Authors (alphabetical order)

Dr. Francisco Flórez-Revuelta (KU)
Dr. Feng Gu (KU)
Prof. Barbara Pierscionek (KU)
Prof. Paolo Remagnino (KU)

Internal reviewers (alphabetical order)

Prof. Mary Chambers (KU)
Ms. Karen Galligan (TCD)
Mr. Daniel Heery (Cybermoor)
Mr. Ángel Martínez-Cavero (TSB)

Graphic design

Erremme Associati

Published on January 2015

BREATHE

Because you have the right to feel good and BREATHE.

WHITE PAPER ON AAL SYSTEMS AND ASSOCIATED PRIVACY ISSUES

TABLE OF CONTENTS

Table of contents 02
Executive summary 03

1 Introduction 04
2 Privacy, ethical and legal issues 05
3 Privacy by Design 07
4 Privacy-enhancing technologies (PETs) 08
5 Privacy by context 09
6 Privacy in AAL system 10
7 Visual privacy 11
8 Privacy preservation in the BREATHE project 13

Disclaimer 14

Due to the aging population and an insufficient amount of professionally trained carers, i.e. informal carers worldwide, Ambient assisted living (AAL) technologies have gained an increasing popularity in terms of assisting both the assisted person and their carers via the information and communications technology (ICT). Majority of the AAL applications utilise different types of sensors to gather data and information of the assisted person, in order to evaluate their wellbeing and subsequently to provide appropriate support if needed. However, handling the data and information of the assisted person and their carers raises ethical, legal and regulatory issues. To resolve this, means of protecting the relevant data and information must be incorporated into the system to ensure the privacy of the assisted person and their carers, throughout the design and development of AAL systems and ultimately their use.

The main ethical principles that apply to AAL are beneficence, non-maleficence, confidentiality and respect for autonomy. Subjects in AAL applications should be treated as autonomous adults who can mentally make decisions about their welfare. This can be problematic when sensing technologies are involved, in particular, cameras. A typical vison system employs a set of cameras to gain complementary fields of views of the monitored scene, to continuously identify the subject's locations and detect their activities. In order to prevent the subject from being visually identified by any images or videos of the scene, the vision system must be modified with respect to privacy. For instance, if such a system operates in real-time, where all video streams are processed to generate locations and activities of the subject without storing any images or videos of the scene, then the subject cannot be visually identified. The processed information, e.g. logs of the locations and activities, can only be accessed by authorised personnel, e.g. the subject's carers. Whenever a dangerous situation is detected, e.g. a fall, if the subject's carers require live streaming of the scene, then computer security methods can be used to authenticate the access and establish a secured streaming channel. In addition, vision-based privacy filters can be applied to ensure the subject is visually unidentifiable while maintaining an informative representation of the situation. For example, the area of the subject can be pixelated or replaced by an avatar with the same pose. As a result, many privacy-related technologies can be introduced to AAL applications to resolve the corresponding ethical issues, it is a matter of whether the developers are able to incorporate and enforce such a design philosophy.

BREATHE aims to design and develop an intelligent monitoring system for AAL environments, by employing cameras and other types of binary sensors. In order to ensure the privacy of user data and information, BREATHE follows a privacy-by-design approach. Particularly, BREATHE considers privacy by context where data is acquired and transmitted depending on a number of parameters established by the identity and state of the assisted person, the carer, and the environment. Moreover, an intelligent access control scheme would be implemented, where the access to user data and information is authenticated based on the pre-assigned security privileges of other parties. For instance, the scheme should automatically recognise and filter data and information that is not pertinent to the carers observing. The main design philosophy of BREATHE is to reduce not only the potential for failure by a person/organisation collecting data to adhere to best practice in safeguarding user data and information, but also the potential for security breaches of data storages.

