Privacy and Data Protection towards Elderly Healthcare

Ângelo Costa
ISLab, Departament of Informatics, University of Minho, Braga – Portugal
acosta@di.uminho.pt

Francisco Andrade
Law School, University of Minho, Braga – Portugal
fandrade@direito.uminho.pt

Paulo Novais
ISLab, Departament of Informatics, University of Minho, Braga – Portugal
pjon@di.uminho.pt

ABSTRACT

Developed societies are registering a dramatic change in terms of population evolution, being the most important fact the high tendency in the ageing of the whole population. An alarming fact is that the birth-rate is dropping very fast, inverting the ageing pyramid that used to have a higher incidence on the young population, now having a higher incidence in the older population. In the quest to provide answers to some problems the elderly population has, applications and projects arise from the Ambient Assisted Living area, providing services that help the user in his daily life, providing the needed help and trying to be the less invasive as possible. The fact is that these systems operate optimally by using information about the user, assisting him accordingly to his preferences. The data gathered for such events is highly personal and sensitive. Being this data escalating several stages until it finally is ready to be inserted in the system. This can cause a loss of privacy and data protection. In this document we present an Ambient Assisted Living project towards assistance to an elderly population and the problems and possible solutions in the legal area towards loss of privacy, data protection and personal information.

INTRODUCTION

The most developed countries in Europe register a tendency for a fast and progressive ageing of the community, mainly because of decreasing both in mortality and in fertility. Due to advances on the medical field, ordinary people is benefiting of increased longevity. Actually, in the past few years, life expectancy increased exponentially, and in the last 10 years life expectancy increased 12 years. The combination of the increase in life expectancy and a simultaneous decrease of births induced changes in the way people live their daily life, such as family composition, living arrangements, housing demand and even in the type of health care services (Nations, 2009).

Both Society and Health Care Services need to get responses to this ageing revolution. There is a need to rethink planning and health care provisioning in order to improve the quality of life of ordinary people. The current availability of medical care and healthcare providers, in form of continued care and surveillance of the user, like nursing homes, are very scarce and are also very limited. Adding to the fact that such services are costly, and most of the persons do not have the resources to sustain it. As technology and computer science progresses towards the construction of applications in the medical and social area, like monitoring software that is used to aid the user in everyday tasks (Chisholm & D. B. Evans, 2007).

Ambient Assisted Living

The Ambient Assisted Living (AAL) paradigm states that a person in need should always be assisted, by persons or technology. This paradigm means that the person should be safe and cared in his own environment, his home (Nehmer, Becker, Karshmer, & Lamm, 2006).

Projects are commonly being developed in terms of visual monitoring and domotics, they provide the monitoring and automation much needed to help the user. Thus the user benefits from constant surveillance and help with basic tasks, but far more interesting help could be provided. The new advances are from discrete processes such as transparent and ubiquitous technology, and intelligent interfaces (Rubel et al., 2004). These technologies adapt to the user, to provide a better and personalized service, adjusting to the user needs. This means that the users that suffer from diseases, such as cognitive problems, mobility difficulties and visual or hearing problems. The interfaces can provide an easier way to operate and interact with the rest of the system, being constructed to provide an intuitive interface that can be used by persons with no technological knowledge.

A common problem with those systems is that they require total cooperation of the user and are heavily based on the user profile and decisions. In order to be useful, the systems have to collect several data in real-time so they can adapt to the variables the user encounters at a certain point, so they can be able to respond accurately to the presented situation. An initial profiling system also requires the interaction with humans who formulate questions; the system avails the responses of the user in order to create a base profile of the system.

Typically these systems require that personal and sensible data are shared between several persons and in some systems the information is also available to other users and relatives, for instance projects that are heavily based in social networks. Although most projects are suggestive, a feature that is often present is the automatic changes related to the execution of events or tasks. The fact that the systems make individual decisions, not consulting the user, can overtake his life and proceed to make substantial changes in it, and the user will only realize some of these changes when serious consequences arise. About this, several questions must be faced: how the knowledge will be protected? How much of the information matters and what should be released? What is the impact of the automated decisions? How sensitive information should be categorized? What control should the user be allowed on the use of his data?

