” — occurs when a police officer looks at the arrestee’s anal or genital cavities, usually by asking the arrestee to bend over; however, the officer does not touch the arrestee’s body cavity. In contrast, a “manual body cavity search” includes some degree of touching or probing of a body cavity that causes a physical intrusion beyond the body’s surface [...] Summarizing the relevant constitutional precedent, it is clear that a strip search must be founded on a reasonable suspicion that the arrestee is concealing evidence underneath clothing and the search must be conducted in a reasonable manner. To advance to the next level required for a visual cavity inspection, the

the man.

²⁸ European Group on Ethics in Science and New Technologies (EGE), Op. N° 20, Ethical aspects of ICT implants in the human body, Adopted on 16/03/2005

²⁹ Ibid.

³⁰ Katz v. United States, 389 U.S. 347, 351 (1967)

police must have a specific, articulable factual basis supporting a reasonable suspicion to believe the arrestee secreted evidence inside a body cavity and the visual inspection must be conducted reasonably. If an object is visually detected or other information provides probable cause that an object is hidden inside the arrestee's body, *Schmerber* dictates that a warrant be obtained before conducting a body cavity search unless an emergency situation exists.³¹

There is an apparent tension between the **EU Charter** and the **US Constitution** perspectives on body integrity. In the European perspective the potential offence to body integrity does not seem to depend chiefly on the way in which the subject perceives the intrusion, nor on whether personal data are properly handled. In other words the offence to human dignity can be hardly mitigated by adopting privacy aware technologies. The potential offence is related to the fact that the human body is not respected, in other words the issue of respect for integrity tends to overlap with the issue of respect for human dignity (see next chapter). On the contrary in the light of the **US Constitution**, effective and legally binding privacy algorithms could protect the right to privacy and then make anti-spoofing systems consistent with the Fourth Amendment.

4.4 Offending human dignity

Respect for human dignity is paramount in the European ethos and constitutional framework. Chapter 1 of the Charter of the Fundamental Rights is entirely devoted to human dignity, which also includes a chapter addressing the issue of informed consent. In the European human right architecture, dignity is the cornerstone of all other rights and values. What is “dignity”? Dignity is not an easy concept to define. In the modern usage it basically refers to the value of a human individual as an unconditioned value, say, each human being possesses an incommensurable value, which is independent from any other specification (e.g., gender, race, ethnicity, age, nationality, professional qualification, health status, etc). It implies that all human being deserves the same degree of protection and are entitled with the same basic rights. Offences to human dignity entail a breach of such fundamental principles either because they discriminate against an individual or a category of individuals, or because they treat human beings as commodities, say, deny their incommensurable and unconditioned value by making their value depended on any further attribute.

There are two major risks concerning human dignity in the field of biometric identification. One is the vexed question whether biometric identification is an offence per se, because it implies an abstraction from any biographical detail and to focus only on ‘bare life’. Biometrics would dematerialise the human body, by turning it into a digital sign, a commodity, a thing among other things. Biometrics would transform the human body into a fetish inhabited by digital identities. This has led to (rather emphatic) questions about the overall ethical and democratic legitimacy of this technology. These questions were not originated by Luddite militants– as one would expect – but by distinguished advisory boards, such the French National Consultative Ethics Committee for Health and Life Sciences, which wrote “Do the various biometric data that we have just considered constitute authentic human identification? Or do they contribute on the contrary to

³¹ *People v. Azim Hall*, 2008 NY Slip Op 2676 (2008)

instrumentalizing the body and in a way dehumanizing it by reducing a person to an assortment of biometric measurements?”³²

