SEVENTH FRAMEWORK PROGRAMME

Networked Media

Specific Targeted Research Project

SMART

(FP7-287583)

Search engine for MultimediA environment generated contenT

D7.8 Ethical Dimensions of SMART technologies

Due date of deliverable: 31-01-2012

Actual submission date: 30-04-2012

Start date of project: 01-11-2011 Duration: 36 months

Summary of the document

Code:	**D7.8 Ethical Dimensions of SMART technologies**
Last modification: **State:**	10/04/2012 Final
Participant Partner(s): **Author(s):** **Fragment:**	ATOS, AIT, IBM, Imperial, Telesto, SDR D. Field, I. Schmidt, P. Moore, J. Soldatos, A. Pnevmatikakis, Z. Kons, J. Pitt, T. García Fresno No
Audience:	☒ public ☐ restricted ☐ internal
Abstract:	A report on the ethical dimensions of the envisaged technologies (including potential misuse). This deliverable will be initially delivered in M3 and it will be up-dated annually.
Keywords:	• *Ethics,* • *data protection,* • *rights,* • *Personal information*
References:	SMART DoW, D7.7 Data Protection Protocol, See within document for further references.

Table of Contents

1 Executive Summary

1.1 Scope

The main goal of the SMART project is to build a novel search engine for multimedia environment generated content. The project involves the deployment of outdoor sensors (notably cameras and microphones), which will become the primary data sources to be searched by the project's search engine. Along with sensor deployment the project develops and deploys advanced sensor processing and context extraction algorithms, which leverage signals derived from the outdoor sensors. The purpose of this deliverable is to highlight the main ethical aspects of the SMART project, including privacy and regulatory issues emerging from the deployment and use of outdoor sensors in densely populated environments (such as urban environments). It will therefore highlight the main ethical concerns associated with the project, along with relevant/possible solutions. Moving one step beyond the SMART project, the deliverable will also attempt to provide insights on ethical issues surrounding similar projects (i.e. projects deploying sensors and processing the relevant signals for extracting context associated with outdoor environments). Note that the present document corresponds to the first release of the deliverable. Successive releases are planned to be produced, during the evolution of the project and as ethical/privacy issues are confronted and resolved by the consortium. Furthermore, successive versions will report on best practices about ethical design and implementation of relevant applications. Some early insights in this direction are already provided as part of this first release.

1.2 Audience

The target audience for this deliverable is manifold and includes:

- **The members of the consortium**: Members of the SMART consortium (especially those involved in the development, deployment and operation of the SMART search engine) need to understand the ethical dimensions of the SMART infrastructure and services. The present deliverable aims at providing these insights in order to ensure that SMART developments are ethical, legal and privacy friendly.
- **Stakeholders involved in the SMART exploitation, sustainability and wider use**: The industrial partners of the consortium will endeavour to exploit SMART results in their business activities, as it will be reflected in their exploitation and sustainability plans. At the same time, the open source version of the SMART engine will allow the community to deploy similar applications. The present deliverable is relevant to all these stakeholders, since it could boost their understanding of the ever important ethical issues, while also providing insights on how these issues could be tackled.
- **Other projects (including EC-funded) projects dealing with similar topics:** The present deliverable provides insights into the main ethical issues associated with the deployment of applications that capture, process and visualized environment generated content. The number of such applications is proliferating, as a result of the increase in the number of sensors (including cameras and microphones) that are deployed in several places all over the world. Subsequently more and more projects and applications leveraging environment generated content will emerge. These projects could benefit from the discussion of issues and relevant guidelines presented in this deliverable.

1.3 Summary

This deliverable describes the ethical implications that are associated with the development, deployment, operation and use of the SMART technologies, thereby covering the full lifecycle of the SMART services. As part of the development of SMART services the deliverable identifies the need for collecting and storing audio and video data, along with the need to get ethical approvals from Data Protection Authorities (DPAs), notably DPAs responsible for areas/locations where the SMART system is deployed and operated. As part of the deployment and operation of the SMART system, the deliverable illustrates the components of the system (such as audio and visual processing components for context acquisition), which can raise privacy concerns such as tracking or identifying people.

Apart from analyzing the ethical implications of the technologies to be developed in the scope of the SMART project, the document provides insights on potential ethical implications of SMART technologies to be developed using the SMART core infrastructure, as part of community development and/or the project's sustainability plans. Such technologies (i.e. developed by third-parties independently of the project) can for example include filters for processing social networking streams, as well as additional visual and audio processing algorithms. The investigation of such (third-party) technologies was deemed necessary, given that SMART aspires to create an open source community around its multimedia search results.

Along with the identification of the ethical implication of the SMART technologies, the deliverable outlined possible measures that can be taken to alleviate ethical concerns, while also ensuring compliance to legal requirements. Furthermore, laws that have to be taken into account are identified. The deliverable opens also the discussion of the ethical-friendly design of SMART-compliant technologies. In this direction some initial best practices and design guidelines are provided. However, more insights and guidelines will be provided during the evolution of the SMART project, as part of following releases of this deliverable (which will be delivered annually in an iterative fashion).

1.4 Structure

The deliverable is structured as follows: Section 2 following this introductory section illustrates the main characteristics of the SMART platform and application, as well as why and how they raise ethical concerns. The section explains that the ethical issues to be tackled within this and subsequent versions of the D7.8 deliverable should not be confined to the scope of the SMART applications that will be implemented in the project, but it should rather address the full range of applications that could be built using the SMART open search framework (including open source community projects and implementations based on the SMART search engine). Section 3 details the main perceptive and sensing components to be developed in SMART, along with their ethical implications. Section 4 presents the laws and regulations that are applicable to the SMART platform and applications. These are the regulations that SMART has to adhere to. Section 5 illustrates measures that SMART solution providers have to employ in order to ensure the legal and ethical-friendly nature of their SMART deployments. The section outlines the important of Data Protection Agencies (DPAs) as part of the EU framework for ethical and privacy friendly applications. Section 6 provides some initial insights on guidelines for designing ethical and privacy-friendly SMART applications. This set of guidelines will be gradually enhanced, during the evolution of the project. In particular, subsequent releases of the project deliverable will provide more guidelines, best practices and measures for ensuring the privacy-friendly nature of applications built using the SMART architecture and/or platform. Such best practices and measures will be produced during the evolution of the project, based on the experience of developing, integrating and evaluating SMART components and applications. Section 7 is the final section of this deliverable, which presents a set of main concluding remarks associated with the first release of the deliverable.

