

DELIVERABLE D3.3a

Ethical Brief on Biometrics & Embedded Technology



HIDE PROJECT

Project funded by the European Commission-FP7

Contract: 217762

Co-ordination and Support Action (CSA)

Start date of the project: 1 Feb 2008

Duration 36 months

1° Reporting Period

Deliverable:	D3.3a <i>Intermediary</i>
Title:	Ethical Brief on Embedded Technology
Due date:	30-07-2009
Actual submission date	30-07-2009
Lead contractor for this deliverable:	ZUYD University
Contact:	Irma van der Ploeg i.vdploeg@hszuyd.nl
Dissemination Level:	PU



Introduction

The Hide project is concerned with the ethical and social aspects of biometrics and other ICT-based personal identification technologies, in particular regarding their use for security and law enforcement purposes. The focus group on Embedded Systems is part of Workpackage 3 on *critical issue identification*, within specific areas of technological development. This task is approached through a series of technology orientated focus groups exploring ethical and social issues in relation to particular (sets of) technologies. The four technological areas are:

- Technology Convergence
- System Interoperability
- Privacy Enhancing Technologies
- **Embedded Systems & Ambient Intelligence**

The focus group on embedded systems and AmI is organised by the Infonomics and New Media Research Centre at Zuyd University, The Netherlands, and the current document is its main output.

This ethical brief is a working document developed from information and discussions collected during the first HIDE focus group meeting on embedded Systems and Ambient Intelligence, held in Maastricht on 31 October 2008. This focusgroup is devoted to identifying and articulating critical issues emerging from the co-development of *embedded and ambient intelligence and identification technologies, in particular biometrics and other body monitoring systems bodies*. This intermediary deliverable will be the input for two further meetings of the focusgroup in 2010. Participants are HIDE project partners and a number of invited external experts. (see http://www.hideproject.org/events/fg-embedded_technology.html)

The document is organised in the following way:

First (1) we will briefly delineate the type of technologies and systems to be considered

Next, in (2) we set out to identify what we consider to be the main critical issues generated by these new technologies and systems.

We continue in (3) by describing how these issues signify considerable potential for contradiction with existing EU legislation and regulation of IT, in particular regarding data protection, as well as for infringing on the human and civil rights of privacy, bodily integrity, dignity, non-discrimination, freedom of expression, and the right not to be subjected to automated decisions.

Finally, in (4) we set the agenda for the next focusgroup meeting by posing the question whether, and, if so, under which conditions benefits promised by such systems might outweigh the costs incurred in terms of the legal and moral issues described above.

1 Embedded systems and identification

One of the most influential developments in ICT in the near future is generally thought to be the shift away of computing power from PCs and desktop-configurations to the physical environment. Embedded software, ubiquitous computing, ambient technology, smart objects, and the emergence of 'the Internet of Things' are all terms denoting a particular aspect or view of this near future.

Due to developments in a.o. radio frequency identification (RFID), miniaturisation, wireless, sensor and networking technologies, people will be moving through and interacting with their physical environment in new ways. Objects themselves will interact and communicate, and send information about themselves, their users, or their environments to electronic networks and databases.

Our daily lives are already organised through a myriad of electronic passage points, negotiated through an increasing number of electronic identifiers, code words, pass words, PIN numbers, user names, access controls, electronic cards or biometric scans. Some are highly visible and negotiated willingly (e.g., a PIN credit card purchase), others are more covert (e.g., a speed camera on a motorway), or entirely embedded (e.g., GPS technology and mobile phones).

On the positive side, huge gains in convenience, efficiency, and safety are predicted to result from this; on a more bleak view, this could mean the ultimate track-and traceability and loss of privacy. In particular, and most relevant to the HIDE project, the information on peoples' behaviors generated by these systems, will, in all probability, prove an invaluable and highly tempting resource for law enforcement and crime prevention and security policy, if not the primary aim of such systems. This would imply a (post-hoc) blanket recasting of all end-users, consumers, and citizens as suspects, which may render them vulnerable in unforeseen ways.

