

**SEVENTH FRAMEWORK PROGRAMME
THEME 3
Information and Communication Technologies**



215372

Comprehensive Report on Ethical, Legal and Privacy Issues Raised by the ActiBio Technologies

Deliverable No.		D8.3	
Work package No.	WP8	Work package Title	Human, Social, Ethical and Regulatory Implications
Activity No.	A8.2	Activity Title	Legal and Ethical Issues and Project Policy
Authors		CSSC - Holly Ashton	
Contributors		Emilio Mordini	
Status (F: final; D: draft; RD: revised draft)		F	

CONTENTS

1	Introduction.....	3
2	Ethical Issues	4
	2.1 The Ethical Manual.....	4
	2.1.1 Five Key Privacy Issues.....	7
	2.2 Privacy Enhancing Technologies (PET).....	9
	2.3 Ethical Issues Specific to the ActiBio Technology	11
	2.3.1 Dynamic Behaviour Profiling.....	11
	2.3.2 Physiological Response to Events	13
	2.3.3 Unobtrusive Sensors	14
	2.3.4 Soft Biometrics	14
3	Legal and Privacy Issues	15
	3.1 International and European Legislation Concerning Biometric Technologies.....	15
	3.2 Relevant National Legislation	15
	3.2.1 Greece	15
	3.2.2 Spain	16
	3.2.3 Switzerland	16
4	Conclusions.....	17
	Annex 1 – Data Collection Consent Form	18
	Annex 2 – International Conventions and Declarations relevant to ActiBio	22
	Annex 3 – Communications from the EC, EC Green Papers and Opinions of the European Data Protection Supervisor.....	23
	Annex 4 – Opinions of the Article 29 Working Party.....	24
	List of Tables	
	<i>Table 1</i> – Ethical Issues Raised by Biometric Technologies	5
	<i>Table 2</i> – Guidance Concerning Security and Identity Theft in the ActiBio Project	9
	<i>Table 3</i> – Ethical and Privacy Issues Raised by the Dynamic Behaviour Profiling Technologies	12
	List of Figures	
	<i>Figure 1</i> – Recommendations Concerning Behavioural Biometrics	13
	<i>Figure 2</i> – Recommendations Concerning Electrophysiological Biometrics	14

1. Introduction

The purpose of this document is to provide a report on the ethical, legal and privacy issues relating to the technologies being developed by the ActiBio project. As described on the project website¹, the aim of ActiBio is to research and develop a completely new concept in biometric authentication, i.e., the extraction of biometric signatures based on the response of the user to specific stimuli while performing specific work-related activities. The novelty of the approach lies in the fact that the technology being developed will be fully integrated in an Ambient Intelligence infrastructure and has the capacity to be completely unobtrusive.

The notion of ‘biometrics’ as a method for authentication can be provocative of quite emotive and fearful responses from the general public² and ActiBio is moving this field further forward in previously unexplored ways. As such, it is vital that the project is able to provide clear evidence that the technology being developed is being explored and created in an ethically responsible manner and with consideration of the laws and privacy guidelines set in place by the European Government concerning factors such as privacy, data protection and so on.

In this document an outline of the work that has been carried out to date in the ‘Human, Social, Ethical and Regulatory Implications’ work package (WP8) will be given, providing an outline of the key issues that have been raised and explored in the first year of the project. It will start with looking at the ethical issues and detailing how the project is dealing with these. It will then provide an outline of the legal and privacy issues facing the project and will summarise their relevance to ActiBio, including ways in which the project is ensuring their adoption throughout the project lifespan. The document will conclude with a summary of why the ethical, legal and privacy issues are being taken seriously and with a look at how this will continue to be the case in the coming years of the project.

¹ <http://www.actibio.eu:8080/actibio>

² See the deliverable D8.2 for a report on Public Perceptions of these technologies.

2. Ethical Issues

As pointed out in the introduction section, biometrics in general are an emotive topic to members of the public and new technologies relating to this field will be greeted with wariness. The greatest fears relate to the potential for misuse of these technologies for example in its potential to be used to control people and take away liberty. The Ethical manual produced for D8.1 explored the ethical issues facing the ActiBio project and provided guidelines for the developers to pursue in keeping with ethical best practice. The resulting document was a comprehensive and important manual containing much useful information.

In this document we will summarise the key issues and guidance described in the manual as well as highlighting the sections of the manual that directly apply to the technology being used in the ActiBio project. We will also discuss the concept of 'Privacy Enhancing Technologies' (PET). In this way, an in-depth ethical consideration and comprehensive discussion of relevant issues can be provided.

2.1 The Ethical Manual

The main goals of the ethical manual were to;

1. Collect a series of reflective considerations on the ethics of biometric technology and in particular on technology used by the ActiBio project
2. Collect and discuss existing ethical guidelines and privacy regulations relevant to the project
3. provide concrete guidance for research involving human subjects in ActiBio

Thus the first port of call was to consider ethical issues relating to biometric technologies in general (these can be seen in Table 1). Various concerns relating to privacy and human dignity are thrown up by this field. For example, at a basic level, is it acceptable to turn the human body into a token? And is the use of biometrics warranted in line with the benefits they can provide or are they simply a different and more obtrusive way of carrying out procedures and checks which can be done just as efficiently using other, less controversial means? There are also issues relating to the specifics of data storage, law enforcement and how to govern the use of such technology. These are all issues which relate to ActiBio and it is important for this reason that the project works in line with international guidelines relating to such topics.

