SEVENTH FRAMEWORK PROGRAMME

Networked Media

Specific Targeted Research Project

SMART

(FP7-287583)

Search engine for MultimediA environment generated contenT

D7.9Report on Ethics

Due date of deliverable: 01-11-2012

Actual submission date: 07-12-2012

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

Summary of the document

Code:	**SMART D7.9-v0.42**
Last modification: **State:**	11/11/2012 Final Draft
Participant Partner(s): **Author(s):** **Fragment:**	Ethical Expert, ATOS, AIT Johann Čas, Irene Schmidt, Paul Moore, Daniel Field, John Soldatos No
Audience:	☒ public ☐ restricted ☐ internal
Abstract:	This is a report on the ethical activities of the SMART project. This deliverable will be initially delivered in M12 and it will be up-dated annually.
Keywords:	• *Ethics* • *Privacy* • *Data protection* • *Rights* • *Personal information*
References:	D7.8 Ethical Dimensions of SMART Technologies; D7.7 Data protection protocol, DoW (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 crowd sensors composed of cameras and microphones but with strict safeguards against detection of individuals or speech), 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 SMART search engine shall also be able to leverage Web2.0 social networks information in order to facilitate social queries on physical world multimedia. The intended boost in scalability in both functional and business terms, extensibility in terms of sensors and multimedia data processing algorithms, enabling the answering of queries based on the intelligent collection and combination of sensor generated multimedia data and of social network generated data is accompanied by a corresponding boost of ethical concerns raised by the intended increase in search engine capabilities.
The purpose of this deliverable is to summarise the responses by the consortium to the main ethical issues raised by the SMART project, including privacy and regulatory issues emerging from the deployment and use of outdoor sensors. It will therefore address the main ethical concerns associated with the project, along with relevant/possible solutions as e.g. described and proposed in D7.8 Ethical Dimensions of SMART technologies.
The present document represents the first release of the deliverable. Successive annual releases are planned to be produced during the evolution of the project, reflecting the progress on how ethical/privacy issues are confronted and resolved by the consortium.

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 appreciate the ethical dimensions of the SMART infrastructure and services and be assured they are being managed correctly. The present deliverable aims at providing this assurance, and together with the deliverable series D7.8.x, to inform the consortium of ethical issues.
- **Management within consortium participants**: 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. As partners start to develop exploitation plans stakeholders within the organisations must be assured that ethical considerations are taken into account and that liability is properly minimised. The present deliverable is relevant to all these stakeholders, as it provides guidance that the correct procedures are in place.
- **The general public and EC:**As for the management levels of the partners, both the general public and the EC will wish to be assured that this project is correctly managed from an ethical perspective, both because from the perspective of the rights of the citizens and the use of public funds.
- **The ethics committee:** This document shall assist the mutual exchange of information among this committee, the consortium and the external Ethics Advisor.

1.3 Structure

This deliverable describes the process and structure for ensuring ethical compliance in the SMART project. It contains nine chapters. This first chapter is an executive summary, followed by an introduction to the document.

The third chapter briefly touches main aspects of the ethical management and appointment of ethical expert looks at basic concepts of ethics. The fourth chapter presents the European legal framework on Data Protection with the Data Protective Directive (1995/45/EC) and the approval requests the SMART consortium have sent to the DPA. In addition to the European framework the deliverable takes also into account the national legal frameworks on Data Protection of the piloting countries Greece and Spain.

Chapter 5 defines a set of contingency planning & requirements which can be derived from the legal frameworks presented in the previous chapters. This leads to the next two sections which will look at the outlook and conclusions performed in SMART and outlines how the project will comply with the legal requirements earlier defined. The chapter 9 includes several Annexes which are very important for the project impact and especially for the ethical issues.

2 Introduction

The deliverable series D7.8.x discusses in detail the specific ethical issues that arise in the SMART project. These are discussed in terms of what the issue is, why it arises, the relevant legislation, the impact the issue has on the project and its exploitation, and the means through which the project avoids contravening regulation or rights.

This deliverable series, D7.9.x, should be seen as an accompanying document with a focus not on the issues themselves, but on the management of the process of issue detection and regulatory compliance within the project itself. This may form best practice for future exploitation of the SMART system, but this is not the primary intention of the document. Rather here our emphasis is on demonstrating sound ethical management during the project.

This deliverable version, D7.9.0 is the first of the series and provides a retrospective discussion of the first 12 months of the project, charting what has been done and what has been put into place.

The primary regulations applicable to SMART are the charter of Fundamental Rights of the EU and the EU and national data protection directives.

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. Finally, Article 8 sets out the need for an independent authority, which shall control the compliance with the data protection rules.

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 principles and regulations. These include:

Article 6 - Principles relating to data quality, stating that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

Article 7 - Criteria for making data processing legitimate, stating that Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

And, to name the most relevant articles, Article 12 - The data subject's right of access to data, stating that Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

Article 22 - Remedies details the right to a judicial remedy for any breach of the above mentioned rights.

The SMART project also affects further Articles of the Charter of Fundamental Rights, Article 11 - Freedom of expression and information is touched by inclusion of Web2.0 social networks information, Article 12 - Freedom of assembly and of association by the crowd control aspects of SMART.

The issues raised in the project in relation to this and other regulation are coved in detail in D7.8.x, to which the reader is directed for further details.

3 The Ethical management process in SMART

To study the ethical issues associated with the implementation and deployment of the SMART multimedia search engine and associated use cases the SMART project management has created an Ethical committee chaired by the project's Ethics Expert. The committee and the external ethics expert are appointed to ensure the full compliance of the project with the legal and ethical frameworks at both a national and EU levels.

Special emphasis is given on the issues of video and audio data collections, as well as issues associated with the privacy management in social networks. As part of the ethical committee discussions the security and privacy impacts of the use of the envisaged technologies will be also explored, to ensure the appropriate consideration of the associated ethical aspects of the SMART project technologies. The ethical issues of the project and the associated ethical management principles are briefly outlined in the following sections.

3.1 Appointment of an ethics expert

The project budget includes the subcontracting of an independent ethics expert. The independent ethics expert should have a minimum of three years' experience on ethical and privacy issues with relation to ICT.

Duties of the independent ethics expert: To ensure the validity of the ethical approach taken in the project, an Ethics Advisor is appointed within the project, under WP7, to manage and guide the ethical content and procedures as part of the ethical management strategy of the project. In the context of the SMART project, the independent ethics expert will lead the effort of producing the ethics related works.

The independent ethics expert is the first point of contact within the consortium for any questions regarding ethical issues, such as privacy, security, freedom of choice, dependency and consent, and is also assisting the communication to the EC regarding ethical reports and advises about approvals where required and will act as a supportive consultant to the activities of the Ethics Committee of the project. His duties include the production of the ethics related deliverables of the project (i.e. deliverables D7.7 and D7.8.x), as well as the annual project reports on ethics (D7.9). He is also a member of the ethics committee

Involvement of the external ethics expert during M0-M12

- The appointed independent ethical expert is ***Johann Čas*** (see Annexes 9.1.1)
- He assists and provides advice to the ethical committee and is available via phone and email)
- Several actions with consortium have been carried out.

3.2 Appointment/Establishment of Ethics Committee

Ethics Committee: SMART will make a significant effort to fully analyse and take in to consideration any potential ethical implications of SMART technologies and results. To this end, SMART established (as part of the management structure) an ethics committee. The committee consists **of five** members from the consortium partners, which are knowledgeable in the handling of ethical issues, notably privacy issues arising from the use of sensors in an urban environment (see **Table 1: Members of the SMART Ethics Committee**). Among these five members, one is a representative of the project coordinator (ATOS) and another of the smart city of the consortium (SDR). The remaining three members are selected from the rest of the partners. The role of the ethics committee will be to guarantee the project services adherence to legal and ethical requirements, while also overseeing the application of the ethical management strategy of the consortium. In particular, the committee (in collaboration with the independent ethics expert) will be responsible for establishing and implementing all ethical procedures described in the ethical section (e.g., auditing of the SMART services against legal and ethical require-

ments, establishment of anonymization procedures, request of permissions from relevant authorities, drafting of material necessary for obtaining permissions, drafting of informed consent forms, etc.). The ethics committee will report about its work to the steering board of the project, as well as to the project coordinator regarding the following actions:

- Composition of ethics committee
- Roles of external ethics committee
- Mode of involvement
- Decisions and minutes of meetings

The mandate of the ethics committee is:

- to review (using a proportionate approach), approve, reject, propose modifications to, or terminate any SMART use cases,
- to ensure that SMART is compliant with data protection requirements,
- to ensure that the technical partners of SMART develop a “socially acceptable” system that considers privacy,
- to conduct an ethical review of each driving experiment using the SMART facility,
- to conduct an ethical review of each open call experiment using the SMART facility,
- to provide ethical oversight for experiments using the SMART facility,
- to assess the informed consent form of each experiment.