Ambient Assisted Living, commonly abbreviated as AAL, plays a major role in helping formal and informal carers to provide support in assisting the person cared for and a higher degree of independent living. AAL systems usually make use of an intelligent system that provides a means to interact between a user (carer and cared for person) and the system itself that can elaborate sensory information to detect events and incidents in a controlled private environment. Technology is gradually gaining acceptance as a means to complement the work of caregivers by monitoring and assisting persons with reduced physical or cognitive capacity in their day-to-day living. Ambient assisted spaces make use of a collection of sensors that collect information from the environment or its dwellers. Binary sensors are employed to detect or record on/off status, temperature, motion, pressure or lighting level[1]. These embedded sensors make it possible to obtain the state or context of the environment. Detection and tracking of people can be implemented using infrared ceiling sensors, sensors embedded in the carpet, and radio-frequency identification (RFID) tags or other sensors worn by the users[2]. Other more complex systems employing audio and video can also be used. These sensors monitor the persons and their interactions with other people or objects and allow the recognition of activities of daily living or untoward events, e.g. falls[3].

Advances in sensor technology together with decreasing costs, in particular of cameras, have led to their extensive use as a tool for monitoring public and private spaces. Cameras are now commonly used to monitor environments such as streets, train stations, airports and hospital buildings and are in widespread use in major cities. While monitoring technology for public security and associated research is relatively mature, attention is now focussed on the use of sensing technology embedded in equipment and devices used to promote health and enhance wellbeing and safety, or in systems to help maintain an independent life at home. Monitoring is often seen as intrusive and as violating rights to privacy. This potential loss of privacy is exacerbated by the use of cameras because video data is easily understandable by unauthorised viewers.

There are a number of ethical and legal requirements that must be adhered to in order to preserve privacy. Thus methods to enhance privacy must be considered when designing assistive technologies in order to avoid seeing them as intrusive and to increase acceptance. Therefore, BREATHE follows a privacy-by-design approach. Particularly, BREATHE considers privacy by context where data is acquired and transmitted depending on a number of parameters established by the identity and state of the assisted person, the carer, and the environment.

1 D.J. Cook, W.Z. Song: Ambient Intelligence and Wearable Computing: Sensors on the Body, in the Home, and Beyond, Journal of Ambient Intelligence and Smart Environments, 1:83-86, 2009.

2 S. Patel, H. Park, P. Bonato, L. Chan, M. Rodgers: A review of wearable sensors and systems with application in rehabilitation, Journal of NeuroEngineering and Rehabilitation, 9:1-17.

3 P.Rashidi, A. Mihailidis: A survey on ambient-assisted living tools for older adults, IEEE journal of biomedical and health informatics, 17:579-590, 2013.

The main ethical principles that apply to AAL are beneficence, non-maleficence, confidentiality and respect for autonomy. Underlying the application of these principles is the presumption that this applies to subjects who can be treated as autonomous adults and therefore adults deemed to be mentally unfit to make decisions about their own welfare, will not be included.

Beneficence relates to the doing of good and the expectation that the proposed research will bring benefits to the researchers, subjects and/or to society at large. It takes into account that the outcomes of safer and more secure home environments will a) allow people to maintain their independence for longer in home settings and b) produce safer communities and societies by improved minimally intrusive surveillance measures.

Non-maleficence addresses the issue of minimising or ideally avoiding any harm and requires that the benefits of the research outweigh any unavoidable risks. This involves a risk/benefit analysis to identify potential risks, eliminate as many as possible and balance remaining unavoidable risks against benefits from the research outcomes. The risks in the data handling aspects can be avoided by ensuring that data is properly anonymised and that confidentiality issues are fully identified and addressed.

Confidentiality requires personal data (that by which an individual can be identified) to be protected. The amount of personal data should be minimised and only acquired where necessary for the project. Such data should only be available to researcher(s) in the case of a research project and in all cases to the carer who needs to access it. It should be kept secure for a period that adheres to the data protection regulations in the member state where it is being collected and maintained as well as to EU regulations.

Respect for autonomy recognises the right for assisted persons (AP) to be fully informed that they are being watched and how and for what their data will be used. They should have control over the times and durations that they are being watched.

Privacy and dignity of the individual

The underlying human factor that needs to be carefully monitored at every stage is maintaining the dignity of the individual. This should take into account the fact that those who require care, the APs are particularly vulnerable. The points that will be considered are:

- Full understanding of what the technology offers and what data will be used, viewed, transferred and stored;
- Who will be viewing, what activities and when; and
- The potential of third parties inadvertently seeing the AP and how this can be averted and managed

Regular updates to the AP of what has been transmitted and viewed will address these issues. The input of the AP and their views, which may alter with time, will be taken into account.