Different types of biometrics also raise different ethical issues. Within the ActiBio project, three types of biometrics will be deployed; behavioural (activity-related), electrophysiological and soft. Concerning activity-related biometrics, these will be detected by sensors in the environment, as well as wearable sensors – both designed to be 'unobtrusive'. It is important that the ethical issues for each

type of biometric being used within the project have been properly considered ahead of the technology development/Pilot phase.

Behavioural biometrics are those which use measurable activity as a way of recognizing people. Examples include gait recognition, signature recognition (analyzing dynamics) and facial movements. It would be possible using behavioural biometrics to discover certain medical conditions (for example, behavioural biometrics could give away information about musculo-skeletal

Table 1 – Ethical issues raised by biometric technologies

ETHICAL ISSUES RAISED BY BIOMETRIC SYSTEMS AND APPLICATIONS
GENERAL QUESTIONS RELATED TO THE NATURE OF BIOMETRIC TECHNOLOGY
Do biometrics respect human dignity or do they turn the human body into a “token”, a “passport”?
Do biometrics erase the historical, biographical, dimension of human identities by substituting names with codes?
When is the use of biometrics proportionate to their benefit?
Are biometrics personal data? Are they sensitive data? What level of protection do they deserve?
Biometrics and Human Dignity
Biometrics and Privacy
Conditions for biometric research involving human beings (e.g., informed consent, respect for autonomy, not harm, data handling, etc.)
ISSUES RAISED BY SPECIFIC BIOMETRIC APPLICATIONS
Large-scale applications (e.g., airports, biometric passports, etc)
Biometric databases
Remote and covert biometrics
Biometrics and Medicine
Biometrics and the Internet
Biometrics and e-government
Biometrics and Law Enforcement
QUESTIONS RELATED TO EMERGING SOLUTIONS AND TECHNOLOGIES
Biometrics data sharing
System interoperability, multiple biometrics and multimodal systems, technology convergence
Embedded biometrics, ubiquitous computing and Ambient Intelligence
Behavioral biometrics and intention detection
People-hard-to-enroll (disabled people, older, children)
Biometrics and Ethnicity
Biometric profiling and soft biometrics
Technology Convergence

disorders such as Arthritis, and neurological/psychiatric conditions by detecting abnormal behaviours) and also to gain insight into an individuals’ intentions and emotional states.

Electrophysiological biometrics are those which use the naturally emitted electrical signals given off by human bodies as a biometric signature. Like behavioural biometrics, they are capable of giving away information about an individuals medical conditions (e.g. cardiac irregularities, neurological conditions, seizure disorders, sleep disorders, metabolic or structural encephalopathies, pre-clinical deficits in multiple sclerosis). Particular fears include the following;

- That employers could be tempted to covertly verify employees' medical conditions and to screen and sort employees according to their medical conditions and risks to develop specific diseases
- That people may unwillingly receive a medical diagnosis or get referred to their GPs
- That legal controversies could be generated by missed or wrong medical referrals, or by a lack of communication about incidental medical findings

In order to reduce the risk of these, it is vital to provide exhaustive and effective information to the data subject and to involve them in the decision about the policy to be followed should incidental medical findings occur. It is also crucial to ensure that no discrimination against the subject will be carried out because of the disclosure of previously unknown medical conditions.

Electrophysiological biometrics may also disclose information about psychological states and there are some fears that they could be used as a means of covertly carrying out lie-detection or studying the emotional states of subjects. For this reason, excellent privacy practices would need to be in place to ensure respect of personal dignity and to maintain psychological integrity. In fact, recommendations concerning this type of biometric can be summed up by the need to maintain;

- Respect for human dignity
- Respect for body integrity
- Respect for fair and just working conditions

Finally, soft biometrics. These are biometrics which by themselves cannot be used to individualize a person but which may be useful in distinguishing between groups. Weight, age, gender and race are all examples of soft biometrics. These may reveal a lot of information about an individual including things such as religious beliefs, medical conditions and ethnicity. As such, they are obviously potentially ethically controversial. Indeed thirty two pages of the ActiBio Ethical Manual are dedicated to describing the potential hazards/issues raised by each soft biometric, and in providing guidance for how to use them.

The most important recommendations to take note of are that;

- Soft biometrics based on race and ethnicity should be banned
- Soft biometrics based on age and gender, should be used with great caution
- All other biometrics are ethically tenable (with some caveats)

The reason for caution is that most soft biometrics are based around stereotypes and lack proper scientific integrity. However, this does not deny the fact that they may also be useful in providing additional authenticating data. As long as technicians are careful with how the soft biometrics are used, they will be a useful addition for the project.

In relation to all the biometrics to be used in ActiBio, five key privacy issues face them; transparency, consent, proportionality, extraction and use of additional

information and finally the issue of security and identity theft. We will now look briefly at each of these in turn to assess how they relate to the ActiBio project.