The ethics committee should as a minimum consider the principles of:

- ‘doing good',
- ‘doing no harm',
- risk management, which encompasses the assessment of hazards (i.e. source of potential harm) and an analysis of risk (i.e. the probability of such harm occurring),
- consent,
- confidentiality,
- data protection.

Where the project management is unable to resolve a particular issue, including any concerns of an ethical or related nature raised by participants in an experiment, the ethical issues coordinator (project coordinator) will relay all relevant details to the executive board of activity leaders chaired by the project coordinator.

Operations of the ethics committee

The communications between the SMART consortium and the ethics committee will be based on workshops and exchange of documents:

- SMART will organise an ethics committee meeting approximately every 6 months. A total of ca. 6 meetings over the project duration of 3 years are envisaged. In order to increase the opportunities for exchanges between the consortium and the ethics committee members, it is intended to organise the ethics committee meetings in parallel (same time, same location) with specific consortium meetings.
- A private website will be set-up to facilitate communications and sharing of information between the ethics committee and the consortium. It will contain documents produced by SMART for review by the ethics committee and also support closed fora for on-line discussions.

As regards its relation to the consortium management organisation, the ethics committee will have an advisory status with the participation the Ethics Expert.

Membership

The ethics committee will be composed of internal project members, assisted by the independent expert in ethics and data protection in complimentary disciplines which are to provide appropriate guidance and review:

Term of appointment

The ethics committee was be established by February 2012 and the members of the EAB will be appointed until the end of the SMART project, October 2014.

Meeting procedures

The ethics committee will convene every six months, for the evaluation of open issues and after the design phase of each use cases phase. In addition, the ethics committee will have a mechanism for review of urgent or short-notice cases.

The ethics committee members could join the meetings via teleconference.

Reporting

Prior to the commencement of the project an ethical review was conducted by the ethics committee. Points raised have been followed by the ethics committee and fully investigated for D7.8. The Ethics Committee will be responsible for the following reports:

- 1st Ethics Review Report [est.: month 12]
- 2nd Ethics Review Report [est.: month 24]
- Final Ethics Review Report [est.: month 36]

The Ethical Review Reports will be submitted to the European Commission as part of the SMART deliverables prior to the commencement of the new use cases.

The Ethics Committee Members are listed in the following table

Ethics Committee Member Name	**Organization**
Paul Moore (Chair)	Atos
John Soldatos	AIT
Zvi Kons	IBM
Javier Lasa	PRISA
Tomas Garcia	SDR
Johann Čas	Independent Ethics Expert of the SMART project

Table 1: Members of the SMART Ethics Committee

3.3 Ethics Committee Meetings

The consortium has decided in the Kick-off meeting, which was held in Santander, to submit an application to the DPA taking into account all relevant ethical issues. The first submission of the DPA document was sent

Madrid meeting 21-23 of February 2012

After the appointment of the ethics expert– Johann Čas, the first physical meeting was held in Madrid (21-23 of February 2012).

At this meeting the consortium has discussed several important ethical issues such as:

- current legislation relevant for the project,
- the data protection directive 95/46 EC,
- rules concerning future implementations the proposal for a regulation (COM 2012/11);
- issues concerning security related users of the system,
- also the proposal for a directive (COM 2012/10),
- law enforcement authorities (the foreseen users),
- the Madrid resolution on the protection of personal data and privacy (which has also influenced the proposal for a regulation)

The outcomes from the meeting were:

- Wait for DPA approval.
- Contingency planning to take into account different solutions in case there are some complications or changes.

Audio meetings in June 2012

The purpose of the meeting was to get the feedback on the ethical and privacy aspects of the use case scenarios for the second submission of the DPA document. The open issues were to agree with all partners to go through the document before the second submission with the following objectives:

- Review of use cases (ethics, data protection, etc.)
- Propose modifications to use cases (if needed)
- Identification of potential risks
- Suggestions on how risks could be mitigated

SMART ethics committee has discussed the comments and suggestions from all partners during the Skype audio meeting. All project partners, and especially who are responsible for the use cases (Santander, Prisa and S3Log) were present, so any further questions would be discussed beforehand.

The outcomes from the meeting were:

- Identification of the limitations of the SMART system deployment, based on the feedback from Spanish and Greek DPAs.
- Elaboration of good practices for writing the revised/resubmitted application with a view to addressing the issues raised by the DPA, while also alleviating relevant doubts on the privacy compliance of the SMART applications.
- Identification of accompanying material (e.g., videos, snapshots of the SMART crowd analysis components) that should be provided to the DPA along with the written application.
- Development of the structure of the revised applications and identification of its contents.
- Wait for DPA approval.
- Adjust different solutions in case there are some complications or changes.

Audio meetings in October 2012

Other audio meetings were hold in October 2012 to discuss the D7.9 content and open issues.

All Ethical committee members were present on those meeting.

The main Ethical and Privacy issues were discussed. The first version of the D7.9 ToC was presented to the SMART Ethical committee.

Content of issues for the ethics committee

A brief list of discussed issues in the ethical committee meetings from June to October 2012 is given below:

Specific Measures on Ethical and Privacy Issues

- Relevance of issues in foreseen use cases; potential relevance in full functionality of developed technologies and applications; reasoning in case of non-applicability
- Measures to avoid or mitigate respective issue

Personally identifiable data

- Which personally identifiable data can be generated / collected by SMART from sensors and particularly from social networks?
- How are anonymisation and/or informed consent guaranteed?

Crowd/colour detection

- what uses are foreseen for the crowd detection capabilities?
- what uses are foreseen for the colour detection capabilities?
- what measures are foreseen that these detection capabilities are not used to limit fundamental freedoms, particularly freedom of assembly?

Detection of suspicious behaviour

- what uses are foreseen for the detection of “suspicious behaviour”?
- how is suspicious behaviour” defined?
- what measures are foreseen that these capabilities are not misused to detect (rate and discriminate) unusual/abnormal behaviour?
- what uses are foreseen for the detection of the permanence of a person?
- what measures are foreseen that criminal activities are distinguished from unwanted or unusual behaviour and that latter is not detected?

Acoustic sensors, audio

- what uses are foreseen for acoustic sensors/microphones?
- what measures are foreseen that these sensors cannot be used to listen to/record conversations in public places?

Location tracking

- to what extent is tracking of persons and objects possible/foreseen?
- what measures are foreseen that tracking is not misused?

Consent for pictures/videos

- as far as volunteers are concerned no additional response to D7.8 is needed.

Biometrics

- to what extent is the use of tracking of biometrics possible/foreseen?
- what measures are foreseen that biometrics cannot be used, particularly face recognition?

Data from social networks

- what data from social networks will be used?
- for which purposes these data will be used?
- what safeguards are foreseen that the use of these data corresponds to initial purposes of persons providing these data and that informed consent on reuse has been given?
- what safeguards are foreseen that identifying data are excluded?

Specific additional data?

- what kind of specific additional data will be used?
- for which purposes these data will be used?
- what safeguards are foreseen that the use of these data corresponds to initial purposes of persons providing these data and that informed consent on reuse has been given?
- what safeguards are foreseen that identifying data are excluded?

Big Data

- what sets of Big Data are foreseen?
- for which purposes these data will be used?
- what safeguards are foreseen that the use of these data corresponds to initial purposes of persons providing these data and that informed consent on reuse has been given?
- what safeguards are foreseen that identifying data are excluded?
- what safeguards are foreseen that data fusion does not create new possibilities of re-identifying personal data out of anonymous/pseudonymous data sets?

4 Obtaining Ethical Approvals

4.1 Overview

SMART is an R&D project in the 7th Framework Programme of the European Commission. This project aims to construct a search engine, theoretically for all types of sensor data (including Audio / Visual data) which are currently not taken into account by the Internet search engines such as Google and BING. At the same type the project wants to investigate combining publically available information from the different social networks such as Facebook, Twitter and Eskup, with the information gathered from sensors in public places. These sensors can be visual or audio sensors as well as sensors of other types (traffic, weather, etc.). In practice, the project will carry out a proof of concept with a small range of sensors, as discussed herein.

It should be noted that information from these sensors will not be broadcast or otherwise released through the aforementioned social networks: information flow is unidirectional: public information is taken from these sites but no information is provided to them.

As it is an R&D Project, SMART is not trying to build a market-ready product. The goal is to produce a pilot that demonstrates both the technologies being developed in the project and the various conceptual ideas that lie behind these technologies. It is not an objective of the project to research individuals, movement of people, behaviour of crowds or other investigations of a social, cultural or otherwise anthropological nature. The project merely seeks to assess the technical feasibility of developing sensor-based data as an input data stream.

There are already many existing software systems that can search in the social networks for key words, persons, etc. and that SMART will be using these already existing systems. This data is considered to be made manifestly public by the user of the social network.