While the question about the legitimacy to use biometric identification appears however quite academic and far from real political and ethical issues, the second issue which concerns human dignity is certainly more concrete and worrisome. In nutshell the question regards what one is entitled to do in order to ensure those values that one intends to protect by using a biometric application. Biometrics can have a variety of applications, for military and civil purposes, for physical or logic access right verification, ecommerce and etrade, for ATM retailers and for ehealth, etc. In each of these cases we ensure identification in order to enable someone to get some benefits or, more generally speaking, to access some rights; and to exclude some others. In a few selected case – biometric screening – we can use this technology to screen in a group whether there is some that should be not in that group; finally in other cases biometrics can be used to profile group of individuals. In all these case we infringe personal intimacy by collecting data on another person’s physical appearance, or physiology, or behaviour, or all of these together. To be sure, usually data collection does not entail any form of humiliation or degradation but there is always the risk that it can be perceived a such by particular individuals or cultural group. This is the case – for instance – of fingerprinting, which is perceived by many individuals (and by whole cultural groups such as inhabitants of former colonies in Africa and in Asia) as a form of humiliating procedures associated to criminal law. Another examples is face recognition, when it obliges religious women of Islamic culture to show their naked face to a male officer. In all these examples one has not to balance two comparable values, such as individual discomfort vs. collective security, which would be still tenable. On the contrary one has to confront on one hand, say, more collective security but, on other hand, humiliation, which is a deep devaluation of humanity, in other words an offence to human dignity. This would make impossible any trade off and any application of the proportionality principle: according to the EU Charter dignity is unconditioned and must prevail against any other value. Yet drawing the border line between, say, acceptable discomfort, and offence to human dignity is not always easy and life is often more nuanced than one pretends when he writes papers or reports. If obliging someone to expose his naked body for a physical search is likely to be always humiliating, could we say the same for collecting a palm vein image, even if the person stated the opposite in order to refuse to undergo the check? In other words, are there “objective” criteria to establish what is and what is not respectful of human dignity?

All these questions, which concern biometrics in general, are also valid for the adoption of anti-spoofing technologies. When one develops anti-spoofing it is paramount to always pose questions about the risk that procedures are perceived by the single individual, or by a class of individuals, as humiliating or degrading. In a multicultural and multiethnic world, where the notion of dignity is embodied in several different practices and perceptions, is not enough to address this question in general terms, but it is always important to articulate it in specific use cases. This has however an important consequence for TABULA RASA: technology design cannot avoid addressing some basic questions about operational procedures that will have to be adopted in order to use that technology. Indeed technology is rarely per se offensive to human dignity, what are humiliating and degrading are operational procedures. Although operational procedures are partly independent

³² OPINION N° 98. 2007, Biometrics, Identifying Data and Human Rights Available at; <http://www.ccne-ethique.fr/docs/en/avis098>

from technology design, it is somehow obvious that technology design can influence future procedures and it is then critical that this aspect is taken into account by engineers and technologists.

Finally the issue of dignity also involves the issue of informed consent. Again, in a field as anti-spoofing it is likely to be problematic to search for a consent, because it would risk to facilitate the “bad guy” who wants to overcome protective measures. Yet this question cannot be avoided and should become one of the main focus of WP8 in TABULA RASA.

4.5 Legally controversial

The amount of details collected to enable countermeasures to be effectively used could potentially be disproportionate in relation to the purpose of the technology. As above, this affects issues concerning privacy and human dignity.

DeHert and Sprokereef (2007)³³ comment:

“As governments have only recently started to use biometrics in public schemes, there is no European case law as yet. It is hence unclear how concerns about the use of biometrics will be addressed by the existing legal framework.”

This is supported by the lack of cases to be found on the EUR-Lex website for case law (<http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en>) – one example was found³⁴.

Action brought on 24 March 2005 by United Kingdom of Great Britain and Northern Ireland against Council of the European Union (Case C-137/05):

The applicant claims that the Court should:

annul Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States

It follows that if case law for biometrics in general is so sparsely covered, there is not much to be ascertained concerning countermeasures for spoofing attacks as of yet.

³³ Sprokkereef, A. & DeHert, P. (2007) *Law, Science and Policy*, Vol. 3, pp. 177–201

³⁴ <http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en&newform=newform&Submit=Submit&alljur=alljur&juredj=jurcdj&jurtpi=jurtpi&jurftp=jurftp&alldocrec=alldocrec&docj=docj&docor=docor&docdecision=docdecision&docop=docop&docppoag=docppoag&d ocav=docav&docsom=docsom&docinf=docinf&alldocnorec=alldocnorec&docnoj=docnoj&docnoor=docnoor&radty peord=on&typeord=ALL&docnodecision=docnodecision&allcommjo=allcommjo&affint=affint&affclose=affclose& numaff=&ddatefs=&mdatefs=&ydatefs=&ddatefe=&mdatefe=&ydatefe=&nomusuel=&domaine=&mots=biometrics &resmax=100>

5. Inventory

In the previous chapters, we have provided some background on spoofing biometrics, countermeasures to spoofing and some of the ethical issues that might be raised by putting such countermeasures in place. The safest way to ensure that ethical integrity can be maintained in the implementation of measures for spoofing prevention is to adhere to relevant legislation set in place to protect the rights of the individuals using biometric technologies (and for security/human rights in general).