Many, if not most, of the envisaged or already developed AmI systems are 'user centric' and comprise personalised functionality. This means that people's interactions with such systems require them to be identified within the system, in order to enable it to retrieve the relevant personal profile and settings.

Moreover, for it to work effectively, ambient intelligence requires intuitive and convenient interfaces, meaning that identification and authentication are usually (half-) automated and as unobtrusive as possible, with little conscious effort from the user needed. This requirement makes identification technologies like biometrics and RFID likely options in this context, but also puts such systems on a direct collision course with the data protection principle that personal data collection must always involve an aware and informed data subject (EU Data Protection Directive, art.7 par.1 – see below))

In addition to identification/authentication to access or activate the system, continued interaction or mere contact with the system generally results in registration of personal identifiers, data on movements, behavior, location, etcetera, communicated to, and stored in central databases. These personal data may be required for the improvement of the systems performance (by updating and perfecting the personal profile) but could, obviously, be used for other purposes.

For example, databases containing data on traffic and mobility, or consumption patterns of citizens could be very valuable to social scientists, and be of strategic interests to policy makers. Perhaps more problematical, national security, law enforcement and crime prevention interests in particular are highly likely to make authorities seek access to, for example, data collected through payment systems for public transport, toll collection, road pricing. Also, the production of profiles from such databases is highly attractive for private companies wishing to refine their marketing efforts to the point of identifying specific potential customers and clients to target with individual offers or advertisements.

This ethical brief aims to identify critical issues stemming from a particular subset of this type of technology, namely embedded systems for covert and 'unobtrusive' digital

monitoring, identification, and assessment of individuals in public spaces and work environments.¹

Such systems have a high probability of generating ethical and legal issues, since their nature and goal is to authenticate, identify or assess individuals from a distance, that is, without their conscious co-operation. Generally, such systems operate by cameras, RFID technology, and wireless sensors, able to pick up biometric and other bodily features and states such as facial expressions, body temperature, pupil dilation, pulse.

These data, then, can be compared with previously stored personal profiles (authentication and identification) or general profiles (assessment), upon which decisions on further actions, be they automatic or not, will be taken. Decisions might include, for example, (dis-)allowing the person to operate critical machinery, vehicles, or weapons (see 'Securing critical workspaces') ; it might lead to picking the person from a crowd for deeper inspection (see 'Airport of the future?').

Common element in these systems is a particular *focus on the human body*, and the generation and use of information on intimate bodily features and states. In addition to 'classic' biometric data such as facial images, fingerprints and iris scans, that in some sense can be considered as 'superficial' (although this by no means necessarily signifies such data being less personal or intimate), some of the new systems are geared to glean a new type of data from beneath the common coverings (clothing) of the body or even the skin, such as heart rates, body temperature, or brain activity patterns.

Also, a set of new biometric technologies focussing on general characteristics, such as age, gender, ethnicity, body weight and height (socalled 'soft biometrics' often to be used in conjunction with classic biometric identification systems to improve performance), and on behavioral activity characteristics, such as gait, are being developed today, that bring a whole range of new human body data within the frame of automated recognition technologies, and their accompanying practices of monitoring, assessing, surveilling and profiling.

A final aspect worth noting is the shift towards multimodal systems in this context, meaning that usually not one but several different biometrics are combined. The reason for this is to increase reliability of the systems, but the accompanying effect is also a prima facie intensification of monitoring and surveillance, because by collecting and using more different features and aspects of the subject, more is 'known' about them, and the profiling potential is increased.

Thus we are concerned here with a paradoxical, dual development, namely the simultaneous 'shifting out' of computing power into the physical and built environment, and 'shifting in' towards the human body, its surface, and even internal functioning. Whereas on the one hand information and communication networks are extending, and becoming more pervasive in our daily activities and movements through space, on the other hand, through various technologies and applications, we become ever more intimately connected as embodied persons to these networks.