The SMART consortium has undertaken work towards the design and specification of the data collection processes which was happening in collaboration with the city of Santander where a proof-of-concept SMART deployment will take place.

To this end, the project must collect data published on social networks, retrievable through the social network's tools, data published on the web in general, retrievable through search engines, and data from the project's own sensors.

As these three data sources may involve data on and belonging to individuals and organisations, it is imperative that the project complies with data protection regulation and for this reason a DPA submission was made.

4.2 SMART Ethical Management Measures

(For further details on this section please consult D7.7 and D7.8)

4.3 Initial Submission

At the beginning of the project (Dec 2011) the SMART consortium contacted the Spanish DPA **(see in Annexes 8.2)** in order to get the required ethical approvals for the project's trials. The project has also investigated contingency strategies in case the answers from the DPA are not as expected. As part of this process, SMART has started the investigation of the ethical implications of the project. In parallel, the coordinator has selected the ethics expert foreseen in the project structure, which will be involved in the project as subcontractor.

Due to the public nature of the A/V SMART sensors (cameras and microphones) and privacy issues, it was necessary to apply to the Spanish Data Protection Agency for permission. The first submission

was rejected **(see in Annexes 8.3)** because it was not sufficiently clear that persons would not be identifiable in the video streams. Therefore a resubmission was prepared where it was stated more clearly (and shown with video examples) that individuals will not be identifiable in the SMART system.

Note: it is not sufficient that individuals are not being identified or that anonymization techniques are being used. The system must be set up in such a manner that identification is impossible due to image quality, camera distance and/or camera angle and that the cameras are at their maximum zoom. The measures adopted were described in deliverable D7.8.0.

4.4 Revised Submission

After the answer of the petition from the DPA the SMART consortium has decided to review and update the document with a series of detailed data and re-submit a document for a new approval to the Spanish DPA **(see in Annexes 8.4).** As part of the contingency plan advisory discussions with the Greek DPA were held.

The project has also paid emphasis on understanding the ethical implications of the project, while at the same time resolving ethical issues that affect the design of the project's demonstrators (especially those concerning environment generated content in the city of Santander). This is the essence of the D7.8.x deliverables. To this end, the project has engaged in consultation and discussion with both the Spanish and the Greek DPAs (Data Protection Authorities). However, the relevant progress has been remarkably slow, demonstrated by the fact that the Spanish DPAs responded to the SMART requests and applications nearly three months after the submission of the project's request for a live demonstrator. Furthermore, the response has outlined the restrictions of the live demonstrations, which will be taken into account in revising the project's application to the Spanish DPA, paying emphasis on the alleviation of issues (e.g., use of cameras, zoom level of the cameras, location of the cameras) that could raise privacy concerns. Indeed we remarked that the combination of audio-visual sensors with algorithms should be regarded as a "crowd sensor" rather than as cameras and microphones, as only the processed data relating to trends, without intelligible conversation or identifiable data being accessible or recorded. At the same time (see in D1.1), the project has elaborated contingency strategies in case where the project application is rejected. These strategies concern both the data collection processes, but also the setup of the live demonstrator. Even though alternatives exist, the slow communication with the DPA has been a main issue requiring the project's attention given that there are tasks and deliverables (such as data collection) that depend on the final results of the communication and consultation with the DPAs. The resolution of these issues is therefore a top priority for the project.

4.5 Interactions with the Greek DPA

Prior to the submission of the revised SMART application, the consortium haD also the chance to interact with the Greek DPA, as a mean of acquiring additional information and insights associated with the ethical approvals needed prior to deployment the SMART applications. To this end, SMART partner AIT arranged a meeting with representatives of the Greek DPA, on April 24, 2012. The objective of the meeting was to consult with the Greek DPA on issues relating to the SMART development and deployment.

As part of the meeting with the Greek DPA, the following important information was documented and accordingly shared among the members of the SMART ethical committee:

- The deployment of outdoor sensors (such as cameras and microphones) cannot be done legitimately without prior approval by the local DPA (i.e. the Greek DPA in the Greek territory).
- In order to get such an approval an application should be submitted to the DPA. In Greece, a template for such an application is available at http://www.dpa.gr/. Such a template is not available in Spain (i.e. by the Spanish DPA). However, the Greek DPA representatives stressed that it is a good practice to provide any additional information that could help the DPA expert to understand and audit appropriately the applications. Therefore, applicants should not restrict themselves to the con-

tents of the given template.

- The examiners of the application to the DPA, will usually audit it against applicable law, taking also into account its purposes. «Research» purposes (as in the case of SMART) are not explicitly quoted by the current Greek laws, and therefore the examiners will have to examine each application case by case. The Greek DPA representatives gave specific examples of applications/proposals that have been recently rejected from the Greek DPA, as well as applications that were accepted (i.e. one such example concerned the deployment of web cams in Greek beaches for touristic purposes).
- Given that SMART is an international (EC co-funded project); the Greek DPA officers stressed the fact that national DPA authorities tend to harmonize their decisions. Hence, applications accepted in one EU member state, will be most likely accepted to other states as well. This was the case for example of Google Street Map applications, which is allowed in several/all EU countries following the decision of the first DPA to allow it.
- The application should stress and make evident the points that ensure the privacy compliance of the application. In the case of camera deployments for example it should be stressed that the relevant deployment/application complies to a set of conditions that would make it compliant for example: (a) The fact that people will be non-identifiable, (b) The fact that the camera would not be able to zoom (on people), (c) The fact that it is need it for research purposes (SMART project description etc.). Applicants had better consult information about relevant applicable laws that are available on-line for example at: in the case of the Greek DPA.
- In Greece, applicants have always the option of meeting IT experts that will examine the application in person. Such meetings provide opportunities for illustrating the scope of the target applications, while also clarifying key questions introduced by the examiner.
- The officials of the DPA pointed out that scenarios in a controlled environment and with the participation of volunteers that give informed consent are most likely legal/compliant. Therefore, the contingency plans of the SMART project (in relation to the DPA issue) are valid in this respect.

As already outlined the above information has been communicated and discussed within the members of the SMART ethics committee. Some elements of the above information have also been taken into account towards creating the revised applications. Furthermore, some of this information has been compared against relevant information derived from the Spanish DPA. Overall, the consortium has therefore exploited the consulting and informational role of the DPAs in the scope of applications/systems that might raise privacy concerns.

5 Contingency Planning

Ethical/Privacy Concerns

The following measures will be taken:

- All services which store images and/or audio must to have permission of the ethics committee of the project.
- All images and/or audio stored must be deleted one month later if they don't have security utilities. All security utilities must be ordered by a judge.
- All images and/or audio signals when are converted in files format must to accomplish regulations of LOPD (Data protection Law) as a Data file.

5.1 Specific Measures and Ethical Management Strategy to be applied in the course of the SMART use cases implementation

B1.1.1. SMART Use Cases Participants

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 with the needs for transmission of electronic data outside the EU. The relevant provisions ensure compliance with these Directives will be part of deliverable D7.7 of the project.

The SMART consortium confirms that no children will be involved at any stage, including during field testing.

Among the key-objective of SMART is to develop use cases involving security and surveillance in urban environments. Such surveillance will be primarily employed in the scope of the security application of the project in WP6, yet the rest of applications (news, social search) might also be combined with surveillance of public spaces (notably urban areas of the city of Santander). The monitoring of public spaces is a very sensitive issue as it entails the tracking and observing of people captured by a deployed network of video cameras.

All recorded/captured data that is sensitive, will undergo processing to render it anonymous and will be operated upon in its entirety to build a statistical model of the evolving scene. By sensitive, we mean data that might reveal the identity of a person, of any member of the public.

The participants can be:

- Members of public: bystanders present in the captured scene;
- Voluntary participants: either selected persons e.g. informed members of the public who have consented to an assigned “token role” in the scene and have accepted to be detected and tracked, 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.).

B1.1.2. Volunteers Recruitment and Sampling

A strict procedure for the selection of the voluntary participants for the exercise will be defined and approved by the ethics committee of the project, in collaboration with the independent ethics expert/advisor of the project.

One issue that cuts across most of the issue areas considered below concerns the extent to which the program's "normal" process of recruitment and enrolment is maintained during the evaluation period. It seems inevitable that the process will be changed to some degree. Large changes, however, may make it difficult to generalize findings to others enrolled through the normal process. Hence, changes to the process that are made for purposes of the evaluation should be minimized, made in a way that is not likely to have an effect on the types of fathers enrolled in the program or the nature of the program itself during the evaluation period, and documented.

The SMART objectives and evaluation plan (especially in terms of scenarios and technology advancements) will be exploited in order to drive the identification of volunteer subjects. The volunteers will be assigned by either a random or non-random methodology (depending on the design) as required to support the SMART scenarios and technologies development. The SMART scenarios will serve as a basis for identifying the number of volunteers (i.e., the sample size), as well as relevant statistical parameters of the sample. Additional details on the sampling and recruitment process will be provided in the scope of the data collection design in WP2.