Next it will be presented the motivation of this work, reasoning about the implications of computer systems and the legal implications. Afterwards it will be presented the memory assistants and the iGenda project and the various sub-modules, a project that assists elderly persons using sensitive information, being the motivator of the discussion about the legal implications about the data privacy. Legal aspects will be discussed and how the Portuguese Constitution see these types of projects and how it is prepared to protect people and legally justify the authorization of exchange of sensitive data. Finally the conclusion and future challenges will be presented, discussing how measures should be adopted to best protect the final user.

MOTIVATION: HEALTHCARE AND PRIVACY

The medical science is now a joint collaboration between humans, machines and computers. Although the decisions are solely made by the physicians computers provide a much needed aid to help in terms of providing easy access to test and results and providing suggestions to help the decision towards the current health condition of a patient.

Most of the suggestions provided by applications that work with sensitive data, such as medical data, are ultimately reviewed by specialized people, like doctors. The fact is that machines currently must not take actions when health-related problems are concerned. This is a normal condition, as the applications available are not developed enough to take into account the principal aspects of human and social conditions. The persons involved in the medical area have to follow a deontological code of protection and safeguard of human life and privacy, being a much discussed aspect. But currently it does not exist a discussion or action taken toward a code of conduct on the computer science area. People and applications do not have to follow a standard of data privacy and protection, being sensitive data shared across people and systems with no regards of protection whatsoever.

Everyday computer technicians read and work on users/patients data and information that the user struggles to keep private, and this is an action that should not be stopped. Hospitals and healthcare facilities rely on the data collection and the treatment they are subjected to, so sacrificing privacy in order to keep the workflow running and helping to provide a more reliant and resolute service provision (Adam & D. B. Evans, 2006; Baltussen et al., 2003; Chisholm & D. B. Evans, 2007). We do not mean that this situation is bearable, but also we do not believe that terminating the current actions is also the solution. New methods should be constructed around the current establishment and workflow in order to embrace a solution that ensures the balance between users concerns and hospital and healthcare requirements (TimesTeam, 2010).

It is clear that the collection of text provided by the user is data, but does it mean anything? The provision of relation and context is what transforms the data into information, is what distinguishes random string of data from an important medical fact. The collection of user facts by a nurse at the triage on a hospital is data collection, and the processing by a computer application or a technician is what provides meaning to data, thus turning it into intelligible information. The leakage and sharing of information across hospitals, physicians and other persons is very important but privacy and data protection are fundamental right constitutionally granted to every person (Miguel, 2004).

MEMORY ASSISTANTS

The Memory Assistants area is growing rapidly and is already a topic of importance and concern in the view of the scientific community. Being a merge between the health science and the computer science, in simple terms it is the introduction of mental and cognitive areas and health-related computer applications. Memory loss has been a recurrent problem that science struggles to solve, but in the meantime support has to be provided to people that are already suffering of memory loss (Charness, 2008; Geda et al., 2008; Nice, 2011; Tucker, 1995).

Memory loss in terms of long-term memory is in fact a complicated problem, studies conducted by the University of Harvard shows that the section of the brain that stores the long term memories is also the one that provides creative envisioning. A simple relation can be drawn: without the ability to remember previous actions and their outcome it is impossible to establish the binomial action-reaction, thus limiting the capacity of generating new ideas, new events or structure of a day flow.

Three stages are clearly identified in terms of cognitive impairment: no cognitive impairment, mild cognitive impairment and severe cognitive impairment. These types of impairment are translated into different steps of memory loss, the first stage meaning that the person has no cognitive impairment or is slightly affected by memory loss ("where are my keys" paradigm), the second stage meaning that the person has some problems in his daily life and the shortages of memory are starting to affect his execution of simple tasks, the third stage meaning that constant surveillance is required and that the person cannot perform on his own almost none of the simplest tasks. The persons that are in first and second stages are the ones that can be aided in terms of technology availability, enabling them to fill the recurrent gaps in terms of memory.