The following is a tentative list of systems and applications in which this growing intertwinement of IT and human bodies takes place:

- ◇ Biometric data *put on* RFID chips (e.g. e-passports) in ID-documents and cards
- Biometric identification/authentication in AmI systems
 - for public security reasons , e.g. access control/crime control and security in public events; continuous authentication in securing critical infrastructures
 - for system/network/information security reasons
 - for convenience reasons (intuitive interfaces)

¹ Although ambient intelligence (' domotica') in the home environment is currently a prominent area of development, we will not consider this application area in this brief.

- ◇ RFID chips *linked to* body data (index to retrieve medical records), and possibly *implanted in* bodies
- Body monitoring sensors *combined with* RFID
 - for safety reasons in work or home environments ('safe living' for the elderly), public sports events
 - for medical reasons in health care (e.g. telemonitoring)
 - for identification/authentication purposes (see above)
- Covert body classifying systems (soft biometrics) categorising people according to, and amongst other things, age, gender, ethnicity, body weight and/or height.
- ◇ Health risk profiling using RFID generated consumer data

As the European Group on Ethics argued in their Opinion on ICT implants in the human body², becoming 'networked persons' is fraught with opportunities and threats. Threats, for example, to human dignity, freedom and autonomy, and inviolability of the human body. Indeed, what might be at stake could be as profound as a transformation of human embodied identity in the personal as well as the anthropological sense.

This brief will not deal with all the potential applications exhaustively, but discusses in particular critical issues relating to the technologies marked '•' in the list above, concrete examples of which are described in vignettes 1 'Airport of the future?' and 2 'Securing critical workspaces'

1 Airport of the future ?

In several places, a new security concept is being researched, aiming at detection of criminal or even 'terrorist intent'. These systems, one of which is already being tested in several US airports, consist of a combination of a set of different, networked sensors and cameras scanning people moving through a corridor from a distance.

The use of remote cardiovascular and respiratory sensors, remote eye trackers (camera plus software), thermal cameras, high resolution video, audio sensors, and other sensor types such as for pheromones, is hoped to enable registering heart rates, body/skin temperatures, facial expressions, eye movements, pupil diameter, breathing rates, body movements, facial features and expressions, and voice pitch.

The idea is that such physiological and behavioral parameters are indicative of particular malevolent intentions, or 'malintent', which, in turn, are predictive of certain harmful and disruptive behaviors. Preventing such behaviors to occur could then become possible by filtering out those people in a crowd, or passing through a checkpoint, that show the physical and behavioral signs and patterns sought, and pulling them out for further inspection and interviewing, while easing security procedures for the rest of the public.

Example projects: (US DHS) Hostile Intent; Future Attribute Screening Technology - FAST, (EU-FP7) Suspicious and Abnormal Behavior Monitoring - SAMURAI

² European Group on Ethics in Science and New Technologies (2005) Opinion on Ethical Aspects of ICT Implants in the Human Body, March 16.

2 Critical Issues

If we delineate our topic as the integration of biometrics and related identification technologies in AmI and UbiComp applications, we are aware of the fact that most biometric systems to date have consisted of applications one could qualify as 'embedded' or 'ambient' under some definition, with biometrics used for PCs and desktop configurations, (log-ons and access control), being a relatively insignificant part of applications.

The critical aspect coming to the fore more urgently with biometrics' current co-evolution with AmI and UbiComp, however, is the emphasis on 'automated' identification, 'unobtrusive' and 'continuous' authentication, and covert data capture. (see: Securing Critical Workspaces) The combination with wireless or contactless sensors and RFID, for example, in many instances enables data capture from a distance, without the biometric data subject noticing. Also, the 'user friendliness, and 'convenience', so high on the priority list of AmI developers, commonly translates into 'as little conscious effort required from the end-user as possible'.

Moreover, biometric applications for securing public spaces develop increasingly towards (potentially) covert biometric data capture, such as, for example, in applications like 'smart' camera surveillance, or products like 'Iris-on-the-move' (see also Airport of the Future?).

2 Securing critical workspaces

Some workspaces such as particular vehicles, laboratories, or control rooms require high level security. To this end, new forms of access and operation control, authentication, and monitoring of persons present are being researched and developed in advanced new forms of multimodal biometrics.