An Exercise Plan Form to describe the single exercising plan, and an Actor Role Form to describe the

actor-role of each voluntary participant in the specific exercising plan, will accompany the consent form as part of the candidate selection procedure.

The inclusion/exclusion criteria will be defined such that each voluntary participant will be selected for their acting role in the exercise. All necessary steps will be taken to eliminate bias within the selection process in order to avoid discrimination based on physical and cognitive aptitude and political, social, religious and cultural, gender orientation. Under no circumstances will vulnerable subjects be selected as a SMART actor; this includes persons under the age of 18 and any other person unable to give the informed consent.

Each participant, including members of SMART consortium, will be informed before each data collection exercise and test session on the ethics directives, principals and implications and they will be invited to sign a consent form.

The Consent Form will be tailored specifically to each different test/technology (e.g., audio technologies, video technologies). In all cases volunteers can withdraw at any time during any exercise and test session.

The SMART partners will be responsible for all activities involving data/information and knowledge exchange. The SMART team will carrying out the collection of information related to the volunteer including but not limited to biographical information such as the volunteer's name, height, age, vision, biological traits, location, biometrics, facial images, discipline field (i.e., fire, emergency medical service (EMS), law enforcement), and years of related work experience, retired or active status; survey and interview information to obtain feedback in test or research settings; contact information to coordinate and schedule tests with the volunteers; and photographs and video recordings that capture audio and images of volunteers. The standard SMART Consent Form is reported in a following paragraph.

In the following paragraphs we also describe the specific measures to be taken for protecting the privacy of both members of the public and volunteering participants.

B1.2. Specific measures to protect the privacy of member of the public

- Information about data collection locations and images/videos potentially capturing the identity of captured bystanders will be stored anonymously in a secure database and will be destroyed as soon as the study/research task is completed and in any case will be automatically destroyed at the end of the project. Access to the database will be permitted only to authorized personnel, whose access is controlled through secure authentication techniques (see also the Annex 2- Indication of how any data storage and handling processes will ensure data protection and confidentiality).

- Any accidental or incidental collection of video data that might be related to personal information of bystanders, captured by SMART monitoring system, such as the capture of a person's vehicle number plate or any other personal data that might be used to identify the person, will be blurred before being made public.

- SMART will notify bystanders of public and private spaces employed in all data collections and testing of the monitoring system. This will be implemented by posting a notice visible from all access points to the employed area.

B1.3. Specific measures to protect the privacy of voluntary participants

The voluntary participants, who agree to take part in a specific exercise, will be asked to fill and sign a "SMART Consent Form" (provided later in this document). 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.

The final report of SMART may include photographs or video recordings of the voluntary participants. All contracted researchers will use the edited photographs and video recordings to demonstrate how to

use technology, equipment or capability in operational or research settings. The contracted researchers will destroy all data containing private data as soon as the study/research task will be completed. In any case all personal data will be destroyed automatically at the end of the project and only anonymous or non-identifiable data will be retained after the completion of the final report.

The voluntary participant data will be processed in accordance with the processes described in the following paragraph titled: “Indication of how any data storage and handling processes will ensure data protection and confidentiality”.

B1.4. Data collection and protection measures for each specific method of data collection

Advancing technology in audio and visual signal processing (as envisaged in WP3 of the project) hinges on the availability of an adequate set of data for training and testing the respective components and subsystems. To this end the project will collect, annotate and transcribe data sets mainly consisting of acoustic and visual data. These data sets will be accordingly processed towards training the systems. As a result, the project involves tasks and processes related to data collection and processing. The consortium will deal with any relevant privacy issues that could be raised during these processes. In particular, appropriate procedures will be established and carried out in the scope of the project towards tackling with:

- Awareness regarding the purpose and the implication of a person’s participation in a data collection process: Each participant in a data collection processes will be adequately notified about the purpose and the implications of his/her participation in the process. The consortium will compile an appropriate «Informed Consent Form», as well as a ‘Data Collection Participation Agreement’, to be completed and signed by both the responsible consortium representative (i.e. Ethics Committee) for the data collection process and the participant. The Participation Form will comprise information aiming at assisting in the identification of the participant with respect to its ability to provide a representative data set, as well as the evaluation of the data set itself. No information that could potential raise privacy concerns will be requested from the participants. The Agreement form will clearly state that the participation consents to participate in the process knowing all the privacy implications. From the consortium side it will be stated that the collected visual / acoustic data will be used only for the process of training the system, and that no discrimination of the speakers according to private personal information will be performed.

- Processing of raw data: The consortium will not make use of raw data, but only appropriately transformed data. In particular, the training of the systems requires transformed data (e.g., MEL CEPSTRA Coefficients for training Hidden Markov Model, results from crowd analysis on multiple faces). Such data are not usable for other purposes (e.g., voice reproduction, synthesis) and therefore cannot compromise the users’ privacy issues. It should be emphasized that appropriate procedures will be established to ensure that the consortium uses raw data merely just for transformation purposes.

B1.5. Anonymization of Data – Measures Surrounding Publication of Personal Data

As already outlined, the project will not maintain or offer indexing capabilities on personal data. The visual and audio signal processing components of the system would not rely on any kind of personal data for their training and advancement. In all cases, data from volunteering participants will be subject to an anonymization procedure to be overseen by the Ethics Committee. As part of this procedure only anonymized data will be kept within the SMART system data structures (i.e. databases, data stores, ontologies) through the corresponding identifiers of the participants. The association of the identifiers with the personal data (kept in the hard copies) of the informed consent forms will be only available to members of the ethical committee of the project. Furthermore, the informed consent forms (hard-copies) will be securely stored (e.g., locked in storage spaces accessible only by the informed consent forms).

Regarding members of the public, SMART will not maintain any data that might reveal identity. Faces, plates and other elements that could reveal people identification will be blurred in all cases where SMART data will be published.

More details on the anonymization protocol will be provided in the relevant protocol to be submitted to the Commission as part of WP7 of the project.

B1.6. Indication of how any data storage and handling processes will ensure data protection and confidentiality

Adequate technical security measures for storage and handling of such data

SMART will use state-of-the-art technologies for secure storage, delivery and access of personal information, as well as managing the rights of the users. In this way, there is complete guarantee that the accessed, delivered, stored and transmitted content will be managed by the right persons, with well-defined rights, at the right time.

State-of-the-art firewalls, network security, encryption and authentication will 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 (depending on the facilities of each partner) the data will be stored in a locked server, and all identification data will be stored separately. Intrusion Detection systems will monitor anomalies in network traffic and activate restraint policy if needed.

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.

Security enforcement within the project

In this section we will describe the data protection measures for information used by researchers during research. Data will be collected at different research sites with surveys and experiments. The collected data will be stored in a secure server, only visible to the research site network, in a locked room at each of the research locations. Anonymous and identity data will be stored separately, and only the project leader will have access to all the users' identities. Anonymity will be granted by separating identifiable data from anonymous data. Each user will be granted a unique identifier that will link one to the other, but only anonymous data will be available to researchers. If any identifiable data is required, access to it will be granted only after explicit user permission and after agreement of the Ethics Committee.

Authentication will be required to access stored data on the research site. Authorized researchers will have access to the recorded anonymous data after authentication with a centralized server and on a need-to-know basis. Researchers performing the survey will have access rights to add data to the identity database, synchronized with the writing of the anonymous data. No editing or reading rights will be granted to them to prevent alteration/disclosure of private data.

Access to the different databases will be granted with an authentication server that will restrict access depending on the user identity, profile and the device he is currently using (identified at the minimum through its IP address or in special cases through strong authentication systems). If the device he is using is not from the local research site network, access will be banned. Access to each of the tables of the database will be also filtered on a user-based policy. A periodic change of password and minimum password quality policy will be enforced to grant the security of the system. Username, password and IP address will be checked before granting access to restricted data.

As stated previously, those researchers working on SMART will be asked to sign a statement that they are familiar with and abide by the contractual obligations of the consortium. If not included in this obligation, they will sign a statement that commits them to make sure project data are not provided to persons outside SMART.

Logs of all transactions in the databases will be kept continuously and backups of the logs will be done periodically, so that actions performed upon the data can be monitored and responsibilities attributed. The server should be stored in a locked room with restricted access. Integrity of data will be granted with periodical backups and redundant images of the database, in case that a roll-back is needed. Only the automatic logger user will have rights to modify those logs, to prevent modification of the recorded data.

If an exchange of data among the different research sites is required, for example, due to the need of

some researchers for data collected in another country, the data will be encrypted prior to the transmission through a private virtual network from one site to the other, and the collected data will be then added to the database by authorized users (who will need the decryption password).

All of the legal requirements presented above have to be taken into account by the SMART project. Fulfilment of these requirements is necessary to ensure legal compliance of the different use cases with the regulatory framework. These requirements will be consolidated and completed in subsequent ethical reports here.