2 Introduction

2.1 Overview of SMART Platform and SMART Applications

The main goal of the SMART project is to research and provide a open search framework for environment generated content, notably content and metadata derived from processing multimedia (i.e. audio and video) signals from the physical world. To this end, SMART will develop an architecture enabling the structured and disciplined integration of a scalable search engine, with components acquiring, processing, fusing and indexing content stemming from sensors deployed in the physical world (such as urban areas). Furthermore, SMART will provide tools and techniques for visualizing physical world content, through appropriate mashup libraries and in-line with recent advances in Web2.0/Web3.0 technologies. Also, SMART deals with the processing of social networks information, with a view to enriching or interpreting sensor network data streams. Overall, SMART is not limited to the development of a scalable multimedia search engine, but it also comprises components for acquiring, processing and visualizing environment generated content, as well as content stemming from social networking sites, Based on the SMART architecture, the project is developing the SMART platform, which comprises:

- The SMART search engine enabling indexing and retrieval of data collections comprising data and metadata relating to the physical world. This search engine is based on the Terrier.org open source search engine and will be provided as a set of open source software libraries.
- A set of middleware elements facilitating the integration of multiple sensors, perceptual components, social network feeds, and mechanisms for their intelligent fusion, with the SMART search engine. In the scope of the SMART validation scenarios the project will deal with specific sensors (such as cameras, microphones and temperature sensors) and perceptual components (such as crowd analysis, colour trend analysis and acoustic event classification). These validating scenarios will also leverage specific social networks and information fusion algorithms.

In order to validate its architecture and the openness of its framework, SMART is also designing and developing two proof-of-concept applications in the areas of live news and security surveillance. These applications will index content stemming from social networks and sensor networks (notably A/V sensors) in order to provide added-value news and security information to their end-users. Their main characteristic is that they are based on a number of queries to the SMART engine, including event driven and/or periodic queries.

While SMART will be allocating effort to the development of these validating applications, the scope of the project is not limited to these application domains. SMART intends to exploit its open nature (and open source libraries) as a vehicle for exploitation and impact creation beyond the end of the project. In particular, we envisage that:

- Enterprises (i.e. ICT solution providers) may use the SMART search framework in order to develop added-value solutions for their customers, in the same but also in other domains that those of the validating applications.
- Academics, researcher and open source developers (including the open source community) may engage in the implementation of creative ideas on the basis of the integration of novel perceptual components and social network processing algorithms. These ideas may span several application domains, including possibly unknown domains.

2.2 Scope of the SMART Ethical Aspects

SMART entails acquisition and processing of content and context from the surrounding environment, including out-doors urban environments. To this end, SMART applications will deploy perceptive algorithms enabling context extractions about the physical environment/world. The development and deployment of such components (in the scope of SMART applications) may entail ethical issues (including privacy issues). For example, although not foreseen in the SMART application scenarios, the project's open architecture could enable the deployment of perceptive algorithms that track people and their behaviour, which could raise privacy concerns. Note that an analysis of ethical/privacy concerns associated with the audio and visual com-

ponents that are developed in the project is attempted in the following section.

Overall, the consideration of the ethical dimensions of the SMART technologies should not be limited to the two validating applications of the project (i.e. live news, security/surveillance) and the set of perceptive technologies that support them (i.e. crowd analysis, acoustic event classification). Rather, the ethical dimensions of the SMART technologies should also address the possibility of other enterprise deployments or community projects that could be developed on the basis of the SMART search framework. Indeed, in this document we attempt to discuss ethical concerns and relevant measures associated with acquisition and indexing of environment generated content, beyond the limited scope of the project's proof-of-concept applications implementations. The deployment of applications based on the SMART framework could entail ethical concerns. Integrators, application developers and solution providers building SMART-based applications must be able to identify these concerns with a view to activating any relevant measures. At the same time, end-users (i.e. corporate users and/or citizens) should be aware of ethical/privacy concerns associated with the use of the SMART multimedia search engine. The present document addresses these concerns in such a wider context (i.e. beyond the scope of SMART WP3 perceptual components and the SMART WP6 applications).

2.3 The need for a Data Collection Process

As already outlined, the operation of the SMART search engine requires the deployment of perceptive components. Typically, these components process multimedia signals stemming from the physical environment and extract context. Their development and robust operations hinges in several cases on their training on the basis of data collected at the deployment location. This is also the case with the development of the audio and visual processing components of the SMART project, which will be developed following data collection processes within WP2 and WP3 of the project. In the scope of the data collection, physical world data (i.e. multimedia signals) will be collected and processed by the perceptive components being developed.

In addition to the need for a process which conforms to scientific rigour, as some of the data may contain personal data, such as people's location, conversation and appearance, there is a need for this data collection to comply with all legislation on data protection and to not infringe on any right that the data subjects may have.

3 Analysis of Ethical and Privacy Issues in SMART

Numerous technologies that have to do with observation of the surroundings are used within SMART. For the development of all these, we need to collect, store and process data from sensors. Once developed, these technologies will be running on live data feeds, without recording any data.

Based on what is observed by these technologies, different ethical and privacy issues arise. In this setion we analyze the subjects of the observation from the SMART algorithms and we consider their ethical and privacy issues.

3.1 Person Observation

These algorithms observe the individual person. In that regard, they raise the most stringent concerns regarding ethical and privacy issues. They are algorithms that are helpful in the security and not in the live news use case.

3.1.1 Person and face tracking

These algorithms consider either the whole body or the face of an individual and observe how he/she moves in space as time goes by. Security-related events like loitering detection need such algorithms.

3.1.2 Identification

Person identification needs an a-priory trained model of the person to be identified. Although of some use to the security use case (e.g. to identify suspect individuals), we do not intend to use any such algorithms within SMART. The obvious reason is their severe privacy implications.

3.2 Crowd Observation

These algorithms observe crowds as masses. No individual can be told apart in the crowd. They are algorithms that are used extensively in both the security and the live news use cases.

3.2.1 Crowd density

Here crowds are considered as collections of foreground pixels, which are processed to get an estimate of how crowded the observed space is.

3.2.2 Crowd colours

Here the foreground pixel colours are also considered, to get an estimate of the prominent colours worn by crowds in the city, i.e. of the fashion trends.

3.2.3 Crowd motion

At this level of analysis, blocks of foreground pixels are compared between frames to extract motion information of the masses. We are interested in five different behaviours: Random directions, prominent direction, convergence towards a point and divergence from a point.