The aim is to develop continuous, and unobtrusive identification and authentication with forms of embedded biometrics based on the internal physiology of the subject, measured by electroencephalogram (EEG) and electrocardiogram (ECG), and using miniaturized, wireless electrode based sensors that are integrated in clothing elements such as a hat (EEG) or a shirt (ECG). Internal physiological biometrics are said to be more difficult to spoof while in addition performing de-facto aliveness checks.

Another new route in authentication is taken with the 'sensing seat', which measures the pressure distribution from the body of the seated person, after which a profile and a biometric signature are created. Though not unique enough for unimodal use, this signature can increase the overall authentication accuracy when combined with other biometrics.

A third direction in advanced biometrics consist of activity and movement patterns such as displayed by a person moving through an office while performing particular tasks.

Combined with classic biometrics such as face recognition, the above new forms of biometrics, provide new ways of integrated, multimodal identification and authentication systems, that are said to be very reliable, and well accepted, because of their embedded and unobtrusive presence.

Example projects: (FP6) Human monitoring and Authentication using Biodynamic indicators and behavioural analysis - HUMABIO; (FP7) Unobtrusive authentication using activity related and soft biometrics - ACTIBIO

Behavioral and physiological biometrics in controlled or private spaces

Embedded forms of biometric authentication systems are being developed in research that explores the possibilities of using physiological measurements (such as EEG and ECG) for authentication purposes. Building sensors in, for example, seats, hats or shirts, allows highly unobtrusive, continuous monitoring and/or authentication of subjects in situations where security stakes are high.

When considering possible issues emerging from such new systems, one needs to take into account that the context described here concerns a working environment where compliance and consent to organisational security and safety policies can be demanded from personnel as a condition of employment. Especially when security and safety of the wider public are at stake in the organisation's activities, compliance and observation of stringent security measures unacceptable elsewhere should be enforceable.

However, the systems under discussion here, even though they are 'convenient' and unobtrusive, in that they do not disturb the person in their activities or require conscious effort, are, in another sense, quite *intrusive*. Having one's brain, heart, gestures and movements registered continuously gives a whole new meaning to the notion of 'worker surveillance'.

As always, a lot depends on the exact configuration of the system: how, where and what exactly gets to be registered, who will have access to data, how and how long they will be stored, etcetera. Be that as it may, such a system, and the various elements it comprises, take the possibilities of control over the worker and their body into a new plain. Not merely their privacy, but their very integrity as an embodied person is compromised in a way that requires protections to be implemented in the system set-up and its default operation. It is important to recognise that distinguishing between normal /intended use versus misuse/abuse, and reserving ethical concern for the latter, is arbitrary (because perspective, power, and interest dependent) and possibly naïve.

Of special concern should be the extent to which sensitive and intimate information about the worker, e.g. about their medical condition, could become available that in principle is unrelated and irrelevant to job performance, and therefore beyond an employer's need or right to know. In general, such intimate physical information becoming available at any level of management and system control, could possibly render these workers vulnerable to inadmissible forms of manipulation and pressure.

Behavioral and physiological biometrics in public spaces

When configuring comparable (though obviously differently configured) systems for surveilling public places, a rather different picture emerges. Physiological and behavioral parameters are then captured in order to assess all persons present, and 'filtering out' those with a particular profile deemed deviant according to a set of predefined norms. The systems of this type designed so far, up to the stage of experimentation in real-life settings, all aim to filter out those people considered potentially 'hostile', 'aggressive', or otherwise posing a threat to public safety. In relation to this type of system, several specific issues come to the fore.

First the *covert and distant* nature of data capture is obviously bringing the persons at whom the system is directed in a vulnerable position that contradicts many assumptions embedded in current discourse on privacy, data protection and user empowerment. For one thing, in contrast to most 'classic' biometric identification or authentication modalities, these persons can no longer in any meaningful way be construed as 'users' or 'end-users' at all. Rather, they become the objects of a new kind of physical search that defies many deeply ingrained values concerning bodily integrity, freedom from arbitrary inspection, and consent requirements.