The issue of privacy and the fact that the carer will be able to view the AP may alter the relationship between the two. This is difficult to anticipate as it may strengthen the bond, increase the dependency and thereby the pressure on the carer or it may make the AP feel that the carer has too much control over the privacy of the AP. This will be carefully monitored and changes in the relationship addressed.

Legal issues

The law on confidentiality in the UK is governed by the Data Protection Act 1998[4] and is summarised in the 8 principles that cover data control, types of data, modes and length of time of storage, permission to use the data and data transfer. Similar legislation is applied in the Republic of Ireland (Data Protection Acts 1988[5] and 2003[6]) and Spain (Organic Law 15/1999 of 13 December on the Protection of Personal Data[7]). The EU data protection reform, which vote was taken in the European Parliament in March 2014 aims to harmonise data protection across the EU.

4 Data Protection Act 1998, http://www.legislation.gov.uk/ukpga/1998/29/contents (accessed on November 2014)

5 Data Protection Act 1988, http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html (accessed on November 2014)

6 Data Protection (Amendment) Act 2003, http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html (accessed on November 2014)

7 Organic Law 15/1999 of 13 December on the Protection of Personal Data, http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/Ley_Orgaica_15-99_ingles.pdf (accessed on November 2014)

The term Privacy by Design[8] was created in the 90s by Ann Cavoukian, Information & Privacy Commissioner of Ontario, Canada. Privacy by Design refers to the philosophy and approach of embedding privacy into the design, operation and management of information processing technologies and systems.

Her office developed the 7 Foundational Principles of Privacy by Design, which are nowadays a reference in the design of technologies. These principles are:

1. Proactive not Reactive; Preventative not Remedial

The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before the fact, not after.

2. Privacy as the Default Setting

We can all be certain of one thing – the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

3. Privacy Embedded into Design

Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that it becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Security – Full Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.

6. Visibility and Transparency – Keep it Open

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy – Keep it User-Centric

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

8 A. Cavoukian: Privacy by Design, http://www.ipc.on.ca/images/Resources/privacybydesign.pdf (accessed on November 2014)

The application of Information and Communication Technologies (ICT) to protect privacy has become extensively known as Privacy-Enhancing Technologies (PETs). They have been described in different ways but the most adopted definition was made in the PISA European Project

> "Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of functionality of the information system [9]."

These technologies are very relevant nowadays. For instance, the European Commission considers that PETs should be developed and more widely used, in particular where personal data is processed through ICT networks. The Commission considers that wider use of PETs would improve the protection of privacy as well as help fulfil data protection rules. The use of PETs would be complementary to the existing legal framework and enforcement mechanisms[10].

PETs incorporate Fair Information Practices (FIPs), following for instance the basic principles developed by the Organisation for Economic Co-operation and Development[11]:

- **Collection Limitation:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject;
- **Data Quality:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date;
- **Purpose Specification:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose;
- **Use Limitation:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except a) with the consent of the data subject; or b) by the authority of law;
- **Security Safeguards:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data;
- **Openness:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller;
- **Individual Participation:** An individual should have the right a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended; and
- **Accountability:** A data controller should be accountable for complying with measures, which give effect to the principles stated above.

---

9 PISA Consortium: Handbook of Privacy and Privacy-Enhancing Technologies – The case of Intelligent Software Agents, G.W. van Blarkom, J.J. Borking, and J.G.E. Olk (eds.), 2003.

10 Commission of the European Communities: COM(2007) 228, Communication from the Commission to the European Parliament and The Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), 2007.

11 OECD: The OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed on November 2014)

Ubiquitous computing, context awareness, intelligence and natural interaction are the main properties of ambient intelligence and smart environments. Context is "any information that can be used to characterise the situation of entities (i.e. whether a person, place or object) that are considered relevant to the interaction between a user and an application, including the user and the application themselves. Context is typically the location, identity and state of people, groups, and computational and physical objects[12]." Context-aware computing refers to an application's ability to adapt to changing circumstances and respond according to the context of use[13].