2.1.1 Five Key Privacy Issues

TRANSPARENCY – This relates to the fact that the use of biometric technologies in a given environment must be made clear to those being surveilled by the technologies. Given that the ActiBio technology aims at the development of an unobtrusive authentication system - in other words, a system which goes about the job of authenticating those in the workspace in a manner which will not disturb the working environment because it will not be visible - the fear is that in the wrong hands, ‘unobtrusive’ could be reinterpreted as ‘covert’ or ‘unknown’. This would put the technology on a slippery slope towards function creep³. Whilst such function creep rarely results outright from intended abuse of the system, it may be a result of exploiting the internal potentialities of a technology up to their legal limits. As the boundaries for these limits are pushed more and more, the technology may eventually be being used in a manner distinctly set apart from that which it was originally intended for. It is therefore important that the system will blend into the background but it is equally important that in doing so, it will not infringe on the privacy rights of those it is monitoring and that it will be designed in such a way as to safeguard as much as possible against the function creep mentioned above. Thus, at the same time as creating technology which is unobtrusive, it is important to also consider what measures can be put in place to ensure that end users are aware of the technology being used around them. In other words, to maintain transparency.

For this reason, guidance has been issued (in the ethical manual) which advises that there should be a system notification mechanism within the sensor network system which makes the subject aware that they are merged into a sensor network and are being continuously authenticated. Further to this, it is noted that all users of the system should be informed on the quality of the system and on biometric reference data. It can be noted that perhaps the enrollment phase for using the technology would be a good moment to educate users on the sensors being used and how they fit into the working environment.

The ActiBio ethical manual notes that;

“in the EU no single data collection can go unnoticed of the subject that is being monitored (that is, as long as the subject can be personally identified). The ActiBio system is not suited for covert operation, because subjects must enroll themselves. Yet subjects could be monitored without being aware that the process of authentication is continuous. In comparison to other biometric applications/systems, ActiBio architecture presents two particularities that may pose some privacy problems,

³ For more on Function Creep see the article by Mordini, E. & Petrini, C. (2007) *Ethical and Social Implications of Biometric Identification Technology*, Ann Ist Super Sanita, 43 (1), 5-11

- **Continuous authentication:** while standard biometrics are based on one time authentication, which takes place once, ActiBio will provide for a continuous authentication throughout the entire duration of that user's access to the monitored area.
- **Invisible sensor network:** ActiBio authentication is going to be almost invisible because it is partly embedded in objects (sensing seat, clothes, jacket), or based on not immediately perceivable cameras. Sensors will be multiple and will collect a wide variety of information about a persons' behavior, physiology and physical (morphological) aspect."

One way to protect the privacy rights of employees using a system such as ActiBio could arise from the use of transparency enhancing tools in order to make personal data collection and processing in ubiquitous environments more transparent. In a section below, we discuss the notion of 'Privacy Enhancing Technologies' ('PET').

CONSENT – Obtaining the consent of subjects to be authenticated by the ActiBio technology is a vital step in ensuring ethical integrity is maintained. Without obtaining consent, the surveillance performed would be covert and a huge invasion of the privacy of the individuals being authenticated – this could be happening against their will. It must also be noted that it may occur that in some situations, people may feel 'blackmailed' into consenting to being surveilled/authenticated by the technology (for example if the technology is introduced in a work place and workers would lose their jobs if they do not agree to working with it), it was therefore suggested in the ActiBio guidance that there should be a possibility to selectively disable some of the sensors within the network so that if someone has a particular concern with a certain biometric, they are still able to use the system overall but without that biometric being captured.

The consent forms for ActiBio have been carefully thought out and have also undergone a review by the ActiBio Ethical Advisory Board in order to ensure that they are clear and cover all relevant issues. A copy of the data collection consent form can be seen in Annex 1.

PROPORTIONALITY – The technology used must be proportionate to the need. In the instance of the ActiBio technology, this means that it's use can only be justified in high security areas (such as control rooms of nuclear facilities or cabins of vehicles carrying sensitive/dangerous goods). This ensures that the invasion of privacy it entails would be proportionate with the need to maintain extremely high security in these areas.

EXTRACTION AND USE OF ADDITIONAL INFORMATION – With all biometric technologies there is a possibility (or even probability) that they will detect things other than and in addition to the things they are set up to measure. For example, they may provide information about the time that an individual performed an activity, or even, at the most basic level, they give information that a person has or has not performed the activity. This is the ability for biometrics to leave a trace or 'footprint' of an individual. For this reason, it has been recommended that the ActiBio technology does not retain any raw data that is not directly relevant to the authentication of an individual. Any additional

information obtained should be discarded and data collection should be minimized to only include that which is necessary to the ultimate purpose of ActiBio.

SECURITY AND IDENTITY THEFT – A system gathering so much personal information on individuals needs to guarantee absolute security for those enrolled into it. Should a breach in security occur it could have drastic and negative consequences both for individuals and also for the environments in which they are working. For this reason, various guidance points were provided concerning these issues within ActiBio as can be seen in Table 2.