Next, the fact that it is *body data* that are being captured increases the potential for ethical and legal problems, since body data should be considered highly sensitive, personal, and intimate; in certain ways more so than other identifiers like passports,

names, social security numbers etcetera. In addition, the likelihood of collateral information on the person's state of health (certain features and values may be indicators of disease or illness) being collected this way should be considered as a serious privacy risk.

But perhaps more importantly, because by design completely intransparent, but at the same time highly consequential, the specific *normative nature* of these systems ought to be questioned. In particular, the ideas concerning *normality* built into such systems carry great potential for legal and ethical problems, for instance regarding discrimination. A society in which information on physical state of arousal, facial expression, pitch of voice becomes routinely collected and used as input for surveilling public spaces is indeed stepping on slippery ground. Once a general awareness of the existence of such systems exists among the public, the occurrence of *anticipatory conformity* will be a highly likely consequence: people will check themselves, up to their facial expressions, to avoid being harrassed, which would constitute serious damage to our ideals of a free and open society.

Next to the assessment of particular measurements as deviant as such, the automated *interpretation* of such data in terms of elevated risk and behavioral intentions ('hostile thoughts') is fraught with problems. The interpretative leap from, e.g. accelerated heartrates or elevated body temperature, to particular states of minds, emotions, and even intentions, let alone hostile ones, is large, prone to error, and hardly scientific.³ Moreover, individual baselines for such values might differ significantly, rather than being the same for every human being. Quite possibly, such differences will turn out to correlate with certain sensitive differences, such as gender, ethnicity, or age, giving rise to new occurrences of (indirect) categorical discrimination of historically already disadvantaged groups. Alternatively, but no less problematic, new categories and profiles may be developed, so that, depending on the tolerance range set for the system, certain individuals and categories of people may experience being flagged over and over again.

One may well ask whether there can ever be a legal and ethical justification for filtering out people for further inspection and interviewing based on such intimate bodily parameters. Moreover, the intent to detect mental and emotional states, based on their presumed correlation with these physiological signs, signifies the introduction of a form of privacy invasion of a new dimension altogether, one that will inevitably lead to people having to justify their emotional and mental states. At the same time, the chances that such technologies will really contribute to security goals, i.e., will actually be able to filter out those with immediate criminal intent, seem at best doubtful.⁴

Soft biometrics

In 1998, J.L. Wayman, then director of the National Biometric Test Centre at San Jose State University, testified in a US congressional hearing:

"We must note that with almost all biometric devices, there is virtual no personal information contained therein. From my fingerprint, you cannot tell my gender; you cannot tell my height; my age, or my weight. There is far less personal information exposed by giving you my fingerprint than by showing you my driver's license."⁵

³ National Academy of Sciences (2008), *Protecting Individual Privacy in the Struggle Against Terrorists. A Framework for Program Assessment*. The National Academies Press, Washington DC

⁴ *ibidem*

⁵ Michael N. Castle (Chair) (1998), *Hearing on Biometrics and the Future of Money*, Committee on Banking and Financial Services, Washington, May 20, p.49.

Despite such reassurances, the at that time still relatively unknown biometric technologies had some people worried enough to include the provision that “collection of a biometric identifier must not conflict with race, gender, or other anti-discrimination laws”, such as in, for example, the proposals for the Californian Consumer Biometric Privacy Act’.⁶

Although this was then seen by many biometrics advocates as being based on unfounded and ill-informed beliefs about biometrics, science historian Simon Cole writes the following on the presumed ‘emptiness’ of fingerprints:

“Galton's [the founder of dactyloscopy] “regret,” his failure to find the key to the code of heredity in fingerprint patterns, has been confused with the notion that fingerprint patterns actually contain no information pertinent to health, ancestry or behaviour. But other researchers found rough correlations between fingerprint pattern type and ethnicity, heredity and even some health factors. These correlations, especially the ethnic ones, have proven robust and still hold up today. As with any correlation, they are not determinative; one cannot predict ethnicity from fingerprint pattern, but fingerprint pattern types do appear with different frequencies among different “ethnic groups” (as defined by researchers). True, not much has been done with these correlations. But the point is that the situation with fingerprint patterns and genes is fundamentally the same — correlations. It is not that fingerprint pattern correlations do not exist; rather, it no longer scientifically acceptable to investigate them — unlike genetic correlations with so called ethnicity. In short, the perceived “emptiness” and harmlessness of fingerprint patterns is a social achievement, not a natural fact.”⁷