3.3 Object Observation

This set of algorithms considers moving vehicles and objects in the background that change.

3.3.1 Traffic density and speed

Vehicles are considered here, not humans. No ethical or privacy issues are foreseen for these algorithms. However if the observation includes recording of license plates in any format (photograph, detection etc.) or

photographs of the occupants of the vehicles, the same issues as in 3.1 occur.

3.3.2 Change detection

Changes of the background are considered here. We are interested in changes caused by moving some background object, leaving objects behind and parking vehicles. All these are objects and raise no ethical or privacy issues. (note however the issue of license plates mentioned above). In extreme cases where a person remains immobile for a very long period, he or she will to be marked by the algorithm.

3.4 Acoustic Observation

The acoustic part of the system processes two types of signals. The first is considered as general audio and the second is speech. The audio processing is relevant to both live news and security scenarios and the speech processing is relevant only to the live news scenario.

3.4.1 Acoustic event detection

Audio signals are collected in different places (possibly public) using microphones connected to the video capture equipment. Those signals may contain different type of noises such as crowd noises from events or from markets, traffic noises and other city noises. For the security cases we'll consider other types of noises such as door opening and closing, footsteps in isolated areas and screaming. The signals are then processed and relevant event are identified in them.

The ethical problems which might arise are related to accidental capture of speech data within the audio signal. Although this speech information will not be processed (e.g. extraction of the information in the speech) speech signals might be identified as a speech event (e.g. pointing that at specific location in the signal it contains speech segments).

3.4.2 Speech processing

Speech is collected using a smart-phone application which will allow the user to record a voice message and upload it to a server. The following processing will be performed on those speech signals:

- Speech transcription using automatic transcription engine. The text of the transcription will be used by the SMART system.
- Speaker verification: users who would like to be identified by the system will have first to perform an enrolment sessions where they will provide several speech samples from which a voice signature will be created. Later, when those users deliver a new message, the voice signature of the message will be compared to the ones from the enrolment in order to verify the identity of the speaker.

The speaker verification process therefore require to manage a biometric voice signature DB for some of the users.

3.5 Environment Observation

SENSORS

In the scope of its proof-of-concept applications SMART will also leverage non A/V sensors and sensor networks, including temperature sensors, meteorological sensors, and wireless sensor networks. These sensors will provide information about the environment in the locations where they will be deployed.

The following sensors will be considered for the SMART project:

1) Temperature

2) Humidity

3) Dust

4) Presence (for indoors usage if applicable).*

5) Vibration

6) Gases (CO, CO_2, Ozone)

**it should be noted that the technical term "presence" reflects the event of recognizing the existence and motion of a person in a given room and there is no possibility of using this sensor for identifying specific individuals.*

The list of non AV sensors has been concluded upon two criteria:

i) measuring environmental conditions for the quality of life of the citizens.

ii) parameters that hinder the visibility captured by the cameras.

3.6 Ethical Issues Associated with the SMART (Sensing) technologies

The following table illustrates the main ethical issues associated with the SMART technologies outlined above. Note that the table focuses on the technologies that are being developed in the project (as part of WP3). The take up of the SMART search architecture following the end of the project, may lead to the integration of many other components (i.e. by third-parties, outside the consortium), within the SMART system. Ethical issues raised by such third-party components are expected to be addressed by their providers, as well as by entities in charge of integrating them in search applications.

SMART Technology	Main Ethical Issues
(Visual) Person and Face Tracking	Knowing the location of an individual at any given point in time infringes on the freedom of the individual
(Visual) Person Identification	There are implications associated with the use of collected/stored on the individual and/or individuals and the institutions or communities where he/she belongs [Gold89]. As a measure, there might be a need to obscure an image [Pink07]
(Visual) Crowd Density	Same challenges as those associated with Person Identification and Tracking
(Visual) Crowd Colour Analysis	No Ethical Implications as soon as components are restricted to colour analysis outputs
(Visual) Traffic Density and Speed	No Ethical Implications as soon as components do not track (e.g., obscure) license plates
Acoustic Event Detection	Audio collection in public places Processing of collected audio for security purposes.
Speech Processing	Collection and processing speech recordings (for building speech models). Collection and processing of voice messages. Biometric verification from voice messages.
Environment Monitoring	No Ethical Implications
Social and Sensor Networks Data Interception/Fusion	Profiling individuals without their consent – Users consent is handled at the social networking infrastructure

Table 1: Association of SMART Technologies (notably perceptive components developed in SMART) with Ethical Issues

3.7 Social Networks

The SMART platform will leverage information stemming from social networks, such as Twitter and Facebook. The project will leverage publicly accessible information streams from social networks. While these streams could raise ethical concerns (e.g., privacy concerns), the relevant privacy management mechanisms at the source social networks apply. For example, Facebook and Twitter users are bound to the privacy management policies of these social networking sites, and they have given their consent/agreement to the publishing of relevant information by the providers of these social networking infrastructures. In doing so they are also considered to have manifestly made public any personal data that may be captured by SMART. Nonetheless where personal data is considered sensitive it is forbidden to create a file specifically for the purpose of listing that data, due to Spanish law. Beyond this, no additional privacy issues are relating to SMART, as a result of its interfacing to social networking sites, for the purpose of collecting publicly available information or personal information that is retrieved after the user has logged on to these sites.

Data captured by the social networks will be definitely not used for deriving unsolicited new information or monitor any status of the person involved.

However, SMART will study any additional privacy or ethical issues that can be raised due to interception of social networking feeds with social networking feeds in the scope of certain applications.

3.8 Safety Issues

The use of the SMART applications (in the areas of live news and security/surveillance) do not introduce any safety issues associated with the use of the respective systems. However, we cannot rule out the use of the SMART search engine in the scope of pervasive applications that are used to regulate the operation of other systems (e.g., operation of machines driven by SMART searches, issue of alarms based on SMART search). Such systems may raise safety issues, which are primarily driven by the inherent imperfection of the SMART perceptive components. Indeed, despite the decent performance of the audio and visual processing components that will be deployed in SMART, their accuracy cannot be perfect (e.g., 100% recognition rates, accurate video or audio scene analysis). This should be taken into account by integrators of SMART technologies, which should not rely on the outcomes of these algorithms for safety-critical applications.