Table 2 – Guidance Concerning Security and Identity Theft in the ActiBio Project

Security and Identity Theft	
8	Non-biometric personal data should not be stored together with biometric reference data. A closed system for non-biometric data should be used having no network access.
9	Apart from sensors no other components or interfaces of the biometric system should be accessible to users
10	Reference data can be stored fragmented and different encryption keys could be used for these fragments. Alternatively a personalized token with the decryption key can be used to access the biometric reference data.
11	All data should be <u>pseudonymitised</u>
12	Protective measures against infiltration with unauthorized reference data should be provided
13	Detection measures for copies of biometric characteristics should be provided
14	Physical protection of core parts of the systems and access control measures should be provided
15	Logging of transactions and appropriate auditing of the systems should be provided

In order to efficiently deal with these five issues, three key principles must be maintained. These are the principles of dignity, freedom and equality/fairness. The moral integrity of the researchers must also be maintained at all times.

2.2 Privacy Enhancing Technologies (PET)

In the following paragraphs we provide an overview of how privacy is perceived and how it can be embedded into technologies and systems similar to ActiBio.

In a useful paper, Marc Langheinrich⁴ discusses the notion of privacy in relation to ubiquitous computing systems (or ‘ambient intelligence’ as used in ActiBio) and highlights several areas of innovation that future research will need to focus on when designing systems in order to comply with privacy legislation. As he notes, “..what should also be within our reach is achieving a good balance of convenience and control when interacting with ubiquitous, invisible devices and infrastructures.”

The first area of note is that of openness or, giving notice to those whose data are being collected. This is basically transparency as outlined above. Langheinrich

⁴ Langheinrich, M. (DATE) Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems, SOURCE

proposes that in rooms or buildings, it would be reasonable to use an announcement system to alert those in the vicinity to the fact that data collection technology is being used. He notes that in such a case, it would not be necessary to identify every single device being used – it would be enough for example to say that auditory data was being collected without naming all the individual sensors gathering the data.

The second area refers to choice and consent. The author notes that it is not enough to merely alert people to the presence of data collection technologies, but their informed consent must also be obtained. Indeed Langheinrich (p.11) also raises the issue of ‘blackmail’ and notes that it is vital to incorporate some kind of ‘take it or leave it’ dualism (Langheinrich, p.11) into the set-up so that people have some control about what elements of the system they accept. Again this is in line with the recommendations provided to ActiBio.

The third area discussed by Langheinrich is that of anonymity or pseudonymity. Anonymity is a state whereby an individual is not identifiable within a set of data that includes a number of other individuals. Complete anonymity is not practical however in situations where authentication is required. As an alternative, pseudonymity can be used instead. This assigns each individual in a system to an alternative ID which can be used to ‘identify’ them enough for authentication whilst enabling them to remain anonymous. The threat to be careful of when using pseudonymous systems is that it must not be possible to link the individual to their pseudonym, as obviously, if this were possible, the anonymity would be a mere illusion. This is quite a danger, especially with the advent of ever improving data-mining technology which allows even remote coincidences to be grouped into a single coherent picture. In Germany, privacy commissioners have called for severe restrictions to be placed on the use of data-mining applications, but Langheinrich notes that their call might not be a realistic one. In ActiBio pseudonymisation of data will be performed with various security measures in place. These are an issue for the technical workplan and as such sit outside of the ethical recommendations remit – they can be seen in the deliverable D6.3⁵. This deliverable was however reviewed by CSSC and no issues of ethical concern were noted.

Another area discussed relates to the notion of security. Langheinrich points out that talk of privacy usually results in discussion of security measures as it is often taken for granted that resolving security issues within a system will automatically enhance its ability to protect privacy. In a high security environment, a sensor network such as that being developed for ActiBio must be especially secure as it must not only respect the privacy needs of the employees using the system, but it also acts as a vital protection to the environment where it is in place. Thus if someone were able to override the security measures in place, as well as threatening the privacy of those enrolled in the system, they would be endangering the critical infrastructure being protected.

⁵ D6.3: “Security, data and system integrity and privacy protection recommendations”

A final point refers to collection and use limitation. Langheinrich comments (p.15) that along with anonymization or pseudonymization, ensuring that data collectors;

- *only collect data for a well-defined purpose (no “in-advance” storage)*
- *only collect data relevant for the purpose (not more)*
- *only keep data as long as it is necessary for the purpose*

is the best way to ensure that time and effort is saved concerning the proper collection, protection and management of large amounts of sensitive personal information. These three points are of course well adhered to within the ActiBio framework and as such, the data policy seems to be responsible and acceptable.

A communication from the European Parliament⁶ writes of promoting data protection via the use of privacy enhancing technologies (PETs). 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 clearly relates to the technology developers within the ActiBio project and once again highlights the responsibility for the project to design the ActiBio network responsibly. 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.

Again, ActiBio plans for incorporating PET can be seen in the previously mentioned deliverable, 6.3.

2.3 Ethical Issues Specific to the ActiBio Technology

The sensor network being developed in the ActiBio project incorporates certain specific biometric technologies. Though these were covered in general terms by the Ethical Manual and in the section above, we shall now build up a more in-depth ethical profile of each of the elements within the ActiBio network.

⁶ COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on Promoting Data Protection by Privacy Enhancing Technologies (PETs), Brussels, 2.5.2007 COM(2007) 228 final

2.3.1 Dynamic Behaviour Profiling

The dynamic behaviour profiling in ActiBio incorporates gait, body and face dynamics and gestures. These will be measured by a number of sensors and cameras within the network.