6 Outlook

In line with the role of the ethics committee, the following work is foreseen for the near future:

- The continued process of DPA submissions
- Evaluation of the use cases
- Monitoring of detected ethical issues
- Identification of new ethical issues.

The DPA submissions are clearly a priority for the committee, although there is little the committee can do whilst waiting for evaluation of the submissions. At the end of the reporting period, the DPA had not provided a final answer regarding the relevant approvals yet, which is a set-back for some of the project's activities. While these answers are expected soon within the next reporting period, the project has also developed fall-back plans in order to be on the safe side in all cases.

In the meantime, the committee has undertaken work towards the design and specification of the data collection processes in the use cases. However, the design of the data collection was not finalized yet, given that some details depend on the reception of relevant ethical approvals from the Spanish authorities, namely the Data Protection Agency (DPA). The approval from the Spanish DPA will be step forward in the project development. The consortium could then start to gather the audio and video data to provide an outdoor use case with real content.

Monitoring of detected issues and evaluation of the risk with newly identified ones is done through the 6-monthly ethics committee meetings. As the project develops the committee is getting more and more involved in the project's ethical issues and in resolving the upcoming and current problems.

The next planned meetings are as follows:

- After the 1st Project review (3rd week in Dec.2012) (Audio conference)
- January/February 2013 (Audio conference)
- June/July 2013 (Audio conference)

7 Conclusions

As an innovative research project, exploring the combination of life data from sensors employed in public spaces and of data from social networks for different use cases, the SMART Project raises a series of ethical and legal concerns. These concerns are related to the capture of and access to the involved categories of data (video, audio, text, speech) – which as such interfere with privacy and related fundamental freedoms – and are aggravated by the development and use of advanced sensor processing and context extraction algorithms, which may render taken precautions to avoid personal identifiable date less effective or useless and open new ethically problematic application areas, e.g. automatic decisions based on "suspicious" behaviour. These issues and the proposed actions for ethically acceptable and legally compliant conduction of the SMART Project itself and planned precautions for future implementations of developed applications are detailed in deliverable D7.8 - Ethical Dimensions of SMART technologies.

This document describes the organisational and procedural aspects of ensuring ethical and legal compliance of project execution, with specific focus on the field trials conducted by the SMART Project. SMART will be conducting research involving human participants. It is, in particular, interested in human behaviour to be observed in the use cases. SMART deploys audio and video sensor technologies in public areas; therefore the project must be very clear and careful with ethics and data protection.

In this document, we have set out the various roles associated with ethics and data protection and their responsibilities: the ethical issues expert, a data protection coordinator along with an Ethics Committee. We have described the terms of reference for these roles and their initial membership composition, mandate, operating procedures and meeting procedures. It also outlines the steps taken to receive the required approvals from the national Data Protection Authorities and the responses received so far. Furthermore, this deliverable contains an overview of the ethical oversight principles that should be taken into account by the ethics expert and ethics committee for each use case.

8 ANNEXES

8.1 Ethics expert and Ethical issues related to the SMART project

8.1.1 Johann Čas CV

Johann Čas holds a degree in Communications Engineering from a Higher Technical College and a degree in economics from the University of Graz. He is a researcher at the Institute of Technology Assessment of the Austrian Academy of Sciences since 1988. He has worked on several aspects of the Information Society and on societal impacts of Information and Communication Technologies. Past foci of research include technological development programmes, impact on employment and regional development, information systems for policy makers, regulatory issues of new telecommunication technologies and privacy. He has also been giving lectures on technology assessment at technical universities. His current research focus is on data protection and privacy in the information society, privacy enhancing technologies and their deployment within Ambient Intelligence, security technologies and health related applications. He was the coordinator of the PRISE EU-Project (http://prise.oeaw.ac.at/), which applied a participatory research approach to develop guidelines and criteria for privacy enhancing security technologies.

Publications: http://www.oeaw.ac.at/cgi-usr/ita/italit.pl?&author=JC&language=en&cmd=get&opt=count

8.2 Initial submission to the DPA (copy of the petition sent on 14th of Dec.2012)

From: Teresa Paula Martinez Zaton
Sent: miércoles, 14 de diciembre de 2011 12:02
To: 'rgpd@agpd.es'
Subject: Consulta a la Agencia Española de Protección de Datos
Importance: High

Buenos días,

Mediante el presente email les aportamos la siguiente consulta para su estudio que esperamos pueda recibir respuesta próximamente.

Por favor, en caso de ser necesario algún documento adicional o la necesidad de ser remitido en papel, hágannoslo saber.

Un cordial saludo

Sr. Director
Agencia Española de Protección de Datos
C/ Jorge Juan 6
28001-Madrid

ASUNTO: Consulta sobre posible tratamiento de datos de carácter personal en proyecto de investigación I+D+i

Teniendo conocimiento de que la Agencia Española de Protección de Datos viene atendiendo las peticiones de informes que se le dirigen a los efectos de facilitar el conocimiento y la interpretación de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, vengo a formularle consulta, en base a los siguientes

ANTECEDENTES

El Ayuntamiento de Santander, junto con un conglomerado de empresas, centros de investigación y Universidades de ámbito internacional, colaboran en la puesta en marcha del denominado “Proyecto SMART”, de investigación científica I+D+i, cuyo documento de síntesis se acompaña en **Anexo** al presente escrito.

Dicho proyecto plantea crear un motor de búsqueda inteligente de contenidos multimedia, basado en la captación de imágenes y sonidos, en vivo, en las calles de la ciudad de Santander y su grabación para dos concretos usos finales: la vigilancia o seguridad pública y la divulgación o difusión de noticias ELIMINARIA ESTE PARANTESIS (en este último caso, previa labor de difuminado de rostros, matrículas u otros posibles elementos identificativos de la personalidad).

La video-vigilancia con el fin de contribuir a la convivencia ciudadana, la lucha contra la violencia, la utilización pacífica de las vías y espacios públicos, como también para la prevención de delitos, faltas e infracciones relacionadas con la seguridad pública, cuenta con una regulación específica contenida en la Ley Orgánica 4/1997, de 4 de agosto, que atribuye la utilización de esa información a las fuerzas y cuerpos de seguridad ciudadana y lo somete a un específico régimen autorizatorio y de control.

En cuanto a la utilización de la información para otros usos, la ausencia de previsiones específicas, hace necesaria la concreción en este ámbito de los principios y garantías que establece, genéricamente, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

Al respecto, debe señalarse que, de acuerdo con la definición contenida en el artículo 3.a) de la LOPD, la imagen y la voz constituyen datos de carácter personal y, por lo tanto, les son de plena aplicación las previsiones de esta Ley Orgánica, en la medida en que dicha información afecte a personas identificadas o identificables.

La falta de una regulación específica, más allá de las previsiones generales recogidas en la citada LOPD, unido al carácter novedoso del Proyecto, hace aconsejable que, previamente a su puesta en marcha, se solicite informe de la Agencia Española de Protección de Datos, en relación con el régimen al que ha de quedar sujeta la gestión de la información que pretende ser objeto de captura y tratamiento.

CONSULTA

Así pues, en virtud de lo señalado, resulta de interés para los socios del Proyecto conocer la opinión de esa Agencia en relación con los siguientes extremos:

1º) Qué requisitos han de observarse y qué autorizaciones es necesario obtener.

2º) Qué sucede si se lleva a cabo un difuminado de los elementos identificativos de la personalidad tras la grabación de las imágenes, es decir, si hace perder a la información capturada la naturaleza de dato de carácter personal, quedando por ello excluido su tratamiento de las determinaciones de la LOPD.

3º) Qué cautelas o condicionados técnicos y legales habrán de observarse para el correcto manejo y utilización de dicha información, teniendo en cuenta, de manera especial, que uno de los aprovechamientos previstos es la difusión de esa información a través de Internet, mediante el uso de las redes sociales o de otras plataformas públicas.

4º) Qué requisitos habrían de observarse en caso de que estas imágenes se captaran en lugares cerrados y privados.

Agradeciendo su colaboración, reciba un cordial saludo.

Teresa Paula Martínez Zatón

Legal consultant

ATOS SPAIN, S.A. Unipersonal

C/ Albarracín, 25
28037 Madrid
Tel: +34 91214 8856
Fax: +34 91214 8272
E-mail: teresa.martinez@atos.net

8.3 Response from DPA

This will be a separated document.

8.4 Revised Submission

From: Teresa Paula Martinez Zaton
Sent: martes, 03 de julio de 2012 17:13
To: ciudadano@agpd.es
Cc: RGPD; Irene Schmidt
Subject: Consulta proyecto I+D
Importance: High

Buenas tardes,

Mediante el presente email nos gustaría trasladarles la consulta contenida en el email adjunto para su estudio y evaluación en relación con la normativa de protección de datos.

No duden en contactarnos en caso de que sea necesaria alguna explicación adicional o mayor información.