Moreover, a few years after the congressional hearing, it has become even more clear that Wayman may not have been entirely right: in an article on so-called ‘soft biometrics’, we read:

“Many existing biometric systems collect ancillary information like gender, age, height, and eye color from the users during enrollment. However, only the primary biometric identifier (fingerprint, face, hand-geometry, etc.) is used for recognition and the ancillary information is rarely utilized. We propose the utilization of “soft” biometric traits like gender, height, weight, age, and ethnicity to complement the identity information provided by the primary biometric identifiers.”⁸

So, today’s developments in ‘soft’ biometrics, i.e. a set of experimental biometric applications aiming at using ‘partial identities’, and recognising general body characteristics such as body weight, gender, age, or ethnicity, yield a set of critical issues that need to be addressed here as well. In particular when they are integrated in the AmI and Ubicomp environments, they call forth an urgent need for critical analysis and assessment. The aimed for ability to distinguish concerns sensitive categories, many of which are overburdened with histories of discrimination of the worst kind.

Whereas at present soft biometrics are often used as a secondary mechanism to improve classic biometrics’ performance, the quoted article gives a few lines of research, that clearly point to potential applications beyond that:

“Methods to incorporate time-varying soft biometric information such as age and weight into the soft biometric framework will be studied. The effectiveness of utilizing the soft biometric information for “indexing” and “filtering” of large biometric databases must be

⁶ Biometrics in Human Services, Vol.2, No.2, May 1998, p.11.

⁷ Simon A. Cole, The Myth of Fingerprints <http://www.genewatch.org/genewatch/articles/19-6Cole.html>

⁸ Anil K. Jain, Sarat C. Dass, and Karthik Nandakumar (2004) *Soft Biometric Traits for Personal Recognition Systems*, Proceedings of International Conference on Biometric Authentication, LNCS 3072, pp. 731-738, Hong Kong, July 2004.

studied. Finally, more accurate mechanisms must be developed for automatic extraction of soft biometric traits.”⁹

One could easily imagine justifiable uses for systems that can categorise, e.g., faces, according to gender or ethnicity, or ‘filter’ a database that way, for example where a reliable witness statement in a crime investigation would render exclusion of particular categories from a database search highly valuable. Another such example would be classifying subjects in broad age categories, in order to determine legal competence to apply for certain services, or buy certain products, while preserving anonymity. On the other hand, there are all too many situations imaginable in which filtering people out on the basis of their gender, age, or ethnic/racial background constitutes illegal discrimination, and developing systems to automate this process could therefore be considered inherently risky.

Also, and contrary to what their apparent self-evident reference in ordinary language and everyday life may lead one to believe, the reification of these categories and distinctions, as the history and philosophy of science have made clear, is essentially contestable and unstable. For example, the distinction between the male and female gender on a genetic level does not entirely match the ones made on the endocrinological, anatomical, psychological, or socio-cultural levels; and even when birth registered gender is taken as a reference point, a problem exists where even this is amenable to change during an individual’s lifetime. In an exacerbated form, similar problems exist with ethnicity and race classifications, all of which have been proven to lack any objective basis in ‘nature’.

These states of affairs render any automated application of such categories an endeavour fraught with risks of error and contestation, risks that will undoubtedly increase when these systems are applied in an embedded and ‘unobtrusive’ fashion.

Multi-modality

The fact that most of the systems described here comprise several, often more than three, biometrics, merits some attention as well. Of course, increasing reliability, reducing false positives and negatives, is in the interest of the persons subjected to these systems. Nonetheless, in terms of privacy invasion, surveillance potential, or vulnerability to manipulation, ‘more’ does not equal ‘better’ at all.