Profiling dynamic behavior raises a number of specific ethical and privacy issues which are set out in the table below.

Table 3 – Ethical and privacy issues raised by the dynamic behaviour profiling technologies

Modality	Issues Raised
Gait	Using gait as a biometric includes the potential for inferring information concerning various medical conditions including; <ul style="list-style-type: none"> • Psychiatric conditions (e.g. dissociative disorders, acute anxiety/panic, major depression) • Neurological conditions (e.g. movement disorders) • Musculo-skeletal and articulation disorders (e.g. foot and ankle disorders, joint disorders)
Body Dynamics	As with gait, body dynamics in general may give away information concerning a person's medical background.
Face Dynamics	Facial dynamics unavoidably gather information on facial expressions, and by doing so, can be used to understand a person's basic emotions, what they are thinking and feeling. This kind of information being available in a work place could be extremely intrusive on the privacy rights of employees. Abnormal facial dynamics could also give away medical information for example relating to the occurrence of a stroke.
Gestures	Gestures may be voluntary or involuntary and can give away much information about an individual. For instance, body language can disclose information including confidence, honesty and comfortableness with the environment. Use of abnormal gestures could also (again) highlight medical conditions, both physiological and psychological in nature.

There is thus much potential within the ActiBio sensor network for the capacity to detect medical conditions and to infer certain things about people's emotions and intentions around the work place. In addition to this, activity-related biometrics could at a more fundamental level, be used to simply check if an individual is doing the tasks they are supposed to be doing. This would be an abuse of the system and would go against its intended use.

The need to carefully consider how the technology for body dynamics could be used out of context of the authenticating system being developed for high security infrastructures leads to a number of recommendations concerning the ethical use of biometrics devices for the capturing of bodily dynamics. These were covered in the ActiBio Ethical Manual⁷ and can be seen in brief in the box below.

Figure 1 – Recommendations Concerning Behavioural Biometrics

- 1) *Behavioral patterns used for authentication purposes must be clearly defined and framed. Too broad and complex series of actions should be avoided.*
- 2) *Only data essential for authenticating the subject are retained by the system; additional personal details will be not collected or, when they are necessarily collected as ancillary information, will be automatically filtered by the system before being processed*
- 3) *No data is permanently stored*
- 4) *The subject is properly informed and has given his explicit consent*
- 5) *The subject has the right to access his personal information, correct inaccurate information, and pursue legally enforceable rights against data collectors and processors who fail to adhere to the law*

2.3.2 Physiological Response to Events

Physiological response to events will be detected by the use of EEG and ECG using ENOBIO sensors within the ActiBio system. It has been noted that the sensors to be used could be capable of extracting dynamically changing, physiological activity related to mood or intense cognitive activity. Thus as well as potentially being used to extract information concerning, for example, sleep deprivation or alcohol intake, the sensors could also extract information about basic emotions. The potential to do this within a system deployed purely for authentication purposes raises a number of ethical issues.

First, using electrophysiological signals for authentication purposes implies a risk of intrusion on the fundamental rights and privacy of those working in the ActiBio environment. It could imply a certain lack of concern relating to the privacy of the mental contents of employees. At its most fundamental level, the issue here concerns respect for human dignity.

Another issue concerns respect for body integrity. Electrophysiological signals are more associated with the medical profession and can be used for the disclosing of a number of serious medical conditions. It could be argued that recording and using electrophysiological signals outside of the medical framework and without medical justification, could trespass on usual ‘body boundaries’ and could even be interpreted as a humiliating procedure.

⁷ ActiBio Ethical Manual chapter 3.4 ‘Recommendations about Behavioural Biometrics in ActiBio’ p.103.

A third issue concerns respect for fair and just working conditions. In essence this raises the issue that the use of electrophysiological signals as a biometric may inhibit a persons' right to dignity at work.

With these points in mind, recommendations were given in the ActiBio Ethical Manual concerning the use of electrophysiological signals as biometric authenticators. These can be seen below⁸;

Figure 2 – Recommendations Concerning Electrophysiological Biometrics

- *Collecting electrophysiological signals for authentication purposes is only exceptionally justified for the purpose of protecting critical, high security, infrastructures, in so far it is authorized by national law providing for appropriate specific safeguards, and provided that there is no less intrusive means to achieve the same purpose.*
- *In order to judge whether all particular circumstances of each case have been evaluated, the rights of the person concerned should be assessed against manifestly overriding interests of the society, notably serious security risks to the public in the context of security-sensitive jobs.*
- *A prior check by a national supervisory authority should be always considered before implementing the system.*

In terms of ActiBio, it is clear that the purpose for which the technology would be used is in line with the recommendations given regarding electrophysiological biometrics.

2.3.3 Unobtrusive Sensors

Within ActiBio, unobtrusive sensors will play a pivotal role in the ambient intelligence infrastructure. Such sensors will be either wearable (in garments such as gloves) or will be integrated into the infrastructure for example in the use of 'sensing seats'. As with electrophysiological sensors, unobtrusive sensors have the potential to be a little controversial, particularly as they may not even be evident in the environment. It is vital therefore that within the ActiBio project, participants are made aware of the sensors being used. As far as the researchers/technology developers are concerned, they must be able to guarantee that only data relevant to authentication will be collected.