Esperamos sus noticias.

Un saludo,

Teresa

Teresa Paula Martínez Zatón

Legal consultant

ATOS SPAIN, S.A. Unipersonal

C/ Albarracín, 25
28037 Madrid
Tel: +34 91214 8856
Fax: +34 91214 8272
E-mail: teresa.martinez@atos.net

Attachment:

INTRODUCCIÓN

El presente documento se remite a la Agencia Española de Protección de Datos con el fin de solicitar su

consentimiento y aprobación para colocar sensores exteriores en Santander, España, con el objeto de realizar un estudio relacionado con las tecnologías de búsqueda multimedia. En los apartados siguientes se establecen el ámbito y los objetivos principales del proyecto para el que se está llevando a cabo el estudio pertinente y, asimismo, se explican las condiciones en las que se colocarán los sensores.

Junto con la presentación de este documento, el proyecto también solicita el asesoramiento de la Agencia de Protección de Datos para garantizar que todas sus actividades (durante el estudio) sean legales y éticas. El proyecto seguirá adoptando medidas correctoras asociadas a los planes presentados con el fin de garantizar la naturaleza ética de sus avances.

¿EN QUÉ CONSISTE EL PROYECTO SMART?

SMART es un proyecto de I+D contemplado en el Séptimo Programa Marco de la Comisión Europea. Este proyecto tiene por objeto crear un motor de búsqueda, en teoría, de todo tipo de datos de sensores (incluidos datos de audio y vídeo) que actualmente no tienen en cuenta los motores de búsqueda de Internet como Google y BING. Asimismo, en el proyecto se pretende estudiar la combinación de información de dominio público proveniente de distintas redes sociales como Facebook, Twitter y Eskup con la información que se recabe de los sensores colocados en lugares públicos. Estos sensores pueden ser de audio o vídeo, así como de otro tipo (de tráfico, meteorológicos, etc.). En la práctica, el proyecto realizará una prueba de concepto con una reducida gama de sensores, del modo indicado en el presente documento.

Conviene señalar que la información que se obtenga con estos sensores no se difundirá ni se transmitirá a través de las mencionadas redes sociales: el flujo de información es unidireccional, es decir, se obtiene información de dominio público de estos sitios, pero no se les facilita información alguna.

Dado que se trata de un proyecto de I+D, SMART no pretende crear un producto para su comercialización. El objetivo consiste en crear un producto experimental que demuestre las dos tecnologías que se están desarrollando en el proyecto y los distintos conceptos que subyacen a estas tecnologías. El proyecto no tiene como objetivo el estudio de personas, la circulación de personas, la conducta de grupos de personas ni otros estudios de carácter social, cultural o antropológico. El proyecto pretende simplemente evaluar la viabilidad técnica de obtener datos de sensores como un flujo continuo de entrada de datos.

Conviene señalar que ya existen numerosos sistemas informáticos capaces de rastrear las redes sociales en busca de palabras clave, personas, etc. y SMART utilizará estos sistemas ya existentes. Se considera que los usuarios de las redes sociales han hecho manifiestamente públicos estos datos.

OBJETIVO

El principal objetivo del proyecto consiste en crear y demostrar técnicas de búsqueda a partir de los datos obtenidos de sensores y redes sociales. De este modo, el proyecto aúna dos ámbitos que, hasta la fecha, permanecían separados:

- acontecimientos que pueden detectarse mediante sensores (como los sensores de datos multimedia (por ejemplo, cámaras) u otros sensores no audiovisuales como los de temperatura);

- acontecimientos que pueden detectarse mediante información de dominio público en las redes sociales. Esta información se extrae de datos textuales que los usuarios han hecho públicos a través de las redes sociales como Twitter. Por ejemplo, una serie de *tweets* relacionados con una concentración pública en una plaza de Santander indicarían un acontecimiento de esta naturaleza.

El objetivo que persigue SMART es desarrollar y evaluar herramientas y técnicas para combinar los flujos de información indicados anteriormente y, a su vez, determinar el valor potencial y la viabilidad de comparar e integrar ambos tipos de información, así como evaluar la manera de poder beneficiarse mutuamente.

TRATAMIENTO, ALMACENAMIENTO Y PRESENTACIÓN DE DATOS DE SENSORES

A efectos del proyecto SMART, no se almacenarán datos de sonido o imágenes de los sensores de audio o visuales. Todo el tratamiento se realiza en tiempo real sobre los datos provenientes de las cámaras y solo se almacenan metadatos[1] relativos a los acontecimientos que sean de interés. Estos metadatos son números que indican la densidad de grupos de personas y el modo en que circulan o los colores que visten. También son metadatos medioambientales provenientes de estaciones meteorológicas o de sensores químicos. Adviértase que las tecnologías SMART no permitirán la identificación de personas. Tampoco se utilizarán en modo alguno para rastrear movimientos o analizar el comportamiento de las personas.

Por consiguiente, no podrán verse datos en ninguna de nuestras interfaces de usuario; solo se presentarán a los usuarios de nuestro sistema los metadatos relativos a acontecimientos.

A efectos de entrenar los algoritmos SMART de señales visuales y evaluar la mejora de su rendimiento durante el proyecto, se llevarán a cabo dos tipos de grabaciones diferentes:

[1]Wikipedia:**Metadatos** (del griego*μετα*, *meta*, 'después de, más allá de'[1] y latín*datum*, 'lo que se da', «dato»[2]), literalmente «sobre datos», son datos que describen otros datos.En general, un grupo de metadatos se refiere a un grupo de datos, llamado *recurso*.El concepto de metadatos es análogo al uso de índices para localizar objetos en vez de datos.Por ejemplo, en una biblioteca se usan fichas que especifican autores, títulos, casas editoriales y lugares para buscar libros.

- grabaciones de vídeo obtenidas en un entorno controlado empleando a actores o personas que hayan dado su consentimiento informado por escrito;
- grabaciones visuales obtenidas en ambientes públicos, en las que se difuminarán las imágenes[2] y, por tanto, se mantendrá su total anonimato. A efectos de entrenar nuestros algoritmos, se difuminarán las imágenes completamente (no solo las partes en las que intervengan personas), por lo que el proceso de difuminado está automatizado.

Con el fin de entrenar los algoritmos SMART de audio y evaluar la mejora de su rendimiento durante el proyecto, se llevarán a cabo grabaciones de sonido. Las grabaciones de audio en lugares públicos se realizarán a una distancia suficientemente alejada de cualquier persona para que el ruido de la grabación impida la detección de voces. Si accidentalmente se detectara alguna conversación durante la grabación, se eliminará de forma inmediata.
La grabación de sonido podría contener alocuciones provenientes de altavoces utilizados en concentraciones públicas. Debido a los altavoces, los niveles de estas alocuciones seguramente serán mayores que los niveles de ruido ambiente. No obstante, por su propia naturaleza, esta clase de alocuciones no debe considerarse información privada.

Por tanto, resulta evidente que el proyecto SMART no identifica, rastrea ni almacena datos personales y, por consiguiente, no viola la intimidad de las personas. Asimismo, no ofrece ningún modo de identificar o almacenar datos personales.

MEDIDAS PARA IMPEDIR LA IDENTIFICACIÓN DE PERSONAS

Es importante subrayar que las imágenes que se capturen en público no permitirán la identificación de las personas. Para ello, el proyecto adoptará una serie de medidas relacionadas con la colocación de sensores audiovisuales y con su funcionamiento. En concreto, los sensores visuales se colocarán a una distancia suficiente para que la cabeza de cualquier persona no supere los 10 píxeles. Se garantizará que no sea posible aumentar la resolución o recolocar el sensor. Para el sensor en cuestión (con una resolución horizontal de 1.920 píxeles y un campo de visión horizontal de 84 grados) esto significa que la persona más próxima se encontrará, al menos, a 16 metros del sensor. El sensor también se colocará a una altura suficiente y apuntando hacia abajo de modo que solo pueda verse la parte superior de las cabezas, a no ser que alguien levante la vista. Dado que en nuestra configuración el sensor se coloca en la segunda planta de un edificio apuntando hacia el otro lado de la calle y hacia abajo, estas condiciones no suponen ningún problema.

Con el fin de impedir la grabación de conversaciones u otro material acústico con el que pudiera identificarse a personas, los micrófonos exteriores se colocarán, al menos, a 10 metros de cualquier persona. De este modo, el nivel de conversación será similar o inferior al nivel del ruido ambiente. A este nivel el lenguaje se hace ininteligible y es imposible identificar al hablante. El sistema final solo procesaría breves segmentos de audio (de uno o dos segundos de duración) y el flujo de sonido en sí no se grabará. De esta manera se impide extraer del audio cualquier otra información, como conversaciones.

En el CD adjunto se recogen ejemplos del tipo de material audiovisual que se capturará. *Queda patente*

[2]Pueden ser personas, caras, colores de ropa, etc.

con estos ejemplos que la identificación resulta imposible.