3.9 Involvement of Human Volunteers

Some SMART scenarios may involve human volunteers. This is foreseen in the following cases:

- In the case that some SMART-based scenarios do not receive approval from the relevant Data Protection Agency (DPA) to monitor bystanders, these will be replaced with consenting volunteers. This may be due to the nature of the scenario or application (e.g., raising privacy concerns) or even due to the national rules and practices of a certain DPA (e.g., a scenario could be allowed in one country but not in another). In such a case human volunteers could be employed to realize the scenario in a controlled environment and based on the consent of the participants.
- In cases where specific technologies (such as tracking technologies and/or behavioural analysis technologies) need to be developed as part of academic research. Human volunteers could be employed in order to enable the research.

In either of the above cases, voluntary participants would be selected and informed members of the public who have consented to an assigned role in the scene and have accepted to be detected and tracked. This may be people acting naturally as bystanders or other selected persons who have been assigned a greater role in the unfolding of a scenario and “acting” in the data collection exercise according to their role in the scene (e.g. “suspected terrorist”, etc.).

The voluntary participants, who will agree to take part in the specific exercise, shall be asked to fill and sign a “SMART Consent Form”. Beyond the Exercise Plan Form and Actor Role Form, each potential voluntary participant will be provided with an information sheet describing the SMART project, an explanation on the

particular research activity related to the exercise, the information to be collected and how that information will be used.

4 Relevant Laws and Regulations

For a detailed discussion of the laws covering data protection, including data collection, data storage and data processing, please see companion deliverable D7.7 (Data protection protocol). Some of this information is repeated here for the convenience of the reader[1].

Based on the SMART components, applications and use potential (even beyond the end of the project), SMART has identified a number of regulations that must be taken into account and respected by stakeholders engaging or participating in the development, deployment and use of SMART Applications.

4.1 The Charter of Fundamental Rights of the EU

The Charter of Fundamental Rights in the course of the respective legal trend dedicates a separate article to the protection of personal data. Article 8 sets out the right to the protection of personal data of an individual and thus the protection of personal data has now its own legal basis apart from the right to respect an individual's private life and the protection of human dignity. Article 8 of the Charter sets out the rules for the legitimate processing of personal data, notably that the processing shall be fair and for pre-specified purposes based on the consent of the data subject or other legitimate basis laid down by law. Reference is furthermore made to two rights of the data subject: the right of access to the data and the right to have it rectified. Article 8 sets out the need for an independent authority, which shall control the compliance with the data protection rules. In particular, according to Article 8:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

4.2 Directive 95/46/EC of the European Parliament

The 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 lays down a series of rights of the data subject. These are:

- The right of access to own personal data.
- The rights of erasure, blocking or rectification of the data, which do not comply with the provisions of the Directive, are incomplete or inaccurate.
- The right to be informed of all relevant details relating to the data processing and the rights granted to self.
- The right to a judicial remedy for any breach of the above mentioned rights.

All these are applicable to SMART. The first three aforementioned rights may be restricted if this is necessary for reasons relating to the protection of the data subject or the rights and freedoms of others or to prevent a criminal offence or for reasons relating to public security.

Note that In the EU Data Protection Directive 95/46/EC, personal data are defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be

[1] In addition D7.8 is a living document with regular formal deliveries, whilst D7.7. is not. Therefore, whilst this version of D7.8 only recaps the key points, any future changes in the legislation during the project will be covered in subsequent versions of this deliverable.

identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

4.3 Data Protection Directive (1995/46/EC) and the Privacy and Electronic Communications Directive (2002/58/EC).

The field study and validation process for SMART will be carried out in accordance with European Community directives on data protection and privacy, namely the Data Protection Directive (1995/46/EC) and the Privacy and Electronic Communications Directive (2002/58/EC). In terms of the Directive 58/2002, special provisions will be taken in order to comply to the needs for transmission of electronic data outside the EU.

4.4 The Madrid Resolution

The Madrid resolution is a Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data. It brought together the privacy guarantors from fifty countries and seeks to better protection of rights in a world characterised by international flows of information. It was presented in November 2009.

The so-called Jerusalem Declaration, made at the 32nd International Conference of Data Protection and Privacy Commissioners held in Jerusalem, October 2010, called for an intergovernmental conference in 2011 or 2012 to negotiate a binding international agreement based on the Madrid Resolution. However this does not yet appear to have taken place or be announced. Whilst at the present time this is not legislation, it does not affect SMART, and until such a time as it is brought into force there is nothing gained by analysing its contents, given that they are liable to change, except to say that there appears nothing in the proposal which significantly differs from the other laws and regulations discussed here and in D7.7. There is however the possibility that it does become law during the project lifetime and so the project will revise the situation periodically.

4.5 Spanish laws and regulations

4.5.1 Fundamental rights

In Spain, article 18 of the Spanish constitution (1978) establishes that:

> *"(1) The right of honour, personal, and family privacy and identity is guaranteed.*
>
> *(2) The home is inviolable. No entry or search may be made without legal authority except with the express consent of the owners or in the case of a flagrante crime.*
>
> *(3) Secrecy of communications, particularly regarding postal, telegraphic, and telephone communication, is guaranteed, except for infractions by judicial order.*
>
> *(4) The law shall limit the use of information, to guarantee personal and family honour, the privacy of citizens, and the full exercise of their rights."*[2]

4.5.2 Data protection

Provision 4, which enshrines the issue of data protection, was further developed by Organic Law 5/1992 on the Regulation of the Automatic Processing of Personal Data. The Spanish Data Protection Agency was formally created by Royal Decree 428/1993 of 26 March.

[2] http://www.servat.unibe.ch/icl/sp00000_.html, Retrieved 06/03/2012

Law 5/1992 was subsequently amended by Organic Law 15/1999 on the Protection of Personal Data. Organic Law 15/1999 implemented Directive 95/46/EC into Spanish law.

Further information on Spanish divergences from, or interpretations of, 95/46/EC can be found in D7.7, as remarked at the start of this chapter.

Although the following Spanish regulations should be considered especially as the affect to the video processing and surveillance:

- Organic Law 4/1997, which regulate the use of videocameras by security forces in public places.l
- The so-called 'Ómnibus Law' 25/2009, which introduced some modifications in several previous laws related to data protection and private security.