Intuitively, the danger of ethical problems is clearly compounded when it is not merely, say, faces that are being scanned, but faces in conjunction *with* e.g. heartrate, temperature, pupil dilation, gender, gait, voice pitch. The cumulation and combination of many instead of one parameter, increases a sense of total observation, and of people becoming completely transparent to system operators. With respect to automated processing, the accumulated set of data allows for more detailed interpretations and extensive profiling as well.

This does seem to affect a basic power balance, with citizens becoming increasingly powerless against a ubiquitous, invisible, but hardly infallible, system of control.

3 Tensions with EU legislation

The potential for the above issues to emerge with the type of system under discussion, is indicative of a serious tension between these developments and the existing regulatory and legal framework within the EU.

⁹ Jain et al. (2004) p.7

In this section we briefly reiterate the principles, rules and regulations that are pertinent here.

Data protection as defined in the Data Protection Directive is generally geared towards **user empowerment**: principles such as informed consent, awareness, and possibilities for objections and demanding corrections, are all attempts to strengthen the position of individual data subjects in relation to data controllers.

However, as mentioned earlier, in the type of biometric system that covertly monitors and assesses from a distance, the individuals intended to be protected by these principles of user empowerment, can hardly still be defined as 'users' in any meaningful way: they (often) do not actively or consciously interact with the system, nor can the end to which the system is the means be assumed to be theirs (in an individual, personal sense that is; of course it could be argued that the public ends said to be served this way are shared by all individuals at whom the system is directed). From this it would seem to follow that principles like awareness, consent, or right of correction will be of little use.

When considering authentication and identification systems in enclosed workspaces, these issues take on a different aspect. Here, a lot can be achieved through the conditions stipulated in the contract between employer and employee, although employees are entitled to the observation of certain limits to the extent and nature of the surveillance to which they can be asked to agree as well. Considering, however that in general employees are in a dependent position vis à vis their employers, third parties or independent overseeing bodies should audit the implementation and operation of such systems, ensure that workers are adequately protected, while eventually labor laws themselves may need to be adjusted to regulate these practices.

A first criterion in EU legislation, in particular in the Data Protection Directive, that seems relevant here would be the existence of a **legitimate purpose** for the deployment of these technologies. Although security and safety appear to be the most cited primary aims of these systems, another important impetus for their development, especially regarding soft biometrics and mood assessment, comes from the private sector, interested in new direct marketing tools. Whereas the first are in the perception of most citizens not controversial as such, the latter may very well be, in particular if it concerns application in public spaces, such as for instance 'smart billboards' installed in shopping malls.

Moreover, even in the case of apparent security and safety purposes, such as in crowd monitoring in airports, the motivation for taking recourse to these technologies, instead of relying on the currently deployed techniques and procedures, are in fact largely economic in nature: the costs of current security procedures, in particular in terms of human resources and passenger processing time, are very high, and airport authorities are above all interested in reducing those costs by installing systems that they hope require less time and effort to operate.

On a general level, the systems under discussion could make one well aware that assessing legitimacy of purpose *apart* from the means of achieving it, can only be a minor part of the considerations, and in itself be of little significance.

Immediately connected to legitimacy of purpose then, is another cornerstone of data protection law in Europe, the concept of '**proportionality**', which, as formulated in the Data Protection Directive, means that "the data must be adequate, relevant, and not excessive in relation to the purpose for which they are collected and/or further processed."¹⁰ Although there is little case law available on this subject, there seems to be good reason to believe that in many instances of the systems described the proportionality may be questionable at least. However, judging whether collecting certain amounts of certain types of data is or is not 'excessive' is inherently value laden: there is no uncontested calculus available for assessing 'proportions' of means and

¹⁰ Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

ends, or measuring costs and benefits. Consequently, there is a lack of harmonisation in the EU regarding the criteria to be used in assessing proportionality, which clearly is a critical issue.