Currently there are several projects and several applications in software and hardware dealing with this. There are advances in various types of projects being developed. As examples there are the Hermes and SenseCam projects (Hodges et al., 2006; Jiang, Geven, & Zhang, 2009).

The memory assistants are better described by the following features: they help the user in their daily tasks in the form of suggestions of events related to what the user is performing at that moment or, at the end of the day, they review the user’s actions or places where he was present.

Still there are no projects currently focused in terms of interactivity and full automation. What is meant by this is that the various projects referred to still require a great deal of attention by the user, both in terms of configuration of all the options and of correction of errors resulting from the execution, regardless of simple notifications that a simple PDA can do without much configurations. The desired interactivity is something near the ubiquitous and transparent operation, having an interface that requires little learning by the user. It must also operate on an almost automatic and intelligent way, demanding from the user little or no repairs. This project places itself on aiding users with second stage of memory loss, a Mild Cognitive Impairment, having frequent memory gaps but fully able to make decisions and choices.

IGENDA PROJECT – AN INTELLIGENT MEMORY ASSISTANT

The iGenda project is a project developed in the University of Minho in Portugal (Â. Costa & Novais, 2011; Â. Costa, Novais, J. M. Corchado, & José Neves, 2011). It is integrated in the AAL environment. It consists in an intelligent agenda that automatically schedules events and free time activities. The events are scheduled by other persons and the system undertakes the task and schedules the tasks in the user’s agenda. It was developed having as objective the solution of a quite common problem elder people have to face, memory loss.

The iGenda works in two fronts, the event scheduling and free time managing. The event scheduling consists in the reception of new events and, using conflict resolution systems, tries to schedule in the requested space, handling the errors that could outcome from that process. The free time manager is in charge of scheduling leisure activities in the user's agenda, keeping the user occupied and active.

Architecture

The iGenda has three main internal cores: the Agenda Manager, the Conflicts Manager and the Free Time Manager.

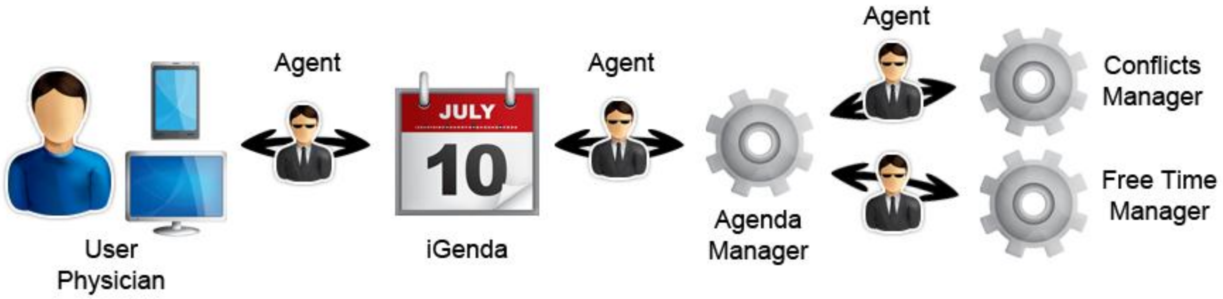

Figure 1: iGenda base architecture

Agenda Manager

The Agenda Manager (AM) serves as the first portal of the system. It is the messages receiver, security manager and the tasks distributer. The messages received have a security signature that should comply with an encryption key generated to each user, creating a security layer that only lets the proper receiver decrypt the message and get its content. It serves also as the task manager, this means that accordingly to the message received, new event or direct chat, it sends the data to the right agent, serving also as the activator of the Free Time Manager.

The AM also serves as a failsafe system that keeps the working agents hidden and serves as a strong gateway - by not interacting directly with the user data and calendar it protects the rest of the system (Gawinecki & Frackowiak, 2008; Moreno, Valls, & Viejo, 2006). The AM has a database with all the users that are authorized to connect with the user, and serving as a protective door to possible intrusions. Also the AM keeps track of all the connections through a log system that records all the incoming and outgoing communications.