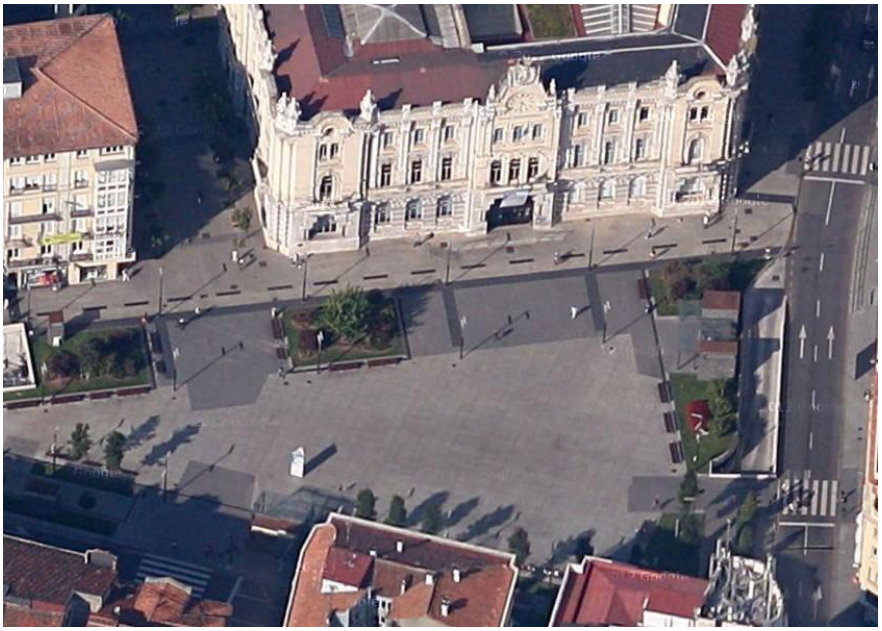
MEDIDAS PARA IMPEDIR LA IDENTIFICACIÓN DE VEHÍCULOS

Dado que los sensores visuales SMART se colocarán principalmente en una zona peatonal, también adoptaremos medidas para evitar la identificación de vehículos (y sus matrículas). Concretamente, todos los vehículos que circulan por la carretera más alejada quedan parcialmente ensombrecidos por las marquesinas de las paradas de autobús y los accesos subterráneos. El ángulo de visión queda perpendicular a la carretera y, por tanto, las matrículas de los vehículos no pueden verse y, en el caso improbable de que sea posible, la resolución del sensor será suficientemente baja para que la matrícula resulte ilegible.

Por tanto, los algoritmos SMART no identificarán ni rastrearán vehículos.

COLOCACIÓN Y LOCALIZACIÓN DE LOS SENSORES VISUALES Y MICRÓFONOS EN EL LUGAR ESPECÍFICO

La instalación de los sensores se realizará en lugares públicos de la ciudad de Santander. Estos sensores consisten en un único sensor visual, un micrófono y diversos sensores medioambientales (estación meteorológica y sensores químicos, por ejemplo). El lugar elegido es la Plaza del Ayuntamiento, donde se colocará nuestro sensor visual del modo indicado en la Figura 1:



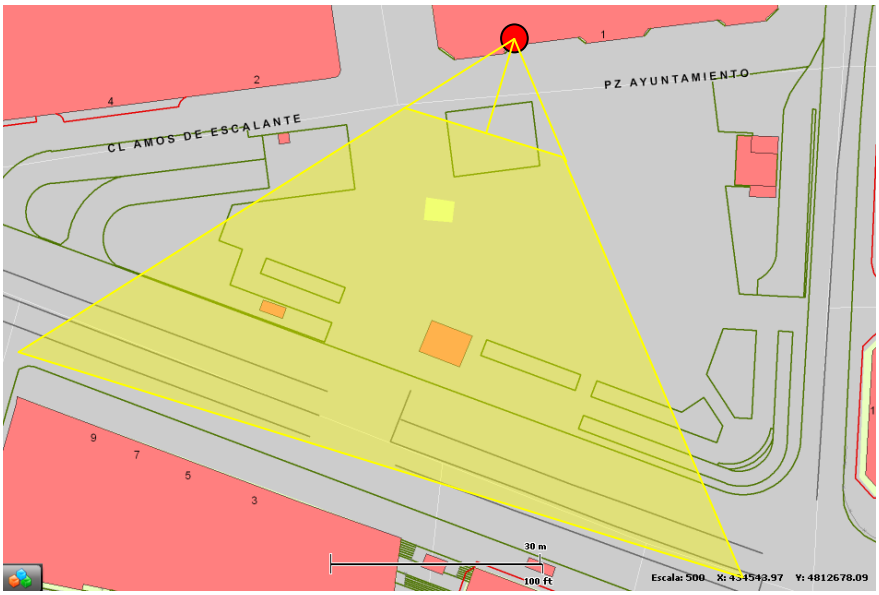


Figura 1:Plaza del Ayuntamiento, fotografía y plano.El punto rojo indica la posición del sensor visual.El trapezoide señala la zona de la plaza que puede verse con el sensor.La distancia *d* del pavimento de la plaza es de 15 metros, que, junto con la altura, garantizan la distancia mínima de una persona y el sensor visual de 16 metros.

Cabe señalar que el área que abarca el sensor no comprende lugares que, por el mero hecho de ser visitados por algunas personas, puedan revelar información personal de ellas:por ejemplo, en el radio de alcance del sensor no hay iglesias (que puedan indicar su religión) ni sedes sindicales (que pudieran revelar su posible afiliación).Por tanto, es imposible que el sensor pueda revelar información, ni siquiera de manera involuntaria, de carácter privado de las personas que entren en su radio de alcance.

CARACTERÍSTICAS DEL SENSOR VISUAL Y DE LOS MICRÓFONOS

El sensor visual consiste en una cámara de exterior AXIS P3346VE, con una resolución máxima de 1.920 x 1.080 píxeles (1.080 p), un campo de visión de 84 grados y una frecuencia de imagen de 20 fps.

Se utilizará un micrófono omnidireccional Larson Davis 426A12-RI para las grabaciones exteriores.

Por este motivo, los sensores audiovisuales no deben considerarse en absoluto “cámaras de vigilancia” ya que esa no es su finalidad ni tienen las características necesarias para poder utilizarlos para la vigilancia de personas.

Sugerimos que se utilice el término "sensores de aglomeraciones" porque describe mejor el sensor visual y de audio ya que, cuando los algoritmos concilian los datos visuales de la cámara, ese es el uso real de los datos obtenidos que grabarán y utilizarán los humanos.

Por tanto, el “sensor de aglomeraciones” se utiliza para:

1. Detectar el tamaño y la densidad de aglomeraciones de gente;

2. Detectar patrones en los movimiento de las aglomeraciones y compararlos con modelos;
3. Detectar cambios de forma y color de las aglomeraciones;

Detectar varios ruidos generados por una aglomeración.

SUPUESTOS PRÁCTICOS

Tomando como base estos sensores y las tecnologías de procesamiento de sensores, el proyecto pretende desarrollar dos aplicaciones TIC que utilizarán los datos de los sensores. A continuación se describen estas aplicaciones con el fin de que despejar cualquier inquietud relacionada con la intimidad.

Noticias en directo:

En el supuesto práctico de ofrecer noticias en directo, el objetivo consiste en crear un almacén de noticias locales y de información general acerca de la ciudad, en este caso, Santander (España).

Este almacén permitirá que los usuarios (ciudadanos) puedan acceder a información y datos estadísticos relacionados con la ciudad.

Principalmente, se mostrará información relacionada con:

- acontecimientos registrados como aglomeraciones de personas, accidentes, etc.;
- tendencias de color de la ropa;
- otros datos y noticias obtenidos de fuentes públicas externas: actualizaciones de noticias, redes sociales, programa de actividades del ayuntamiento...

Esta información podría provenir de los datos procesados que sean captados por los sensores instalados. Solo se precisa la descripción del acontecimiento, la hora y el lugar para el almacén de noticias en directo. No se necesitarán ni se mostrarán datos audiovisuales.

En este supuesto práctico, no se precisa ninguna identificación individual, ya que el objetivo es detectar el acontecimiento y no a los participantes.

Seguridad urbana:

En los escenarios en los que se utilice SMART con fines de seguridad, el tratamiento y la transferencia de los datos y la información se realizarán de manera global para que nunca sea posible la identificación de personas en un lugar determinado.

En estos escenarios, se manejan los datos globales y de proceso en busca de variaciones repentinas respecto del promedio de datos.