In this final section of the deliverable we present an inventory including existing regulations, reports, working papers, academic articles and so on which relate to the ethical, legal and policy implications of systems for biometrics spoofing prevention in various contexts and applications. It must be noted that there is very little (if any) existing policy on countermeasures for spoofing and the majority of the documents we mention are those relating to biometrics, security and human rights in general. They can be interpreted in the context of countermeasures for spoofing however and it is with that in mind that we present them. In general, the documents presented here are those which should protect people from the ethical issues raised in the previous chapter and are therefore the key factors that designers working on anti-spoofing mechanisms should be aware of as they go about their work. In each section, we list the main relevant documents and then include an explanation of how these are relevant to systems for spoofing prevention.

5.1 International Conventions and Declarations

The conventions and declarations listed here cover human rights and data protection issues, both of which are key issues relating to potential concerns of countermeasures to spoofing.

1. *Convention for the Protection of Human Rights and Fundamental Freedoms Council of Europe, Rome, 4th November 1950, ETS n° 5*
<http://conventions.coe.int/treaty/en/Treaties/Html/005.htm>

Systems implemented for biometrics spoofing prevention must not in any way impinge on the Human Rights of individuals using the systems. In particular, technicians involved in creating countermeasures for spoofing must be conscious of the following: Article 5 – Right to liberty and security; Article 8 – Right to respect for private and family life; Article 14 – Prohibition of discrimination; Article 53 – Safeguard for existing human rights.

2. *European Social Charter - Council of Europe, Turin, 18th Oct 1961, ETS n° 35*
<http://conventions.coe.int/treaty/en/Treaties/Html/035.htm>

Of particular relevance to biometrics spoofing prevention is Article 3 – The right to safe and healthy working conditions. Increasing the security of work places that use biometrics for authenticating workers (for instance, by using anti-spoofing measures) would be supported by this Charter. In implementing such measures however, the workplace must not impose other risks to workers (i.e by introducing countermeasures which might raise

other ethical concerns).

3. *European Framework Equality Directive, COUNCIL DIRECTIVE 2000/78/EC of 27 November 2000*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:303:0016:0022:en:PDF>

In this directive, the importance of not discriminating between groups of workers is emphasized. This could be relevant to the implementation of countermeasures to spoofing because certain groups may not be able to engage with sensors as easily (for instance it is known that fingerprints of older people are often harder to verify due to changes in the skin with age³⁵). Thus it would be important to implement countermeasures which were equally effective for all workers and did not include the potential to discriminate between different groups of people.

4. *Charter of Fundamental Rights of the European Union*
http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Similar to point 1, this Charter covers the fundamental rights expected for people in Europe amongst which, a number may be vulnerable to certain countermeasures for spoofing if they are not implemented with care. These include: Article 1 – Human Dignity; Article 3 – Right to Integrity of the Person; Article 6 – Right to Liberty and Security; Article 8 – Protection of Personal Data; Article 21 – Non-discrimination; Article 22 – Cultural, Religious and Linguistic Diversity; Article 26 – Integration of Persons with Disabilities; Article 27 – Worker’s Rights to Information and Consultation Within the Undertaking; Article 31 – Fair and Just Working Conditions.

5. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.*
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

Where countermeasures may involve the generation of new data, there must be strict procedures and policies in place concerning how it is used and who gets to see it. In essence, any personal data generated by anti-spoofing procedures should be treated with the same respect as it would be in any other context.

6. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.07.2002*
http://www.dataprotection.ie/documents/legal/directive2002_58.pdf

³⁵ E.g. Sickler, N.C. & Elliott, S.J. (2006) *An evaluation of fingerprint image quality across an elderly population vis-a-vis an 18-25 year old population*. 10.1109/CCST.2005.1594817. See summary online at: http://www.cerias.purdue.edu/news_and_events/events/symposium/2004/posters/pdfs/Fingerprint%20Image%20Quality%20Evaluation.pdf

This directive may be less relevant to countermeasures for spoofing however it is included in order to cover the eventuality that any countermeasures to spoofing systems may include the passing on of data via the use of electronic communications systems.