Conflicts Manager

The Conflicts Manager is responsible for the incoming events. It uses a logical inference process to make decisions. There are several approaches to select and to sort the scheduled events. In our project it follows a string of processes; first it uses a classification system that uses numeric values to classify the importance of the event; secondly the system verifies if there is space to fit the new event.

The system follows an intricate process. The received events follow a hierarchic scheme that is based on user reputation. The user that schedules an event is verified in a database related to the receiving person and it is retrieved the classification of the said user is retrieved. Then a priority value is set accordingly to the classification of the user in the hierarchical ranking. The scheduler user can set a priority value for the event, and this value will paramount the value given by the system.

For instance: If the user’s personal doctor is making an appointment than the event is treated has a "Priority 1” event, if the physician declares that is a low priority event the value steps down to 2. If it is a friend of the user then the event reaches a maximum of 4 in priority value, depending on the friend’s ranking in the system.

The person that schedules a new event can set a value of importance to the event, but the system will verify what the base value is attributed to that specific user. Medical and similar services have the highest rankings, playful activities the lowest and everything else floats in the middle.

Free Time Manager

The iGenda project is built on a concept of helping others in terms of the user's collection of events and activities. This is achieved at the expense of methods that automate the receipt of events and its addition to a calendar assigned to each user. The Free Time Manager (FTM) will provide the user with leisure activities in the available time. This keeps the user active and connects him with other persons and helps providing the social integration that home isolation usually denies.

A database will contain several different activities that the user enjoys performing, either solo or multiple user activities involving other persons. FTM will be scanning all the free space the user has in his calendar and, using linear distribution functions, scheduling an activity on that space. If the activity involves other persons the system will connect with the other user's iGenda system in order to schedule the activity.

Minding the fact that the activities of the FTM are fairly low in terms of priority and are merely suggestive, it is the user decision to perform them or not. The decision will be captured in real time or be collected through a regular questionnaire allowing the user to avail the efficiency of the system. The results will be collected and used by the system, allowing changing the priority value of activities and fine tuning the system so it gets more adapted to the user.

The functions used to suggest activities to the empty space are linear but they introduce a random variable to the equation, thus the same activity may not always be chosen. Clearly the most preferred activity will more often be chosen, but other available activities will also sometimes be chosen in order to keep a balanced activities chart and to break monotony and repetition.

Connectivity and Interfaces

The typical use will be done through a mobile device that should always be carried by the user. This device gives access to all the information made available by the server, while it also provides valuable information captured by the sensors present in this mobile device, such as GPS tracking. The project is also capable of connecting with the user relatives, and scheduling new events with them or letting the relatives view the user calendar, so they can avail it if the events scheduled are the most appropriate. These connections are transparent and provide full access to the user calendar and notes of the events.

The interfaces available to the users are as simple as possible and were constructed minding the most current user usability guides (Wu et al., 2005), building a streamlined and user friendly interface. The fact is that the less complicated interface will be the most adopted. In case of the Personal Computer (PC) the user will have a window that keeps tabs of the news and recent agenda activities, having a specific window to send a message with specific fields. The mobile system is also alike the PC in terms of functionality but in this case by using the Android platform, the interface is streamlined to be like the common interfaces of the system, so the user that is already familiar to the platform can easily operate with the iGenda interface. The display of the calendar itself is left to the operating system. As the chosen formats of the calendar are universal, every operating system has tools to visualize them, and there are also several different and well-built applications that provide good calendar visualization. In our opinion it is best to let the operating system display the calendar with his tools, and this for main two reasons: compatibility and familiarity. Compatibility towards the portage of several applications to different operating systems, and the current familiarity that the user could have towards an application he already uses.

The modules are basically very advanced agents so their communication is done by network (LAN, WiFi, 3G), and because of their characteristics they can be executed and be present in different servers or even in different countries. The same happens to the iGenda Interface Clients, being provided with data connection the iGenda platform can synchronize automatically with the Agenda Manager, receiving updates of the calendar or being available to send messages in real time.