5 SMART Ethical Management Measures

5.1 Ethical Approvals and the role of Data Protection Authorities

As mandated by Article 28(1)(1) of the Data Protection Directive, all EU Member States have established one national supervisory Authority with the responsibility of monitoring the application of and ensuring respect for data protection legislation within their territories (see Table 2 for a list of the DPAs in EU-27). This supervising authority is characterized as Data Protection Authority. Article 28 specifies the rights, responsibilities and obligations of the DPA authorities, including:

- The power to advise legislative or administrative authorities in the process of drafting legislation or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data
- The power of investigation, of intervention and of engagement in legal proceedings and
- The power to hear claims.

However, these powers have not been fully and equally implemented at the various states, see for example Table 3 on the power of intervention of the various authorities. However, DPAs are a crucial part of the EU's practices towards data protection, since (at national and regional level) each DPA serves as the single point for requesting approval and advice about ethical and privacy issues, including protection of personal data. As a result, deployers of SMART edge nodes (i.e. proxies to the physical world comprising one or more sensors and perceptive components) can ensure the ethical-friendly and legal nature of their deployment by applying to (or consulting with) the DPA for relevant ethical approval. Likewise, SMART application developers can apply and receive similar approvals.

The SMART project has already applied to the Spanish DPA with a view to soliciting approvals associated with the deployment of SMART sensors and infrastructure at the city of Santander. This is a step that could be taken by all SMART stakeholders.

Country	Data Protection Authority	URL
Austria	Österreichische Datenschutzkommission	http://www.dsk.gv.at/
Belgium	Commissie voor de bescherming van de persoonlijke levenssfeer	http://www.privacycommission.be/
Bulgaria	Комисията за защита на личните данни	http://www.cpdp.bg/
Cyprus	Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα	http://www.dataprotection.gov.cy/
Czech Republic	Úrad pro ochranu osobních údajů	http://www.uoou.cz/uoou.aspx
Denmark	Datatilsynet	http://www.datatilsynet.dk/
Estonia	Andmekaitse Inspektsioon	http://www.dp.gov.ee/
Finland	Tietosuojavaltuutetun toimisto	http://www.tietosuoja.fi/
France	Commission Nationale de l'Informatique et des Libertés	http://www.cnil.fr/
Germany	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	http://www.bfd.bund.de/
Greece	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα	http://www.dpa.gr/
Hungary	Adatvédelmi biztos	http://abiweb.obh.hu/abi/
Ireland	Data Protection Commissioner	http://dataprotection.ie/
Italy	Garante per la protezione dei dati personali	http://www.garanteprivacy.it/
Latvia	Datu valsts inspekcija	http://www.dvi.gov.lv/
Lithuania	Valstybinė duomenų apsaugos inspekcija	http://www.ada.lt/
Luxembourg	Commission nationale pour la protection des données	http://www.cnpd.public.lu/
Malta	Data Protection Commissioner	http://idpc.gov.mt/
Netherlands	College bescherming persoonsgegevens	http://www.cbpweb.nl/
Poland	Generalny Inspektor Ochrony Danych Osobowych	http://www.giodo.gov.pl/
Portugal	Comissão Nacional de Protecção de Dados	http://www.cnpd.pt/
Romania	Autoritatea Națională de Supraveghere a Prelucrării Datelor	http://www.dataprotection.ro/

	cu Caracter Personal	
Slovakia	Úrad na ochranu osobných údajov	http://www.dataprotection.gov.sk/
Slovenia	Informacijski pooblaščenec	http://www.ip-rs.si/
Spain	Agencia de Protección de Datos	https://www.agpd.es
Sweden	Datainspektionen	http://www.datainspektionen.se/
United Kingdom	Information Commissioner's Office	http://www.ico.gov.uk/

Table 2: List of Data Protection Authorities

Member State	Register processing operations	Authorize processing operations likely to present specific risks	Halt processing operations	Order the erasure or destruction of data	Issue a warning or reprimand the controller
Bulgaria	●	●	●	●	●
Belgium	●	●			
Czech Republic	●	●	●	●	●
Denmark	●	●	●	●	●
Germany	●	●	● [57]		●
Estonia	●	●	●	●	●
Greece	●	●	●	●	●
Spain	●		●	●	●
France	●	●	●	●	●
Ireland	●	●	●	●	●
Italy	●	●	●	●	●
Cyprus	●		●	●	●
Latvia	●		●	●	●
Lithuania	●	●	●	●	●
Luxembourg	●	●	●	●	●
Hungary	●	●	●	●	●
Malta	●	●	●	●	●
Netherlands	●	●	●	●	●
Austria	●	●	●	●	●
Poland	●	●	●	●	●
Portugal	●	●	●	●	●
Romania	●	●	●	●	●
Slovenia	●	●	●	●	●
Slovakia	●	●	●	●	●
Finland	●	●	●	●	●
Sweden	●	●	●		●
United Kingdom	●		●	●	●

Table 3: Power of Intervention of the DPAs in the EU-27 (source [FRA10])

5.2 Informed Consent

For scenarios where no DPA approvals are possible, (e.g., data collection scenarios, scenarios for research, scenarios targeting data collection only), volunteers may be employed. Volunteers should give informed consent accordingly.

The SMART Informed Consent Form has been included as an Appendix to this document. At the time of writing this document, approvals from the Spanish DPA regarding SMART scenarios are still pending and therefore no provisions for recruiting volunteers and resorting to informed consent have been made.

5.3 Data Storage

In cases where personal information is entailed in some scenario, state-of-the-art technologies for secure storage, delivery and access of personal information, as well as for managing the rights of the users must be used. There should be complete guarantee that the accessed, delivered, stored and transmitted content are managed by the right persons, with well-defined rights, at the right time.

State-of-the-art firewalls, network security, encryption and authentication can be used to protect collected data. Firewalls prevent the connection to open network ports, and exchange of data will be through consortium known ports, protected via IP filtering and password. Where possible the data must be stored in a locked server, and all identification data will be stored separately. Intrusion Detection systems can be used to monitor anomalies in network traffic and activate restraint policy if needed. Moreover, a metadata framework will be used to identify the data types, owners and allowable use. This will be combined with a controlled access mechanism and in the case of wireless data transmission with efficient encoding and encryption mechanisms.

In the case of data collected by SMART, deliverable D7.7 discusses in detail the measure the project has put in place to store and protect it.

6 Ethical/Privacy Friendly Design of SMART Applications

6.1 Overview

In addition to investigating the ethical implications of the technologies that are developed in SMART (notably the implications of perceptive technologies), SMART endeavours (as part of this deliverable and subsequent releases) to provide wider best practices and guidelines on the design of ethical applications over the SMART platform and based on the associated open search architecture. In the sequel we provide some initial considerations, including considerations for privacy and security models, as well as for usability and application design concepts.