2.3.4 Soft Biometrics

Certain soft biometrics will be used in the ActiBio project. These include; age, hair colour, eye colour, skin colour, height, weight, gender, glasses, beard and make-up.

⁸ As taken from ActiBio Ethical Manual

As previously mentioned, the ActiBio Ethical Manual provides much detailed information about the ethical issues surrounding a number of soft biometrics, including those to be used within the project, thus for a clearer outline of such issues, a look at the Manual is recommended.

3. Legal and Privacy Issues

The safest way to ensure that ethical integrity is maintained is to adhere to relevant legislation set in place to protect the rights of the individuals using biometric technologies. Below we highlight the relevant international and European declarations, conventions and directives which may impact on biometric technology and thus the technology being developed in ActiBio. We will also contemplate the specific legislation of the countries where data gathering and tests of the ActiBio technology will be carried out.

3.1 International and European Legislation Concerning Biometric Technologies

All ActiBio partners will be expected to respect relevant international conventions and declarations (listed in Annex 2), communications from the European Commission to the Parliament and Council, EC Green Papers and opinions of the European Data Protection Supervisor (all in Annex 3) and also the opinions of the Article 29 working party (Annex 4).

These conventions, opinions and papers cover such topics as fundamental human rights, data protection, critical infrastructure protection, security and availability of data, the inclusion of biometric elements in passports, travel documents, visas and the like. These are topics that are highly relevant to the development of new biometric technologies and as such, it is important that the technology developers on the ActiBio project are aware of them.

3.2 Relevant National Legislation

Within ActiBio, data collection and testing of systems in the form of PILOTS will be carried out in three countries; Greece, Spain and Switzerland. It is important to take into account the national laws relevant to each of these countries in order to carry out the data collection within the boundaries of the law. Indeed, the Ethical Manual explored this legislation and included it within its contents. Here we provide a brief summary/overview of the laws applicable in each of the three countries.

3.2.1 Greece

Law 2472/1997 of the Hellenic Parliament

Relevant regulatory authorities and ethical committees include:

1. Hellenic Data Protection Authority <http://www.dpa.gr/>
2. The Hellenic Parliament – Standing Committee for TA [<http://www.parliament.gr/>]
3. The National Bioethics Commission <http://www.bioethics.gr>

Relevant decisions issued by the Hellenic Data Protection Authority:

1. Decision 52/05.11.2003 Biometric data in International Athens Airport
2. Decision 9/31.03.2003 Biometric technology in Athens Metro high-risk installations
3. Decision 63/2004 CCTV cameras on the Attica road network
4. Decision 58/2005 Traffic Management Cameras

3.2.2 Spain

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Título VI con rango de ley ordinaria).

Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos

Ley 5/2002 (Comunidad Autónoma de Cataluña), de 19 de abril, de la Agencia Catalana de Protección de Datos.

Relevant regulatory authorities and ethical committees include:

- Agencia de Protección de Datos: website <https://www.agpd.es/>
- Fundación Española para la Ciencia y la Tecnología (FECYT) <http://www.fecyt.es/>

Relevant decisions issued by the Agencia de Protección de Datos:

- PS/00109/2004 - Resolución de fecha 10-12-04 (Artículo 5.1 LOPD) (RESOLUTION),
- 2004 Videovigilancia en el lugar de trabajo (REPORT), 2001
- Instrucción 1/2006, of 8 November, by the Spanish Data Protection Agency, on processing personal data for surveillance purposes through camera or video-camera systems, 2006
- Seguridad en la comunidad de Vecinos. Criterio anterior a la Instrucción 1-2006, 2006
- Videovigilancia en los colegios, 2006
- Uso de cámaras para analizar hábitos de consumo, 2006
- Cuestiones Generales sobre Videovigilancia, 2006
- Instrucción 1-2006, Informe Jurídico 0019/2007, 2007
- Deber de informar en videovigilancia, 2007
- Medidas de seguridad, 2007
- Cartel informativo, 2007
- Prevalencia en le ejercicio de derechos, 2007
- Clausula de Videovigilancia, 2007
- Banco tratamiento de imágenes, 2007
- La Videovigilancia en los parkings, 2007
- Grabación de imágenes en tiempo rea, 2007
- Cuestiones Generales de videovigilancia y ejercicio de derechos, 2007
- Legitimación para el tratamiento, 2007
- Videovigilancia en los taxis, 2007
- Cuestiones Generales, 2007

3.2.3 Switzerland

- Swiss Federal Act on Data Protection (DPA – 1992, status as per 2000)

Despite not being a member of the EU, Switzerland based this Act along similar principles to Acts in force in other European countries and the law won adequacy approval from the EU in 2000⁹.

- Commission Decision 2000/518/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland - Official Journal L 215/1 of 25.8.2000
- Swiss Data Protection Authorities;
http://www.privatim.ch/content/pdf/the_swiss_protection_authorities_text_slides_2006.pdf

4. Conclusions

Ethical, legal and privacy issues must be taken seriously in a project dealing with the sensitive issue of new biometric technologies – particularly ones designed to operate in an unobtrusive system.