Más concretamente, la información relevante es la siguiente:

- densidad de personas excepcionalmente alta en una zona de interés;
- una densidad de personas excepcionalmente alta en una zona de interés mediada por una ventana temporal: el número de personas aumenta o desciende muy rápidamente;
- la velocidad media de las personas es superior o inferior a un nivel umbral específico;
- el movimiento medio de una aglomeración de personas en la zona de interés sufre un cambio repentino;
- partes de una aglomeración de personas cruza la línea en una dirección específica (dirección prohibida);
- partes de una aglomeración de personas cruza la línea en sentido opuesto al que sigue la mayoría de las personas;
- el número del flujo de personas sufre un cambio repentino.

Conviene señalar que:

1. Los sensores no cambian su orientación, profundidad de campo ni ninguna otra característica en caso que se detecte alguna de las incidencias anteriores. Por tanto, es imposible que los sensores se centren en una persona o la sigan.
2. No se establecerán correlaciones entre sensores de manera individual: el sistema no reconocerá ni tratará de identificar si las personas que aparecen en un sensor son las mismas que aparecen en otro sensor. En este sentido, la libre circulación de las personas no se rastrea de forma automática entre los distintos sensores. Asimismo, tampoco resulta posible hacerlo manualmente por la imposibilidad de identificar a las personas que aparecen en los sensores, como ya se comentó en el apartado 4.
3. El objetivo del estudio en este escenario es simplemente registrar la detección de alguno de los acontecimientos descritos en la lista anterior. No se activa ninguna alarma ni se adopta ninguna medida adicional. Por tanto, no habrá ningún tipo de consecuencia para las personas que puedan formar parte de una aglomeración que se produzca dentro del radio de alcance del sistema.

Teniendo todo esto en cuenta, creemos que el sistema no plantea ningún impedimento para la libertad de circulación.

COMITÉ DE ÉTICA

El proyecto SMART es consciente de las implicaciones éticas de estas tecnologías. Por este motivo, el proyecto ha contratado a un asesor ético independiente (véase el currículum vítae en el anexo) y ha constituido un Comité de ética para estudiar las posibles repercusiones y hacer recomendaciones para su uso futuro. Este Comité de ética está integrado por cinco representantes del Consorcio SMART con experiencia en materia de protección de datos y ética. Estos cinco representantes provienen de Atos, en calidad de coordinador del proyecto, Santander, Prisa, AIT y S3Log.

La función del Comité de ética consiste en garantizar que se cumplan todos los requisitos jurídicos y éticos y supervisar la aplicación de la estrategia de gestión de las normas éticas durante el proyecto.

Más concretamente, el Comité (en colaboración con el asesor ético independiente) se ocupa de establecer y aplicar los procedimientos éticos del proyecto. Estos procedimientos podrían tener que ver, por ejemplo, con la confidencialidad de los datos, la solicitud de permisos, la elaboración de impresos para el consentimiento voluntario (en caso de ser necesarios), etc.

El Comité de ética informará al Consejo de Administración del Consorcio y al coordinador del proyecto de cualquier actividad que realice.

ASESOR ÉTICO INDEPENDIENTE

Con el objeto de garantizar la validez de la estrategia ética del proyecto, se ha subcontratado a un experto en ética externo. Puede consultar su currículum vítae en el anexo de este documento. Su función consiste en orientar y asesorar en materia de ética y procedimientos del proyecto. Esta persona es el primer punto de contacto del consorcio para realizar consultas sobre asuntos éticos, como seguridad de la intimidad, dependencia y consentimiento y elaborará el informe ético anual del proyecto.

DETALLES DEL PROYECTO

Socios del consorcio

NÚMERO DE PARTICIPANTE	**DENOMINACIÓN DE LA ORGANIZACIÓN PARTICIPANTE**	ABREVIATURA DEL PARTICIPANTE	PAÍS
1 (coordinador)	**ATOS SPAIN**	ATOS	ES
2	**Research and Education Laboratory in Information Technologies - Athens Information Technology**	AIT	EL
3	**IBM Haifa ResearchLab**	IBM	IL
4	**Imperial College London**	IMPERIAL	UK
5	**Consorzio S3LOG**	S3LOG	IT
6	**TELESTO Technologies Ltd.**	TELESTO	EL
7	**University of Glasgow**	GLA	UK
8	**Prisa Digital**	PRISA	ES
9	**Ayuntamiento de Santander**	AYUNTAMIENTO SANTANDER	ES

El proyecto tiene un presupuesto de 4.155.817 €, de los cuales la Comisión Europea financia 2.686.000 €.

La duración del proyecto es de 36 meses: del 1 de noviembre de 2011 al 31 de octubre de 2014.

Conclusiones

SMART es un proyecto de investigación, financiado con fondos públicos y supervisado formalmente por la Comisión Europea, y tiene por objeto evaluar la viabilidad de utilizar datos obtenidos mediante sensores como flujo de datos multimedia. Estos sensores son meteorológicos, de flujo de tráfico y audiovisuales.

Por lo general, no se almacenan datos audiovisuales. Sólo se guardan metadatos obtenidos de los sensores audiovisuales, como son el volumen y movimiento en masa. Con el fin de entrenar los algoritmos, se utilizarán grabaciones de vídeo de voluntarios a los que se informará y solicitará permiso para ello, además de grabaciones públicas que se difuminarán completamente (serán anónimas) en el momento de su grabación. Por tanto, en ningún momento se grabarán o almacenarán datos de personas susceptibles de ser identificadas individualmente.

Dadas las características y la posición del sensor visual y de audio, será imposible:

1. identificar los rostros u otra información particular de las personas;
2. descifrar las conversaciones de las personas;
3. identificar las matrículas de los vehículos;
4. deducir información personal relacionada con las personas que se encuentren en el radio de alcance del sensor.

Por este motivo, los sensores audiovisuales no deben considerarse “cámaras de vigilancia” ya que esa no es su finalidad ni tienen las características necesarias para poder utilizarlos para la vigilancia de personas.

El sistema se probará en dos supuestos prácticos. En el primero, se intentará correlacionar información de dominio público obtenida en medios sociales con los datos de los sensores con el fin de ofrecer noticias. Por ejemplo, accidentes o tendencias de color de la ropa. No se hará público ningún contenido audiovisual, simplemente metadatos (cuándo, dónde, en qué medida) procedentes de los sensores. El segundo supuesto práctico emula un escenario de seguridad en el que se detectan movimientos imprevistos de aglomeraciones de personas (aumento, movimiento o dispersión de aglomeraciones). En este caso, las personas que conforman la aglomeración no constituyen ningún objetivo ni son rastreadas. Simplemente se emula el escenario de seguridad y no hay consecuencias si se detecta algún acontecimiento (no se activa ninguna alarma): el objetivo es simplemente evaluar la viabilidad hipotética de la tecnología.

El proyecto ha contratado a un asesor ético y ha constituido un comité de ética para garantizar el cumplimiento de las normas.

Además de obtener la autorización para colocar sensores y llevar a cabo los experimentos pertinentes, el proyecto SMART tiene la intención de obtener y divulgar el asesoramiento y las mejores prácticas para la creación de aplicaciones TIC similares de manera legal y ética. A tal fin, el consorcio está interesado en establecer y mantener el contacto con la Agencia de Protección de Datos.

Anexo 1: Currículm Vítae del experto ético

Johann Čas es licenciado en Ingeniería de Comunicaciones por el HigherTechnicalCollege y en Economía por la Universidad de Graz. Desde 1988 trabaja como investigador en el Instituto de Evaluación Tecnológica de la Academia Austríaca de las Ciencias. Ha trabajado en varios aspectos relacionados con la sociedad de la información y sobre las repercusiones sociales de las tecnologías de la información y comunicación. En estudios anteriores se ha ocupado de programas de desarrollo tecnológico, impacto en el empleo y desarrollo regional, sistemas de información para responsables políticos, temas normativos relacionados con las nuevas tecnologías de la comunicación y la confidencialidad. También ha dado conferencias sobre evaluación de tecnologías en universidades técnicas. Su actual campo de investigación se centra en la protección de datos y la confidencialidad en la sociedad de la información, las tecnologías de protección de la intimidad y su aplicación en entornos inteligentes, las tecnologías de seguridad y aplicaciones relacionadas con la salud. Fue el coordinador del proyecto PRISE de la UE (http://prise.oeaw.ac.at/), en el que se adoptó un enfoque de estudio colaborativo para el desarrollo de directrices y criterios dirigidos a las tecnologías de la seguridad y protección de la intimidad. Actualmente coordina y participa en varios proyectos del Séptimo Programa Marco sobre tecnologías de vigilancia y seguridad con especial interés en el impacto en la sociedad y el cumplimiento de derechos y valores fundamentales. También ejerce como crítico y asesor ético de propuestas y proyectos de investigación.

Publicaciones:

http://www.oeaw.ac.at/cgi-usr/ita/italit.pl?&author=JC&language=en&cmd=get&opt=count

8.5 SMART Informed Consent Form

Purpose of data collection: *The following data will be collected for an 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 ethics committee Members>	
Who has access to this information: By signing the form you give your consent 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* .....