Primarily, SMART deals with pervasive multi-sensory applications that leverage content and context associated with the surrounding environment. If one simply examined *homo sapiens* as a data processing device, one would find five senses which range from sight (two sensors processing at a rate of GB/s) through feel (millions of sensors processing at a rate of several MB/s) to taste (one sensor at approximately 10 bits/s). Coupled with a CPU (i.e., a brain) and actuators (hands, tongue, etc.) this 'device' is able to generate data in the forms of picture, gestures, speech and orthographic forms (written text). In tribal societies, this was generally the preserve of cave painters, shamans and scribes of one sort of the other, and communication was restricted within that tribe. However, technological developments from the printing press through to the Internet has seen to it that an increasingly larger number of data generators could produce output, that was digital rather than analogue, and which in turn was accessible to a correspondingly increasingly larger audience of data processors.

As a result of Web v2 (Web 2.0) and mass participation, everybody is now potentially a data generator as well as a data processor. Moreover, the development of new sensors and new communication channels means that in addition to *explicit* data generation, everybody is also potentially an *implicit* data generator. This can happen continuously and consists of many different forms of interpretable signal besides language and pictures, i.e. physiological signals, brain waves, etc. The risks are that implicit data collection of such user-generated content can be conducted unknowingly and without consent rather than contributed knowingly and with expressed consent, it can be processed in ways that are not intended or expected by the generator, and in its digital form, it persists.

This opens up a completely new form of human-computer interaction. The design space for a traditional interactive systems design could be conceived of a space with four degrees of freedom: users, tasks, environment and equipment. These degrees of freedom established constraints and boundaries on system design (i.e. they defined a design space) and could be traded off, one against the other, as the system designer 'moved' in that space. In SMART, we argue that we still need a four-cornered design space, but those corners should be labelled privacy, security, usability and design contractualism.

6.2 Privacy Model

The need for a foundational privacy model is apparent from the convergence of the personal computing paradigm and ubiquitous computing with the rise of cloud computing and ever more sophisticated data mining techniques [Solove]. Quite clearly, there is enormous value in both personal data and its aggregation as *Big Data*, and corresponding risks as it disappears behind corporate firewalls or off-shore ICT. The public awareness of such risks was being downplayed by Google in its 2012 'Good to Know' UK advertising campaign, which masked its Internet search engine near-monopoly behind the claim that it was promoting nothing more than beneficial customer relationship management.

On the issue of personal data, there is plenty of evidence that people (users) will trade personal data in exchange for enhanced services or individual social benefits [Witkowski]. Equally, there are examples where members of online social networks will voluntarily donate data, even highly sensitive data about personal health, for collective social benefits, such as medical research studies into public health issues (e.g. [Weitzman]). These examples highlight the need for a user-centric (rather than legalistic) model of privacy. Adams and Sasse [Adams] present the basis for precisely such a model, based on an identification of, and distinction between, the user's perception of the information sensitivity, the information receiver, and the informa-

tion usage, defined as:

- Information sensitivity: the user's perception of (non-)personal data, context, risk and benefits;
- Information receiver: the user's perception of who stores and manipulates their data;
- Information usage: the user's perception of how their data is used, now and in the future.

The point is that 'privacy', from a user-centric perspective, is a highly nuanced, context-dependent and culturally pre-determined social concept. Although a poor rephrasing of the 'nothing to hide' argument dismissed earlier, it is completely inadequate to claim, as Google's Eric Schmidt did, that: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" [Dwyer]. An activity that is entirely acceptable and appropriate in one context, might not be in another, which is why the user's perception of the information sensitivity and receiver are so important. Similarly, given the known socio-psychological benefits of forgetting [Storm], the idea that 'the Internet *giant corporation* never forgets' is extremely disturbing, given all the possible future uses of personal data, as is already happening with Facebook pages to users who do not understand privacy settings, commercial imperatives (i.e. the profit motive) – or political control. Note that Schmidt also said: "we are all subject in the United States to the Patriot Act, it is possible that that [sic] information could be made available to the authorities".

On the issue of aggregated personal data, or Big Data, there are a range of possible applications emerging, from seismic early warning systems using mobile phone accelerometers, through to tracking the spread of disease from search engine queries. These are only made possible if the data itself is made available to a participatory platform (and under the user-centred conditions outlined above). The requirements of just such a global participatory platform are outlined in a FuturICT project (*www.futurict.eu*) white paper [Shum].

In the scope of SMART user-centred privacy modelling is required because the project proposes to collect implicit, user -generated-content. This information has to be used for the benefit of generator, or if it aggregated, then it should be anonymised. It should only be stored for as long as t is required to serve its intended purpose, and should not be used for any other purpose. Those providing the data should be those benefit from its use.

6.3 Security Model

It is possible to trade off some of the impositions of a user-centric privacy model if we had in place an appropriate security model, one that, we argue, is based on a notion of *trust*. The notion of trust is, like privacy, a highly nuanced socio-cognitive concept, but a trusting decision can be intuitively characterised (rather than defined) by a willingness to expose oneself to risk by depending on the deliberate action of another party. In the context of pervasive and affective computing, for explicit data generation this is an intentional decision to expose oneself to a subjective expectation of an objective risk.

This requires decision-making under uncertainty, which covers a spectrum of possibilities from 'risk' trust, for a first encounter, to 'reliance' trust, for a *n*th encounter. In the case of 'risk', the trust decision is a complex calculation based on numerous cognitive and economic factors; in the case of 'reliance' trust, the decision is a short cut to save this complex calculation based on expectations established by prior beneficial experiences (and it has been said that, akin to reflex actions, people could not function if they were not able to perform such mental short cuts, and had to re-evaluate every trust decision from first principles).

Therefore, the trust basis for a new security model for pervasive adaptive applications should be based on decision support for at least three dimensions:

- A cognitive dimension: signs and signals to support evaluation of 'risk', 'reliability', etc.
- An economic dimension: utility, costs/benefits, etc.
- A normative dimension: beliefs that (a) there is a rule, and (b) someone else's behaviour will conform to that rule [Jones].

In addition, if a trusting decision is a willingness to accept an exposure to risk by depending on the behaviour of another, then there is a chance that the outcome will not be favourable (it must be possible as otherwise there is no risk; if there is no risk then it is not a trust decision). Therefore, some consideration should also

be given to a complementary mechanism for dealing with what happens when a trust decision goes wrong. The idea of forgiveness has been proposed [Vasalou] as the complementary socio-cognitive construct to trust, and indeed the motivating factors for a forgiveness decision (judgement of offence, actions of repair, historical relationship and empathy) complement the cognitive, economic and normative dimensions of the trust decision.