Sensing Module

Upon the creation of the iGenda it was realized that different modules could be connected to it, gaining the function of automatic and intelligent scheduling. This was the case of the Sensing Module (SM). The SM is a standalone module that has as objective a mobile monitoring of a user (Carneiro, Novais, R. Costa, Gomes, & José Neves, 2009; E. Corchado, Arroyo, & Tricio, 2010; DeLong, 2003; Triantafyllidis, Koutkias, Chouvarda, & Maglaveras, 2008). This can be achieved by providing the user with body sensors that collect vital data, remotely processing the data and presenting to physician information of the health condition of the user. The sensors collect data as electrocardiogram, blood pressure, oximmetry and fall detection (abrupt G-Sensor modifications) among others, the data is then processed to collect viable information about the overall health status. This data is then sent to the user physician for further analysis. This liberates both the hospital and the user without losing the constant monitoring that hospitals currently provide. The physician becomes also more available to other emergency cases, reading the daily reports and taking decisions upon their content.

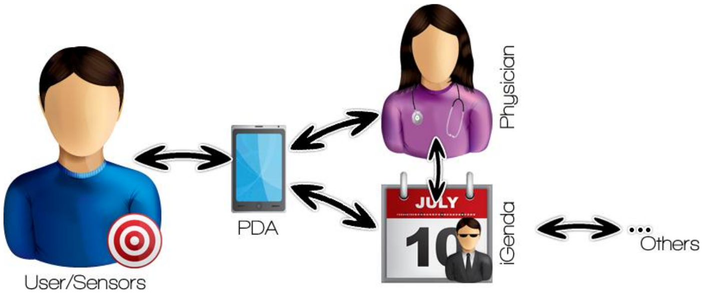

Figure 2: Sensing Module information pathway

In this scenario the integration of the iGenda is obvious, maintaining the connection user-physician. If, upon a daily report, the physician takes a decision to call in the user for a personal appointment all he has to do is to open the iGenda and to schedule an appointment when he has available time. That event will be automatically scheduled in the user calendar and the user will be notified. The same is true to the user, but instead the physician will receive a notification that the user is trying to schedule an appointment, leaving to the physician the decision and an appropriate reply.

Also the current processing system is able to perform small proactive decisions, based on standard health conditions, such as sustained drop of the user health condition. In these cases the Sensing Module can effectively ask the iGenda to schedule a high importance event in both the user and physician agenda.

The Sensing Module is able to point out to the sustained condition and to factors that may not be noticed in a normal routine scan, thus creating an efficient pre-emptive system. Also because of the nature of the sensors, the sensing system and the iGenda would run from the same portable device, creating a strong synergy between them.

Privacy and Data Protection Threats

This type of projects rely on a heavy use of personal and private data, and because of its nature the data and information collected has to pass through several methods of scrutiny provided by various specialists in order to make the system more reliable. Also the social components require that the information is visible to other users, like a social network, adding to the fact that, if required, full access will be granted to the user relatives or care takers that have the responsibility towards the user.

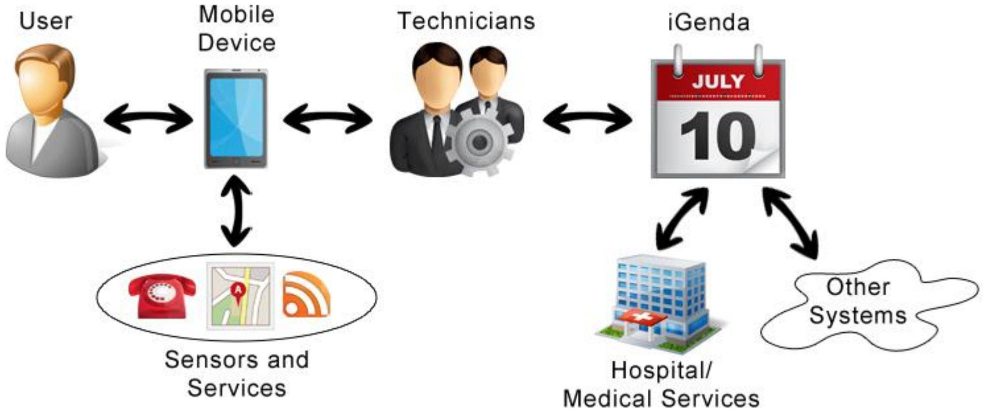

Figure 3: Data Flow schema

Data Collecting Modules

The iGenda has several modules that comprise the use of several different sensors and devices that read and process personal information related to the user. As it was mentioned before, the GPS module can give real-time access to the position of the user. The Sensing Module collects data from sensors attached on the user's body. The data is, in an early stage, processed and analyzed using logically defined medical guidelines. These guidelines support decision flow that is translated to an early stage medical diagnosis. In case of an immediate problem or emergency the system notifies the Emergency Services, giving them the location of the user and the immediate data collected.