An additional problem with this principle stems from the vagueness about the required level of specificity on which the 'purpose' should be defined. One could either define the purpose of, e.g., a particular physiology based authentication system in general terms like 'improving security of this critical infrastructure', or in highly specific terms like 'authenticating the user in a continuous, nonobtrusive, convenient, and afterwards auditable way' (in other words, the 'purpose' might be defined as the function the system is intended to perform); In the first formulation, much more space remains for seeing the system as one of more possible alternatives, and potentially evaluating the system as 'disproportionate'. For example, and contrary to what one might expect, The Privacy Impact Assessment (PIA) of the FAST project developed for the US DHS (see *Airport of the Future?*), and conducted by the DHS Privacy Office,¹¹ does not assess the potential of such a system to infringe on the privacy of the public subjected to it when it will be in operation, but merely assesses privacy implications of the *research* on the project. So when the purpose of the implied collection of sensitive personal information is defined, it regards the *testing* of the suitability of various types of sensors and their comparison as the goal of the research, rather than, say, surveilling the public at large. Moreover, since, in this research phase, the information is collected from 'volunteers' participating in the tests, who therefore can be considered as consenting to being subjected to the system, no serious privacy problems are identified.

Despite such difficulties one can foresee in applying this criterion, however, there is an undeniable common sense relevance to it, which underscores the need for clarification of its rules of application.

As said, any 'calculation' of proportionality implies an assessment of the material and immaterial costs, in order to weigh these against the value of the purpose. This is inherently value laden and not amenable to neutral calculation. However, it is clear that, on the cost-side of the equation, several fundamental values, enshrined in, amongst other, the Charter of Fundamental Rights of the European Union, and the European Convention for the Protection of Human Rights and Fundamental freedoms are indeed at stake.

To begin with, the principle of **non-discrimination** prohibits using many of the specific characteristics used in soft biometrics (e.g. gender, ethnicity, skin color, age) as criteria in decision making, including automated decisions; moreover, this applies not only to identifiable individuals, but also to anonymous group members (group profiling)¹²

Furthermore, the body data collected in these systems, are, for the most part, to be considered as sensitive personal data: data (more or less directly) related to health or sex life, ethnic origin, the processing of which falls under an especially strict regime as laid down in the Data Protection Directive, because of the potential for discrimination.

A basic principle in criminal law, the **presumption of innocence**, may become threatened when security practices start treating members of the public, such as in the airport case, as suspects on the basis of their biometric profile. Even if merely to select those 'worthy of further inspection', the effect of such a practice will be that one will have to explain oneself, and 'prove' one's innocence (no 'bad intentions') in order to pass security.

One of the most worrisome aspects of the technologies described generates from the clear threat to privacy, and, in particular to **bodily integrity** that they pose. More than mere collection of data and information - however 'sensitive' these may be

¹¹ Privacy Impact Assessment for the Future Attribute Screening Technology (FAST) Project, Department of Homeland Security, Washington, December 15 2008

¹² Wright and Gutwirth et al. (eds) *Safeguards in a World of Ambient Intelligence*, Springer, 2008, p. 99

considered - the biometric systems aiming at internal physiological states cross a boundary that concerns the integrity of the body as such. This is exacerbated when sensors are used that pick up these bodily states and processes from a distance from (possibly unaware) subjects. The fact that it is mostly contactless sensors that are employed does not alter the fact that subjecting people in public spaces to this type of surveillance effectively amounts to *dragnet bodily searches*, and as such is probably in breach with every currently existing law and regulation concerning bodily searches.

4 Next steps: setting conditions

Considering the serious nature of the issues at stake with the implementation of the technologies under consideration and the inherent tension with various important elements in current EU legislation and regulations, the following question suggests itself:

Is it possible to formulate conditions under which any of these systems could be used legitimately and responsibly, and if so, what would a minimum set of such conditions consist of?

The next meeting of the HIDE Focus on Biometrics in Embedded Systems and AmI will have on its agenda :

- Reviewing, discussing, and, where necessary, amending the current document, which is the intermediary deliverable Ethical Brief.
- Formulate tentative answers to the above question.

Maastricht, May 2009