This model should be sufficient for explicit data generation, but the normative dimension is crucial for the security of implicit data generation and Big Data, and we return to this issue below.

Security modelling within SMART will consider what are the necessary trust cues required that users can 'safely' reveal personal information, and make queries, in return for value-added services, ensuring that user-centred configurations of rules will be respected, i.e. that there are well-understood rules about the collection and use of user-generated content, and that the SMART search engine will conform to those rules.

6.4 Usability Model

Bitter experience has given rise to the ideas of the precautionary principle and the 'law of unexpected consequences'. Two examples of unintended outcomes of affective and pervasive technology are biometrics and RFID implants.

Biometrics uses measurements of physical characteristics for purposes of identification, for example for access control. There are, however, well-documented cases of laboratory-based trials failing to work 'in the field', with even low rates of false positives and false negatives causing significant problems. Moreover, the technology can lead to worse behaviour (e.g. access control based on fingerprint recognition causing car thieves to cut off fingers in order to steal cars).

However, the real issues begin when a policy-maker mandates that a particular technology will solve a problem, for example (as discussed above) that CCTV will increase security by reducing crime; or that a technology designed for one purpose is applied for another. Michael and Michael [Michael1] document the transition of implant technology being used for managing livestock to possibly being used for tracking and monitoring people instead.

In the UK, it has argued that biometric-based identity cards will reduce illegal immigration, expose social security fraud, and prevent terrorist attacks. In practice it may have an impact on these security issues, but if the UK's recent experience of saturation CCTV, phone hacking, and infiltration of legitimate protest groups by undercover police officers is anything to go by, it is just as likely to be used by a supposedly democratic state for covert surveillance, to infringe civil liberties and to suppress legitimate protest by its own citizenry.

The usability model then is not so much from the perspective of human-computer interaction, but society-technology interaction. It is incumbent on technology developers to think through the social implications of pervasive and adaptive technologies, and to engage with policy-makers to explain clearly what the limitations and intended applications of these technologies are.

In SMART, some consideration needs to be given to exploring the possible abuses of the user-generated content search. For example, Google maps was unwittingly used by lead thieves to target churches. This will require participatory design to identify potential misuses and abuses of the new technology developed in the SMART project.

6.5 Design Contractualism

The tripartite privacy, security and usability models for pervasive and affective computing are underpinned by the need for *design contractualism*.

This requirement is based on the observation that affective and pervasive applications are implemented in terms of a sense/respond cycle, called the affective loop [Goulev] or the biocybernetic loop [Serbedzija]. The actual responses are determined by decision-making algorithms, which should in turn be grounded within the framework of a mutual agreement, or a social contract [Rawls]. This contract should specify how individuals, government and commercial organisations should interact in a digital, and digitised, world.

In the context of affective computing, this contractual obligation has been called *design contractualism* by Reynolds and Picard [Reynolds]. Under this principle, the designer makes moral or ethical judgements, and encodes them in the system. In fact, there are already several prototypical examples of this, from the copyleft approach to using and modifying intellectual property, the IEEE Code of Ethics and the ACM Code of Conduct, and TRUSTe self-certifying privacy seal. In some sense, this is a reflection of ideas of Lessig that 'Code is Law' [Lessig], or rather in this case, 'Code is Moral Judgement'.

Returning to the security implications of user-generated content and Big Data, design contractualism also underpins the idea of using implicitly-generated data as input streams for Big Data, and treating that as a knowledge commons [Hess]. Using the principles of self-governing institutions for managing common pool resources identified by Ostrom [Ostrom], we advocate managing Big Data from the perspective of a knowledge commons. Design contractualism, from this perspective, effectively defines an analytical framework for collecting and processing user-generated content input to Big Data as a shared resource with normative, social and ecological dimensions. The normative dimension is existence of the institutional rules embodying the social contract; the social dimension is the belief that there are these rules and that others' behaviour will conform to these rules, as a trust short cut [Cox], and the ecological dimension is that the principles offer some protection against 'poisoning the data well', for example by the 'merchants of doubt' identified by Oreskes and Conway [Oreskes].

7 Conclusions

This deliverable has illustrated the main ethical dimensions of SMART-technologies, including both technologies to be developed in the project, but also technologies that might be developed from third-parties (e.g., the open source community). Special emphasis have been put on illustrating the privacy implication of visual and audio scene analysis technologies, notably visual analysis that can reveal the identity and/or the position of individuals thereby infringing on their human rights. Ethical implications are also associated with the analysis of social networking feeds, since they can enable profiling of individuals. In order to deal with these ethical implications, Additional ethical implications are raised in the scope of the data collection processes within SMART, which involve the collection, storage and later analysis of audio and visual signals from the surrounding environment where SMART is deployed. Overall, in the scope of the above processes, SMART has to ensure compliance with a number of laws, regulations and principles, which are briefly outlined in the document. These laws, regulation and directives include both EU-wide directives, as well as local-directives relating to the areas where SMART sensors are deployed. In particular, Spanish laws have to be taken into account in order to ensure the legal compliance of the SMART proof-of-concept deployments, given that SMART involves trials at the City of Santander.

Ethical compliance measures for the SMART technologies include reception of ethical approvals from the Data Protection Authorities, where SMART technologies (i.e. SMART edge nodes) are deployed. DPAs are acknowledge at EU level, as the local/national points in charge of providing approvals and advice associated with experiments which have ethical implications. In line with this direction, SMART has applied to the Spanish DPA in order to get approval (and relevant feedback) associated with the integration and operation of the SMART use cases in the City of Santander. Note that SMART has the option of performing experiments with human actors under a controlled environment. In this case, human actors can provide explicit consent by filling-in the Informed Consent form, which is briefly outlined (in draft form) as an Appendix in this document. The SMART ethical measures include also tools and techniques for the secure storage and anonymization of collected data. The ways in which these measures will be activated and used in the project will be detailed in a following release of the present document, taking also into account the feedback of the DPA.