The overall data collected by the sensors is transferred to the main server so that it can be processed and from it created a clinical map of the health condition of the user. The map is archived and if needed sent to the user's personal physician, so that he can analyze thoroughly the case.

Using the overall health map the system can identify eventual problems and automatically schedule an appointment in the user and physician agendas, notifying them immediately.

Profiles

In terms of adjusting to user needs, it was built a personalization platform that saves the user profile and the choices it made over time. These profiles contain private and personal data of the users, data that even his relatives know nothing about. The data is used to create a database of preferences and automations, thus creating a pattern model iGenda can easily use to suggest decisions. The data collected is reviewed by a technician (subject to secrecy obligation) that will insert them in the model, giving heights and linking data so that it can be more effective. Also the profiles store the typical medical condition of the user, providing an easy access to the Sensing System so the proactive activity can be effective (Robinson et al., 2010).

The profiling system collects several sensitive raw data. The process of transforming it into viable information takes several stages and different persons, analyzing content and providing meaning and importance to data.

This association between data and information is not totally reliable. These operations can sometimes induce the system in error, therefore creating unforeseen outcomes. To correct this situation technicians have to review again all the information and, if necessary with the help of the user, provide the correct meaning.

A learning system will also collect over time the choices and activities the user made. The system will operate silently learning what the user does and what are his chosen activities, in order to effectively change the weights involved in the decision algorithms.

Data Sharing

The data will go through several technicians in order to be reviewed and inserted. The authorized personnel are vast and any technician can proceed to the needed technical operations.

Data sharing is also supported by clinical data. The clinical status and health records could be shared between different medical organizations or projects with modules associated with the iGenda. Data such as the health electronic records can be shared to projects such as VirtualECare (R. Costa et al., 2009; Novais, Â. Costa, & R. Costa, 2010) and distributed to various hospitals or medical centers.

In terms of other persons the data will be shared by the various elements of family and friends. People who have previously been authorized, having different stages of access, to view the data will have the ability to add new events, manipulating existing events or view events that the user considers private.

Data must be sent from the devices where it is collected, to iGenda. The data will have to go through processes of reception and transmission, supported by communication systems such as GSM, UMTS and WiFi, among others; this implies that a third party, the mobile service provider will also have access to the information in the transaction.

For proper operation of the system, it is necessary to store all information received; this means that all data will be stored permanently in digital format on a hard drive.

Such systems provided a loss of privacy and access to sensitive information on a daily basis.

Summarizing, this project provides assistance to the user through an array of different services that treat different actions. Centered on the user this project cannot work only by a generic system. Every user has different disabilities and characteristics that the system has to attend to. The feature that is personalization is what differ the iGenda from the rest of the projects. The right response to the problem, accounting the user profile is very different from the one-for-all solutions. Thus this project requires that each product is adapted to each user, requiring that personal information about the user is used to feed the system. Also it is the private and sensitive information that most changes the system to adapt to the user, adding the information that is generated by the system internally. This exchange and creation of information can generate a precedent about how the information is used and who has access to it. It raises much questions about the technical and legal safeguard about the information flowing in the system and how the final user is legally protected.