7. *Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001*

http://ec.europa.eu/justice/policies/privacy/docs/application/286_en.pdf

This includes recognition for the need of an external supervisory body to regulate the processing and movement of personal data. Systems pertaining to countermeasures to spoofing would need to work within the sanctions of such a body.

5.2 Communications from the European Commission to the Parliament and Council

The listed communications from the European Commission highlight issues relating to data protection and achieving a secure information society. Systems for biometric spoofing prevention contribute to providing more security in the use of the growing field of biometrics which is rapidly growing as a security control. In the implementation of countermeasures, care must be taken that they do not inadvertently expose people to alternative risks.

1. Promoting Data Protection by Privacy Enhancing Technologies (PETs) Brussels, 2.5.2007 COM(2007) 228 final
http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf

It is noted that;

“Whilst strictly speaking data controllers bear the legal responsibility for complying with data protection rules, others also bear some responsibility for data protection from a societal and ethical point of view. These involve those who design technical specifications and those who actually build or implement applications or operating systems.”

This also relates to those designing systems for combating spoofing of biometrics systems. The communication goes on to note that;

Article 17 of the Data Protection Directive lays down the data controller's obligation to implement appropriate technical and organisational measures and to ensure a level of security appropriate to the nature of the data and the risks of processing it. The use of technology to support the respect for legislation, in particular the data protection rules, is already envisaged to some extent in the ePrivacy Directive.

A further step to pursue the aim of the legal framework, whose objective is to minimise the

processing of personal data and using anonymous or pseudonymous data where possible, could be supported by measures called Privacy Enhancing Technologies or PETs - that would facilitate ensuring that breaches of the data protection rules and violations of individual's rights are not only something forbidden and subject to sanctions, but technically more difficult.

2. Follow-up of the Work Programme for better implementation of the Data Protection Directive, Brussels, 7.3.2007 COM(2007) 87 final
http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0087en01.pdf

The document comments on Directive 95/46/EC, stating:

“The Commission considers that the Directive is technologically neutral and that its principles and provisions are sufficiently general, that its rules may continue to apply appropriately to new technologies and situations. It may be necessary, though, to translate those general rules into particular guidelines or provisions to take account of the specificities involved in those technologies.”

We suggest that biometric technologies and methods to combat the spoofing of them may be technologies which will warrant particular guidelines once they become more mainstream.

3. First Report on the implementation of the Data Protection Directive, COM (2003) 265(01), 15.5.2003
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF>

A survey of 9156 Individuals showed that “although the Data Protection Directive incorporates high standards of protection, most individuals (4113 out of 9156 or 44.9%) considered the level of protection a minimum” (p.9). Given the extent that biometrics are seen as a sensitive topic in terms of data, it is vital that the countermeasures introduced to make biometric systems more secure are demonstrated to be at the highest level of data protection standards.

4. Communication on a strategy for a secure Information Society, COM(2006) 251 of 31 May 2006
http://www.consilium.europa.eu/ueDocs/COUNCIL-LIVE/20061211_103939_2.PDF

“The ubiquitous information society, while providing great benefits, also poses significant challenges, thus creating a new landscape of potential risks; threats to security and privacy, also through unlawful interception and exploitation of data, are becoming more and more serious, targeted and clearly aimed at economic benefit, new responses for the emerging and already existing threats should be created in an innovative manner and they should also cover issues arising from system complexity, mistakes, accidents or unclear guidelines” (p.4)

5. Communication on an area of freedom, security and justice serving the citizen, COM (2009) 262 final of 10 June 2009
http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/COMdocs/2009/COM2009_262_EN.pdf

In particular, section 2.3 discussed ‘protection of personal data and privacy’ and states:

“Technology is currently developing very fast. It is transforming communication between individuals and public and private organisations. A number of basic principles therefore need to be restated: purpose, proportionality and legitimacy of processing, limits on storage time, security and confidentiality, respect for the rights of the individual and control by an independent authority” (p.8)

6. Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:164:0003:0003:EN:PDF>

Of particular relevance to countermeasures for spoofing is Article 3 - ‘Offences linked to terrorist activities’ which lists the following as crimes:

- (a) aggravated theft with a view to committing one of the acts listed in Article 1(1);
- (b) extortion with a view to the perpetration of one of the acts listed in Article 1(1);
- (c) drawing up false administrative documents with a view to committing one of the acts listed in Article 1(1)(a) to (h) and Article 2(2)(b).