In addition to ensuring the legal and privacy-friendly development and deployment of the SMART system, infrastructure and applications, the project will be producing guidelines for the privacy friendly design of the SMART system. Some early insights have been provided in this document, covering the broader task/field of designing pervasive and ubiquitous computing systems. These guidelines (along with associated best practices) will be extended in later iterations/releases of the present document. The best practices to be published will gradually incorporate the experience of designing, developing, deploying and operating the SMART infrastructure and proof-of-concept applications (in the areas of live news and security/surveillance).

8 BIBLIOGRAPHY AND REFERENCES

[Adams] A. Adams and A. Sasse, "Privacy in Multimedia Communications: Protecting Users, Not Just Data", *People & Computers XV – Interaction Without Frontiers, Joint Proceedings of HCI 2001 and ICM 2001*, pp. 49–64, 2001.

[Cox] M. Cox and G. Arnold and S. Villamayor-Tomas, "A Review of Design Principles for Community-Based Natural Resource Management", Ecology and Society, vol. 15, no. 4, pp. 38 [online], 2010.

[Dwyer]. C. Dwyer, "Privacy in the Age of Google and Facebook", *IEEE Technology and Society*, vol. 30, no. 3, pp. 58–63, 2011.

[FRA10] European Union Agency for Fundamental Rights, «Data Protection in the European Union: the role of National Data Protection Authorities», Luxembourg: Publications offi ce of the European Union, 2010, 2010 – 50 p. ISBN 978-92-9192-509-4, doi:10.2811/47216 (available at: http://fra.europa.eu)

[Gold89] Gold, S. 'Ethical issues in visual fieldwork' in Blank, G., McCartney, J. & Brent, E. (1989) New Technology in Sociology: Practical Applications in Research and Work New Brunswick, NJ, Transaction

[Hess] C. Hess and E. Ostrom (eds.), *Understanding Knowledge as a Commons: From Theory to Practice*, Cambridge, MA: MIT Press, 2006.

[Jones] A. Jones, "On the concept of trust", *Decision Support Systems*, vol. 33, no.3, pp. 225-232, 2002.

[Lessig] L. Lessig, *Code: And Other Laws of Cyberspace, Version 2.0*, New York, NY: Basic Books, 2006.

[Michael1] K. Michael and M. G. Michael, "Implementing 'Namebers' Using Microchip Implants: The Black Box Beneath The Skin", in J. Pitt (ed), *This Pervasive Day*, London: IC Press, pp. 163–206, 2012.

[Michael2] K. Michael and M. G. Michael, "The Fallout from Emerging Technologies: Surveillance, Social Networks and Suicide", *IEEE Technology and Society*, vol. 30, no. 3, pp. 13–17, 2011.

[Oreskes] N. Oreskes and E. Conway, *Merchants of Doubt: How a Handful of Scientists Obscured the Truth on Issues from Tobacco Smoke to Global Warming*, London: Bloomsbury Press, 2010.

[Ostrom] E. Ostrom, *Governing the Commons*, Cambridge: CUP, 1990.

[Pink07] Pink, S. «Doing Visual Ethnography» Second Edition. London: Sage, 2007

[Reynolds] C. Reynolds and R. Picard, "Affective sensors, privacy, and ethical contracts", Proceedings CHI 2004 extended abstracts on Human factors in computing systems, pp. 1103–1106, 2004.

[Serbedzija] N. Serbedzija, "Reflective Computing – Naturally Artificial", in J. Pitt (ed), *This Pervasive Day*, London: IC Press, pp. 69–98, 2012.

[Shum] S. Buckingham Shum, K. Aberer, A. Schmidt, S. Bishop, P. Lukowicz, A. Anderson, Y. Charalabidis, J. Domingue, S. de Freitas, I. Dunwell, B. Edmonds, F. Grey, M. Haklay, M. Jelasity, J. Kohlhammer, J. Lewis, A. Nowak, J. Pitt, R. Sumner and D. Helbing, "Democratising Big Data, Complexity Modelling and Collective Intelligence", to appear.

[Solove] D. Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy", *San Diego Law Review*, vol. 44, pp. 745–772, 2007.

[Storm] B. Storm, The Benefit of Forgetting in Thinking and Remembering. Current Directions in Psychological Science, vol. 20, no. 5, pp. 291–295, 2011.

[Vasalou] A. Vasalou, A. Hopfensitz and J. Pitt, "In praise of forgiveness: ways to repair trust breakdowns in one-off interactions", International Journal of Human-Computer Studies, vol. 66, no. 6, pp. 466–480, 2008.

[Weitzman] E. Weitzman, B. Adida, S. Kelemen and K. Mandl. "Sharing Data for Public Health Research by Members of an International Online Diabetes Social Network", *PLoS ONE*, vol. 6, no. 4, pp. e19256, 2011.

[Witkowski] M. Witkowski, J. Pitt, P. Fehin and Y. Arafa, "Indicators to the Effects of Agent Technology on

Consumer Loyalty", in: Stanford-Smith, B and Chiozza, E. (eds.), *E-Work and E-Commerce: Novel Solutions and Practices for a Global Networked Economy*, Amsterdam: IOS Press, pp. 1165–1171, 2001

9 ANNEXES

SMART Informed Consent Form

Purpose of data collection: *The following data will be collected for a EU research project SMART funded by European Commission under the Seventh Framework Programme. SMART will use this data for training, improving and evaluating audio and video signal processing algorithms*
SMART Consortium Contact Point(s): <Names of the Ethical Committee Members>
Who has access to this information: By signing the form you give your conset to collect visual and audio data with your participation in the images and your voice in the acoustic clips. The SMART ethical committee members and the SMART ethical expert will be the only members of the project that will have access to your personal information. The SMART Consortium members who see/access this information will keep it confidential. SMART researchers will have access to anonynized data only.
Withdrawal Information: Your participation in the SMART project is completely voluntary, and you can choose to stop participating at any time. If you decide to withdraw from the project, please contact the SMART consortium contact points outlined above, and they will explain the best way for you to stop taking part. You should know that you may be withdrawn from the project for any of the following reasons: • If you don't follow the project's ethical committee instructions. • If you don't attended the scheduled data collection sessions. • If the whole project is stopped, for reasons not known now.

Voluntary Participant Data	
Name	
Status	
Email	
Telephone	
Fax	
Chair of Selection Panel of Voluntary Participant	
Name	
Address	
Email	
Telephone	
Fax	
Exercise details	
Exercise Plan Form	(Id number)
Actor Role Form	(Id number)

Applicable Laws/Directives	
Date	(dd/mm/yy)
Declaration	I have read the terms outlined and understand them. I consent to the terms *Signature* *.....*