TECHNICAL AND LEGAL SAFEGUARDS

This application manages user vital and private information and makes them available to other persons, tracking also the current position of the user. As it is, this project enables the loss of privacy on a daily basis. And it is important to consider what spheres of personality will be affected: German jurisprudence considers that beyond a sphere of publicity, it must also be considered a personal, a private and an intimate sphere (Farinho, 2006). The right to privacy was expressly acknowledge in article 8 of the European Convention on Human Rights and, later on, on article 7 of the Charter of the Fundamental Rights of the European Union, and it is intended to protect individuals against intrusions by public authorities or by other individuals (Rouvroy, 2008). But besides privacy issues, also data protection is at stake, since Article 8 of the Charter of the Fundamental Rights of the European Union raised the protection of personal data to the status of a Fundamental Right (Miguel, 2004; Rouvroy, 2008). These two different subjects, Privacy and Data Protection, while almost always connected by legal doctrine, may indeed require some different approaches. For instance, privacy rights may imply a "prohibition against surveillance in certain spaces or situations (e.g., in bathrooms)" (Hert, Gutwirth, Moscibroda, Wright, & González Fuster, 2008), while data protection rights may imply restrictions on the collection and processing of data (Castro, 2005).

The core question is what kind of legal obligations and legal protection can arise from the previous described situation. The issue is particularly delicate, as it involves the collection, storage and transmission of health and personal data, which is considered by European Law as "sensitive data". In this regard it is important to look at the Legal Framework and try to understand if there are exceptions to the consideration of sensitive data and whether or not the perception of sensitive data is somewhat context dependent. The incidence of issues like the distribution of raw data, the necessary surveillance (cameras, sensors) and profiling systems can become an open door to the users' privacy and personal data. Moreover not only the data collected is important but also the knowledge generated from it. Nowadays, the knowledge is a serious matter; since it relates all the information and provides it with context, giving a meaning to unassociated events. Also, we may have different attitudes towards the system and its use: while the user has to be totally honest, he does not receive any type of feedback by the system.

Privacy

The right to intimacy and private life is a right related to the personality (Castro, 2005). It is a right under which every person decides on his own what and when must be shared with third persons, allowing the individual to control his own life and experiences, in the spheres where it is not admitted an intromission of the State or of third persons (Janeiro, 2002). It relates very closely to freedom, to the construction of one's identity and to the control one has over "aspects of the identity one projects to the world". In the Portuguese Legal System this right to privacy is expressly recognized by article 26 nr. 1 of the Constitution of the Portuguese Republic and by article 70 of the Portuguese Civil Code.

Privacy is currently under threat, due to technological developments: increased possibilities of surveillance, specially RFIDs and other technologies making it possible "to follow whatever we do and wherever we go", that is to say, constant observation and monitoring, through the establishment of links between persons and objects, leading to "the tracking of people" once the link is established (Hert et al., 2008). To this, it must be added the possibilities of data mining and profiling, the use of sensors monitoring aspects like "blood pressure, body temperature, heart rate and facial expression throughout the day", with the ultimate possibility of constant observation of “choices, behaviors and emotions”, making people “decreasingly capable of living by their fully autonomous choices and behaviors” (Rouvroy & Poullet, 2009). Furthermore, this increased possibility of surveillance brings along a blurring on the distinction between what is public and what is private and the danger of “dataveillance”. Currently, there is a strong urge in defending intimacy and private life through an insurance of confidentiality, enhancing two different aspects of intimacy:

a negative aspect of intimacy, excluding a knowledge by third parties of what is own to the self;

a positive aspect of intimacy, meaning a control of the individual on the information relating to himself (Domingo Bello Janeiro 2002)

It is this second aspect of intimacy that makes visible the strong link existing between Privacy and Personal Data. Anyway, privacy is particularly related to a need to impeach, through law and through technology, the collection and the dissemination of information about an individual, especially thinking of what it may be called PET or Privacy-Enhancing Technologies (Hert et al., 2008).

Personal Data

By Personal Data we mean any data relating to a single (identified or identifiable) person, considered to be the holder of the data (Castro, 2005). Health Data are referred to as data including information relating to all aspects, physical and psychological, relevant to the health of a person, as it was stated by the Court of Justice of European Union in an interpretation of art. 8 nr. 1 of Directive 95/46/CE (process C-101/01, decided on the 6th November 2003). Being this kind of data considered as sensitive data, according to European and Portuguese Law (art. 7 of Law 67/98), and thus being its treatment is, in principle, not allowed, unless the holder of data consents and security measures are ensured, namely the logical separation between health data and other personal data (art. 15 nr. 3 of Law 67/98).