Recently, a privacy-by-context paradigm was introduced for remote visual monitoring of assisted persons[14]. This paradigm proposes a level-based scheme to access video data (although it could be extended to any personal data) in order to protect privacy. Each level establishes the way in which the video stream is modified and displayed and, therefore, which protection degree is provided. In this scheme, the appropriate level is dynamically selected according to the context, modifying the raw video before it is displayed, as originally proposed in the "Good Brother" proposal[15].

The context should provide enough information to empower the assisted persons to adapt privacy to their preferences, in such a way that they can decide who, how, and when their carers can watch them. In an assisted living environment the context may be described by:

1. The identity of the subject, in order to retrieve the privacy profile;
2. The appearance, e.g. dressed;
3. The location, e.g. kitchen, bathroom, bedroom;
4. The on-going activity, e.g. having a shower, watching TV, sleeping, receiving a visit; and
5. The identity of the observer: the closeness of the assisted person with a particular carer.

Using these variables, an individual can then select in advance a visualisation level to any situation that could be modelled by the context, i.e. giving different permissions to access the video stream to the various different carers in different ways according to what is happening at the assisted person's home.

12 A.K. Dey, G.D. Abowd, D. Salber: A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications, Human-computer interaction, 16(2):97-166, 2001.

13 N. Bricon-Souf, C.R. Newman: Context awareness in health care: A review, International Journal of Medical Informatics, 76(1):2-12, 2007.

14 J.R. Padilla-López, A.A. Chaaraoui, F. Flórez-Revuelta: Visual Privacy by Context: A Level-Based Visualisation Scheme, 8th International Conference on Ubiquitous Computing & Ambient Intelligence, in Lecture Notes in Computer Science, 8867:333-336, 2014.

15 J.R. Padilla-López, F. Flórez-Revuelta, D.N. Monekosso, P. Remagnino: The "Good" Brother: Monitoring People Activity in Private Spaces, 9th International Symposium on Distributed Computing and Artificial Intelligence, in Advances in Intelligent and Soft Computing, 151:49-56, 2012.

AAL solutions may also be designed to learn the daily behaviour of the assisted person, in order to perform context analysis and to detect relevant deviations a predefine normality. These solutions often collect large amounts of user data that is extremely sensitive and confidential. As a result, the usual rule of data handling is to avoid transferring raw data to a central location, where various decision-makings are made. Even if this requirement most likely increases the equipment costs at the assisted person's premises, all data collection and processing should be done on a local level and raw data must not leave the home. Later, processed information from the raw data is allowed to transfer outside the home to inform a second party, e.g. the informal carer, but via a secured channel. This is especially true when a critical situation is detected and the resulting alert should be sent to a third party, e.g. a cloud-based server for communications between the first party (assisted person) and second party (informal carer). Privacy and security can be preserved by designing an AAL solution with respect to the following aspects[16]:

- **Integrity** – any data transmission must be verified, e.g. checksum and digital signature etc.
- **Authenticity** – evidence of data source must be provided, e.g. sensor identification etc.
- **Confidentiality** – privacy protection by encryption of sensitive data and information, e.g. anonymity of the assisted person
- **Multi-Level User Control** – different level of protection on confidential data and information via user access control methods

In an AAL application it is crucial to guarantee safety of the confidential data and information, while offering privacy to the users whenever requested. An important requirement is to balance between unobtrusive and completely hidden technology. Acceptance of assisted persons is reduced if too much visible monitoring technology is in their homes. However, a completely hidden system, where the technology is embedded in the environment, could become ineffective and potentially unable to detect potentially dangerous situations. An AAL solution should offer both safety and comfort for the assisted person.

16 F. Winkler, B. Rinner: TrustCAM: Security and privacy-protection for an embedded smart camera based on trusted computing, in Proceedings of the IEEE Conference on Advanced Video and Signal Based Surveillance, pp. 593–600, 2010.

Video cameras are being used more frequently in AAL applications. Computer vision gives the possibility to monitor 24/7 an environment and report on visual information, which is commonly the most straightforward and natural way of describing an event, a person, an object, actions and interactions. The advances produced in the last decades have contributed to this. The computational power has been increased while, at the same time, costs have been reduced. Furthermore, computer vision advances have given video cameras the ability of `seeing', becoming smart cameras. This has enabled the development of vision-based intelligent monitoring systems that are able to extract useful information from visual data to analyse actions, activities and behaviours[17]. Video cameras are being increasingly used in order to offer novel telecare services that rely on visual information, e.g. monitoring of activities of daily living (ADL), fall detection, warning system, and many others. They are also been considered to evaluate the quality of care. These uses are beginning to be explored by care providers[18] and regulators[19] .