The use of biometric spoofing by terrorists would relate to this.

5.3 EC Green Papers

The Green papers provide an endorsement for the implementation of relevant and successful countermeasures for biometric spoofing in order to enhance the security of Critical Infrastructures and public areas vulnerable to crime and terrorism.

1. Green paper on detection technologies in the work of law enforcement, customs and other security authorities COM(2006) 474, September 2006
http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0474en01.pdf

“Law enforcement, customs and other security authorities are often scrutinised for whether they comply with applicable legal standards. Even if the technology as such is not in breach of legal standards, the manner of its use may raise concerns. Accordingly, identifying the legal framework governing the use of, and setting limits for, technological solutions could help to raise greater awareness in both public and private sectors and facilitate compliance with existing standards. The private sector could also benefit from

such a study when proposing and designing technological solutions and services for the public sector.” (p.21)

This highlights the earlier comments about the need to design countermeasures for spoofing in such a way that they cannot be used for additional purposes and obtaining more information about individuals than is necessary.

In particular, the document goes on to state that “the Commission suggests that a study should be undertaken to identify the legal framework governing personal detection technology and biometrics”.

2. Green Paper on a European Programme for Critical Infrastructure Protection - COM(2005) 576, November 2005
http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf

The document talks about Critical Infrastructure Protection (CIP) and, though never specifically referring to biometrics or spoofing attacks, it is pointed out that CIP relates to: “the ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction” (p.19).

5.4 Opinions of the European Data Protection Supervisor

1. Opinion of 19 December 2005 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM (2005)475 final), OJ C 47, 25.02.2006
2. Opinion of 26 September 2005 on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM (2005)438 final), OJ C 298, 29.11.2005
3. Second Opinion of 29 November 2006 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, OJ C 91, 26.04.2007
4. Opinion of 28 February 2006 on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005)490 final), OJ C 116, 17.05.2006
5. Opinion of 20 January 2006 on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM (2005)600 final), OJ C 97, 25.04.2006

5.5 Opinions of the Article 29 Working Party

The following opinions and documents relate to areas of law and policy which may have some bearing on countermeasures for spoofing due to the content of the topics dealt with (e.g. personal data, detection technologies, discussion of areas where biometrics – and thus countermeasures for spoofing – may be relevant such as border and transport security).

- Working document on biometrics
http://www.statewatch.org/news/2004/feb/biometric-wp80_en.pdf
- Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf

Provides further insight to Directive 95/46/EC, including measures that should also be common practice in systems for biometrics and countermeasures to spoofing such as obtaining the consent of the subject before obtaining any data about them.

- Opinion 4/2007 on the concept of personal data
<http://www.garanteprivacy.it/garante/document?ID=1707337>
- Working document on the future of privacy 02356/09/EN WP 168 of 1 Dec 2009
<http://www.garanteprivacy.it/garante/doc.jsp?ID=1717928>
- Seventh report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the years 2002 and 2003
<http://www.statewatch.org/news/2005/feb/7th-rep-data-prot-02-03.pdf>
- Opinion N° 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics, including provisions on the organisation of the reception and processing of visa applications COM(2006)269 final
http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0269en01.pdf

It is foreseen that: “depositing the visa application form and the taking of biometric identifiers should intervene at the same place and at the same time” (p.5) This would present the potential for false enrollments to a biometric system.

- Opinion 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp96_en.pdf

- Working Document on the processing of personal data relating to health in electronic health records (EHR)
<http://www.garanteprivacy.it/garante/document?ID=1386451>

Whilst this does not explicitly deal with biometrics or spoofing, it does highlight the importance of privacy relating to medical information – it should be possible for a patient to prevent disclosure of his medical information from one medical professional to another if s/he wishes. As mentioned previously, though small, there is a risk of systems for biometrics spoofing prevention to detect medical abnormalities. Thus the treatment of any data falling into that category should be treated accordingly.