As can be seen from this document, a number of ethical and privacy issues and considerations have been taken into account regarding the ActiBio project. As well as consideration of the specific issues relevant to the project, the notion of PET technologies in general has been explored a little to create a better picture of how ActiBio fits in with current thinking and recommendations on the use of these.

Specifics concerning different types of biometrics (e.g. activity-related, electrophysiological and soft) have been addressed as different types of biometric technologies may throw up different issues. As noted, various guidance points and recommendations have been made to the technology developers of the project – a full in-depth coverage of these, can be found in the ActiBio Ethical Manual.

Relative legal documents have been researched and listed so that they may be easily found and referenced by those who need to use them. This will ensure that any relevant legislation covering the topics of biometric/surveillance technologies, data protection, human rights and so on will be taken into account during the continuation of the project.

In summary, the ethical and legal work carried out within the scope of this project will ensure that ActiBio continues to operate within all necessary boundaries as it moves forward.

⁹ See <http://www.privireal.org/content/dp/switzerland.php>

ANNEX 1

*Universitat Politècnica de Catalunya (UPC)
Grup de Processament d'Imatge i Video
Departament de Teoria del Senyal i Comunicacions
Campus Nord UPC, edifici D5
Jordi Girona 1-3
08034 Barcelona SPAIN*

1. Purpose

The *Universitat Politècnica de Catalunya (UPC)* is carrying out a scientific research on a number of physical and behavioural features that may allow recognising people by using automated means. The overall goal of the study is to develop better technology for human recognition to be employed in situations in which it is paramount to be sure of the identity of the operating personnel (e.g., the operational room of a city metro, a plane cab, a driver's place in a bus, etc.). Additionally this technology could be also used to verify the identity of patients suffering from dementing disorders who are not able any longer to identify themselves. The study is part of a larger European research project called **ACTIBIO** (Unobtrusive Authentication Using ACTivity Related and Soft Biometrics), funded by the European Commission within the scope of the 7th Programme on Research, Technology & Development.

2. Procedure

In order to test the technology for human recognition, a number of physical and behavioural features will be recorded in a controlled environment, notably in a smart room. In the session you are invited to participate we will record signals from several cameras in the room, a pressure sensitive seat and a wearable, modular and wireless electro-physiology sensor system for the recording of EEG (Electroencephalogram - brain activity), ECG (Electrocardiogram - heart activity) and EOG (Electrooculogram - eye movement) known as [ENOBIO® by Starlab](#).

In this session, apart from the sensor signals you will be given a questionnaire by means of which we are going to collect the following personal characteristics:

- Age
- Height
- Weight
- Whether you wear glasses or contact lenses and its color
- Eye color
- Hair color
- Gender
- Facial hair (moustache/beard disposition, whether you are unshaved)
- Whether you have applied makeup

Each session will last approximately 45 minutes, and individuals may discontinue their participation at any time for any reason without any need to give an explanation for their will to stop their participation.

3. Personal data handling

Although the goal of the study is only to evaluate the capability to recognise people of these features, and data collected will not be used for any kind of medical or clinical diagnosis, notwithstanding you should be aware that it can happen that sensitive personal information about you can be disclosed during the study. In particular there is the possibility that

1. The technology detects any medical condition that affects you
2. The technology detects signs of a medical condition that you are not aware of
3. The technology detects signs of risk that you develop a medical disorder in the future
4. The technology reveals surgical treatments that you underwent to, including interventions of cosmetic surgery
5. The technology reveals a transgender condition and other form of transsexualism
6. The technology unravels details about your religious, political, philosophical beliefs
7. The technology reveals your emotional reactions, possible states of anxiety, and, more in general, provides a picture of your psychological conditions.

Your personal data will not be analysed by medical personnel, except electrophysiological signals, which will be processed by health care professionals or by personnel bound by rules on medical confidentiality equivalent to those incumbent upon health care profession.

Sensitive personal information not relevant to recognition, including medical conditions that you want to keep confidential, will not be retained and will be immediately erased. Should any incidental medical findings arrive, you will be immediately informed and advised to consult an MD. You should be aware, however, that in no way data captured for recognition purposes could be considered valid medical data. Any incidental medical findings must be considered only a generic warning signal to consult an MD.

All personal data stored during the pilot will completely and irreversibly anonymised or simply erased at the completion of the ACTIBIO Project.

No personal data will be ever used for any purposes different from those stated in this form. Your personal data will not be transferred to any third party or even commercialised. You may exercise your rights of access, rectification and deletion of data at any time. In order to do so, you will need to communicate it to *Universitat Politècnica de Catalunya (UPC)* by a letter addressed to

Josep R. Casas
Campus Nord UPC, edifici D5, Jordi Girona 1-3
08034 Barcelona SPAIN

or by e-mail to the following address: josep.ramon.casas@upc.edu.

4. Confidentiality

The researcher responsible for the data collection sessions will record the data collected in a file. These data will be identified only by a code and an identification number. The code of the study consists of a letter or digit to which a number assigned by the researcher is added after (eg, S01_02). The relationship between the ID number and your name is recorded in a computer and is stored separately and securely. This file will be accessible only to the principal researcher, *Prof. Josep R. Casas*. The key to link your name to the code which identifies the data file will not be provided to anyone and the privacy of your data will be protected. The results of the study could be published in books or magazines or could be used for didactic purposes. However, your name will be never revealed in any document, publication or teaching materials.