Traditionally cameras have been used in public spaces for surveillance services in streets, parking lots, banks, airports, train stations, shopping centres, museums, sports installations and many others. Generally the use of video cameras in public places has been tolerated or accepted by citizens, whereas their use in private spaces has been refused. There may be several reasons to explain this difference. On the one hand, the perceived public-safety benefits favour the usage of cameras in public places for crime prevention, fight against terrorism and others[20]. On the other hand, there is a widespread belief that while staying in public environments, people's sensitive information will not be exposed. However, they are not commonly used within private environments due to people's concerns about privacy as video can convey an enormous amount of information that can be qualified as sensitive.

Intelligent vision-based monitoring systems jeopardise individuals' right to privacy because they can acquire, store and show a variety of information about people habits, relationships, and so on. This evolution in people's monitoring may be seen as approaching an Orwellian Big Brother, as people may have the feeling of being constantly monitored. Therefore, privacy-aware smart cameras become essential for AAL applications. Thus, if individuals' privacy can be guaranteed through the use of smart cameras, acceptance would be increased.

17 A.A. Chaaraoui, P. Climent-Pérez, F. Flórez-Revuelta: A review on vision techniques applied to Human Behaviour Analysis for Ambient-Assisted Living, Expert Systems with Applications, 39(12):10873-10888, 2012.

18 HC-One Limited: HC-One's Consultation on an Opt In Visible Camera Scheme, http://www.hc-one.co.uk/media/image/Visible_Camera_Consultation_Report_Oct_2014_LATEST.PDF (accessed on December 2014)

19 Care Quality Commission: Care Quality Commission Board meeting: 19 November 2014, item 8, http://www.cqc.org.uk/content/care-quality-commission-board-meeting-19-november-2014 (accessed on November 2014)

20 S. Graham, J. Brook, D. Heery: Towns on the television: Closed circuit tv in british towns and cities, Local Government Studies, Volume 22, Issue 3, 1996.

There are two approaches in order to protect and preserve individual's privacy in videos and images. These depend on when privacy protection is applied: before the image is acquired (image acquisition time), or after (image processing time). On the one hand, it is possible to prevent others of successfully capturing images in which an individual appears. On the other hand, once an image has being acquired and is going to be distributed, shared, or visualised; some parts from it, which are considered private, can be filtered or removed.

Current methods for visual privacy preservation include intervention, blind vision, secure processing and redaction (Table 1).

Intervention	Intervention methods deal with the problem of preventing someone to capture private visual data from the environment. They can be as simple as to empower the monitored person to turn off the monitoring. There are also automatic methods that physically intervene camera devices to prevent the acquisition of an image by means of a specialised device that interferes with the camera optical lens
Blind vision	Blind vision addresses privacy related processing issues by means of secure multi-party computation techniques that are applied to vision algorithms. Secure multi-party computation is a subfield of cryptography that enables multiple parties to jointly compute a function in such a way that their inputs and the function itself are not revealed.
Secure processing	This approach is similar to blind vision but it is not based on secure multi-party computation. These methods process visual information in a privacy respectful way, e.g. working with images in a domain that does not reveal visual information, rejecting visual information that is not necessary for the algorithm to work. Recently, some systems employ depth/range sensors that allow working only with silhouettes avoiding using any other visual data.
Redaction	Image and video modification or redaction methods are the most common visual privacy protection methods. They modify the sensitive regions of an image (faces, bodies, objects, number plates, etc.) to conceal private information concerning the subjects appearing on it. Redaction methods include ad-hoc distortion/suppression methods, image encryption, face de-identification, and in-painting based algorithms. In order to determine the sensitive regions in which a redaction method operates, computer vision algorithms are used. This is one of the main difficulties, as those private regions must be correctly detected at every moment.