Furthermore, the document states “reliable identification of patients in Electronic Health Record systems is of crucial importance. If health data were used which relate to the wrong person as a result of incorrect identification of a patient the consequences would in many cases be detrimental. If we imagine that biometrics may play a role in identifying individuals in HER systems then the need to carefully and responsibly implement countermeasures for spoofing is significant here.

- Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp129_pl.pdf

A key passage in terms of countermeasures for spoofing is:

“The Working Party also underlines the obligation to respect the principle of proportionality in relation to any measure restricting the fundamental right to privacy as required by Article 8 of the Convention on Human Rights and the relevant case-law. This implies inter alia, the obligation to demonstrate that any measure taken corresponds to an “imperative social need”. Measures which are simply “useful” or “wished” may not restrict the fundamental rights and freedoms” (p.4)

Whilst it is evident that greater security is required for biometric systems, the countermeasures introduced to detect and deter spoofing attacks must not go beyond what is necessary to the level of protection required.

- Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp112_en.pdf
- Working document on data protection issues related to RFID technology
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf
- Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism.
<http://www.statewatch.org/news/2004/nov/wp99.pdf>

- Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf
- Opinion 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:EN:PDF>

5.6 ISO Standards

There are 58 published International Standard Organization (ISO) standards relating to biometrics which can be found online in the ISO website catalogue:

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770

These fall under JTC 1/SC 37- Biometrics, the scope of which is described as:

“Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects” (http://www.iso.org/iso/jtc1_sc37_home)

Of particular interest for TABULARASA is an ISO on anti-spoofing that is currently under development: ISO/IEC NP 30107 - Anti-Spoofing and Liveness Detection Techniques:

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=53227

Whilst there is no draft version as of yet (the standard is still at an early stage of development), it will cover various themes that are of relevance to the work of TABULARASA including:

- Description of techniques and principles to evaluate anti spoofing techniques
- Definition of a common format to define the type of technology used
- Identification of conditions that allow using anti spoofing techniques and liveness detection

Other ISOs are of relevance to the work on countermeasures for spoofing of biometric technologies

“A Framework for Security Evaluation and Testing of Biometric Technology” known as ISO/IEC JTC1 SC27 NP 19792 (http://www.iso.org/iso/n05_final_report_agc.pdf) notes that personal identification is an extremely important area in the security domain and is actively covered by ISO/IEC JTC1 SCs 17, 27, and 37. The AGS (American Global Standards) recommends continuing focus and if possible acceleration of this work.

Work in the field of countermeasures for spoofing needs to be carried out in accordance with the appropriate technical standards, and given that these are regularly updated, particular attention must be paid to the ongoing changes in this field.

6. Conclusion

In this deliverable we have highlighted that systems for biometrics spoofing prevention may raise ethical issues similar to those raised by biometric and security technologies in general. This is because, despite the fact that the aims of countermeasures are laudable (with the aim of increasing the security of biometric systems and thus rendering them more user-friendly and acceptable to society), they may also, by their nature include the use of techniques and measures which in themselves raise concerns.

In particular, the key methods used to detect a spoofing attack of a biometric system potentially raise the following issues:

Multiple biometrics:

- Results in the generation and processing of more data and thus creates more chances for data protection concerns to surface.
- May not be proportionate to the needs of the biometric system in general.

Liveness detection:

- The methods used to determine that a presented biometric comes from a real person may be invasive of physical and mental privacy
- They may have the potential to reveal medical information about an individual
- May subject people to an additional process to which they are not happy to comply with

Although there is not yet much literature or policy relating specifically to countermeasures for spoofing, a vast amount of information can be determined from existing documents which relate to biometrics and security in general. In the previous chapter we compiled the relevant documents into an inventory which can serve as a guide for the considerations to think of in order to sensibly and responsibly implement systems for biometrics spoofing prevention and to avoid the concerns outlined above. In further deliverables of work package 7 on the Ethical, Social and Cultural Factors of TABULARASA, the concepts, ideas and concerns raised in this first paper will be expanded on so that by the close of the project we will be able to present a fully formed consideration of the ethical factors related to the development and implementation of countermeasures for spoofing of biometrics.