5. Right to get more information about the study

You can ask any questions about the study at any time throughout the record. The principal researcher will be available to answer your questions, interests or concerns about the study. You will be informed of any new discovery that could occur throughout the study and that may affect your participation in future studies. If during the study and thereafter you wish to discuss your rights as a person who participates in an investigation, your participation in the study or your concerns about it, or if you do not want to continue in that investigation or future researches, please contact the principal researcher, *Prof. Josep R. Casas*, at the address provided above (cf section 3) any time you wish

6. Refusal or cessation of participation

The participation in this *data collection session* is voluntary. You do not have to participate in the pilot if you do not want. If you choose to participate, you can change your mind or leave the study at any time without having to give explanations and without being yourself affected in any way. Similarly, at the discretion of the researcher responsible for the data collection sessions, you may be withdrawn from the study for any of the following reasons: (a) if the minimum requirements of the study are not met (b) if for any reason the study is interrupted.

7. Risks and discomforts

The personal risk by participating in this study does not exceed the risks of daily and normal life. None of the procedures represents a danger to the health or to the physical and mental integrity.

8. Compensation

You understand that there is no compensation for participating in this study, but a reimbursement for the working hour lost to participate, which is provided in the

form of a ticket for the lottery of an "iPod nano®" which will be drawn among the participants in this study (researchers involved in ACTIBIO are excluded).

9. Consent

By signing the present form, I understand and consent freely that my personal data, including biometric data, including my name and contact details, will be processed by the *Grup de Processament d'Imatge (GPI)* at the *Universitat Politècnica de Catalunya (UPC), Jordi Girona 1-3, 08034 Barcelona, Spain*, the data controller, and by appointed processors on behalf of the data controller, in accordance with applicable laws and with what is stated in the present clause.

I have been explained and informed of the research Project ACTIBIO and its purposes. I understand that some personal data may reveal directly or indirectly sensitive data, including health related data or data revealing age, religious or political affiliations, psychological conditions, and that this is necessary for the project

I declare to be aware that the data collected will not be used for any kind of medical or clinical diagnosis. I am aware that health professionals will not be involved in data processing (except in case of electrosignals) and in no case data collected in this study should be considered medical data. I am also aware that whether any (suspected) incidental medical findings arrive, I will be informed and suggested to consult an MD.

I understand that my personal data will be encoded in order to safeguard confidentiality, and that if results of the study are published, my identity will not be revealed. I also understand that I have the right to request access to my personal data, to correct, if applicable, and delete my personal data in conformity with the applicable legislation. For these purposes, I can contact *Prof. Josep R. Casas* at the address provided above (cf section 3).

I have read the above and I understand that I can refuse to participate in this study without any direct or indirect negative consequence on my life.

By signing the present form, I agree with the above stated.

Date: _____ Place: _____

Name: _____

Signature: _____

E-mail: _____ Telephone: _____

ANNEX 2

International Conventions and Declarations relevant to ActiBio;

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

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

European Framework Equality Directive, COUNCIL DIRECTIVE 2000/78/EC of
27 November 2000,
http://ec.europa.eu/employment_social/fundamental_rights/pdf/legisln/2000_78_en.pdf

Charter of Fundamental Rights of the European Union,
http://www.europarl.europa.eu/charter/docs/default_en.htm

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.
ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

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
ec.europa.eu/information_society/policy/ecomms/info_centre/documentation/legislation/index_en.htm

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
www.europarl.europa.eu/register/pdf/r1049_en.pdf

ANNEX 3

Communications from the European Commission to the Parliament and Council

- Promoting Data Protection by Privacy Enhancing Technologies (PETs) Brussels, 2.5.2007 COM(2007) 228 final
- Follow-up of the Work Programme for better implementation of the Data Protection Directive, Brussels, 7.3.2007 COM(2007) 87 final
- First Report on the implementation of the Data Protection Directive, COM (2003) 265(01), 15.5.2003,
- Communication on a strategy for a secure Information Society, COM(2006) 251 of 31 May 2006
- Implementing The Hague Programme: the way forward, COM(2006) 331 final Brussels, 28.6.2006

EC Green Papers

- Green paper on detection technologies in the work of law enforcement, customs and other security authorities COM(2006) 474, September 2006
- Green Paper on a European Programme for Critical Infrastructure Protection - COM(2005) 576, November 2005

Opinions of the European Data Protection Supervisor

- 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,
- 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
- 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
- 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
- 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

ANNEX 4

Opinions of the Article 29 Working Party

- 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)
- Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data
- Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities
- Working Document on the processing of personal data relating to health in electronic health records (EHR)
- Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities
- Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)
- Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data
- Opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement
- Opinion 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States
- Opinion 4/2006 on the Notice of proposed rule making by the US Department of Health and Human Services on the control of communicable disease and the collection of passenger information of 20 November 2005 (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71)
- Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995
- 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
- Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology
- Working document on data protection issues related to RFID technology

- Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines
- 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.
- [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)]
- Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America
- 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)
- Opinion 6/2004 on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection.
- 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
- Joint Statement in response to the terrorist attacks in Madrid
- Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance
- Working document on biometrics
- Level of Protection ensured in the United States for the Transfer of Passengers' Data