Table 1. Methods for visual privacy preservation

The main objective of BREATHE is to provide an ICT-based solution to support and relieve the burden experienced by informal carers and improve the quality of life of both the carer and the person who is being cared for. The platform is composed of two different modules, namely the AAL home system and the informal caregiver tool. The first module consists of a group of cameras and an array of sensors installed at the assisted person´s home and is responsible for collecting information on a daily basis and in an automatic way about the activities and behaviour of the assisted person. The cameras allow different types of video processing to enable varying levels of privacy. The informal caregiver tool will be based on a Web platform that provides, to the family carer community, guidance and support to improve their living conditions and enable, as a result, a better quality of care.

BREATHE develops the principles of privacy by design in the following way:

- Access to the reports generated by the system occurs through a password-protected and encrypted online interface. Besides, access to individual information is restricted to the individual's caregivers following the permissions granted by the assisted person;
- Embedded privacy does not negatively impact the availability of critical information to the caregivers including real-time alerts;
- Broadcasting of video follows the privacy-by-context approach where different visualisation alternatives are offered according to the context, i.e. on-going activity or event, location of the assisted person, and identity of the observer;
- Different redaction methods, which avoid to see the real image of the assisted person, are employed to support those visualisation levels established by the context;
- The assisted person is empowered to turn off the monitoring system at will;
- The assisted person is empowered to assign the different visualisation levels to different contexts.

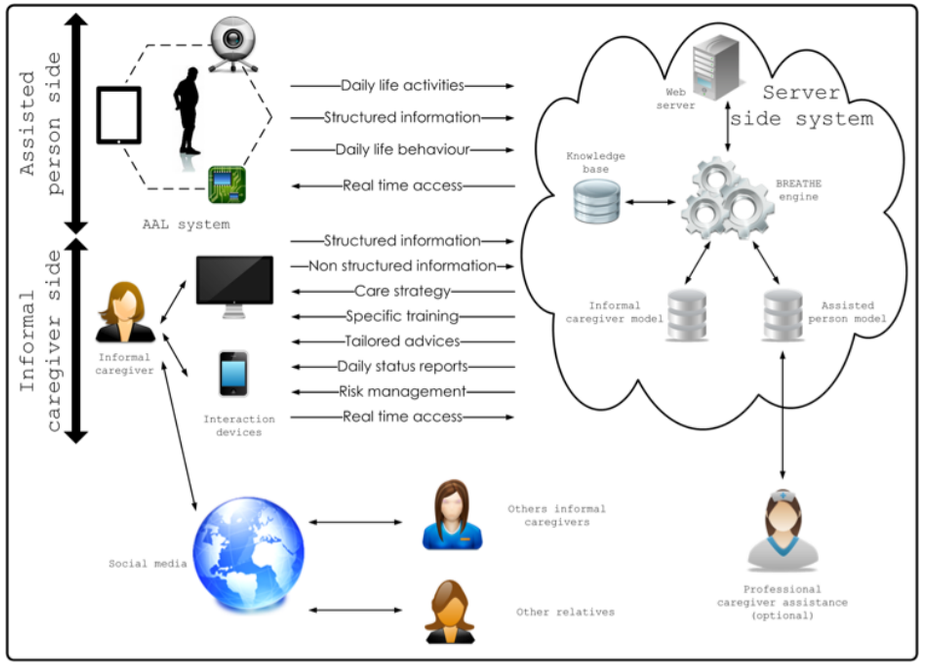

Figure 1. Overall BREATHE system

BREATHE Project has been co-funded by the Ambient Assisted Living Joint Programme (Call 5, 2012) and some National Authorities and local Research Programmes in Spain, United Kingdom, Ireland and Italy.

The ownership of IPR (Intellectual Property Right) as well as all foreground information (including the tangible and intangible results of the project) will be fully retained by all partners without exception. All issues regarding confidentiality, dissemination, access rights, use of knowledge, intellectual property and results exploitation are included in the Consortium Agreement (CA), which was signed by all partners before starting the project.

DISCLAIMER

TRINITY
COLLEGE
DUBLIN

Contact Us

Juan-Pablo Lázaro-Ramos
- Project Coordinator -
+34 96 182 71 77 | jplazaro@tsbtecnologias.es

Visit us on the Web
http://www.breathe-project.eu

Project reference
AAL-JP-2012-5-045