There is a general prohibition under Portuguese law of treating personal data. The Constitution of the Portuguese Republic, in article 35, expressly forbids the use of informatics for treating data relating to private life. Portuguese Law 67/98, according to European Directive 95/46/CE, extended this prohibition in order to include, as sensitive data whose treatment is prohibited, data referring to private life, health, sexual life and genetics.

Yet, one obvious exception to this prohibition must be referred: that is when the holder of the data expressly consents (art. 7 nr. 2 Law 67/98), through a free, specific and informed manifestation of will (art. 3 h) Law 67/98.

Anyway, although justifiable as it might be, the treatment of health data requires free and express consent of the holder of the data, upon a free, informed and specific manifestation of will. This implies recognition of an information principle, that is to say, the holder has the right to know exactly what data about him/her is contained in the file. And the requirements of consent will not be fulfilled whenever this is obtained through the indication of a vague and generic finality. But it also contemplates a right of control, in the sense that the holder has the right to cancel or rectify data. Furthermore, as a principle of loyalty, data must remain accurate and must be used according to the finality that was invoked for its collection, in a secure and confidential way (Miguel, 2004). And whenever the finality is somewhat changed, a new consent must be obtained (Castro, 2005).

This requirement of a free and express consent must always be in connection with the main principles recognised by law doctrine for the allowance of treatment of personal data: first of all, we must refer a general principle of transparency, that is to say that the person responsible for the treatment of data has to be clearly identified and he also must clearly inform the holder of the data (to be treated), of the finalities and delays of its treatment and conservation, of its communication to third parties. Moreover, this principle of transparency clearly implies a right to information and to access to data (that must be assured to the holder) and, whenever required, registration, authorization, or notification to the National Data Protection Commission (Castro, 2005). Also relevant, must be the conformity with a principle of finality. This is to say that data can only be used according to the finality that was considered for its collection. And this finality must be determined, explicit, legitimate (not contrary to the Law). The precise aims of the data treatment must be indicated and data cannot be used in a way contrary to the said finality. Having all this in consideration, consent must be unambiguous and informed (Hert et al., 2008). Anyway, it must be stressed that data protection principles must always apply and thus "the individual should always be informed of the presence of tags and readers, the purposes for which data are collected and processed, who is the responsible controller, whether the data (and what kind of data) are stored, the means to access and to rectify data, and whether the data will be made available to third parties" (Hert et al., 2008).

But the consideration of this finality principle must not be dissociated from another quite relevant requirement of data treatment and processing: the collected data must be necessary and adequate to the said finality and the treatment and processing of data must not exceed what is really needed in order to the fulfillment of its aims. That is to say, there must be proportionality between the collected data and the finality that was intended with its collection (Castro, 2005). On the other side, it must be recognized that the criteria to appreciate the need of collection of data must be objective, according to the finalities expressed (Castro, 2005).

It must not be forgotten here the legally appointed rights of the holder of the data: first of all, the right to oblivion or right to be let alone (Castro, 2005): data must only be kept during the necessary delay according to the finalities of collection and treatment (art. 5 nr. 1 e) Law 67/98). It is understood that only the establishment of a due delay for the conservation of data may prevent a "perpetual appropriation of quite broad aspects of personal life" (la Cueva & Lucas, 1993). To this extent, some authors speak of a need for informative auto determination (Castro, 2005) or even to a Right to Informational self-determination (Rouvroy & Poullet, 2009). For this to be considered, it is obvious required not only a right of access of the holder to the data (a right to look at, that needs not to be justified), but mainly the rights of rectification and actualization of data and, for the fulfillment of a control by the holder, the right to an accuracy of data within the fixed delays. That is to say, the holder of the data must be able to verify that data concerning his/her person is accurate or not – in case it is not, he has a right to the rectification and actualization of the data. On the other hand, it must not be forgotten that data must not be conserved beyond the necessary or fixed delay. If data is inaccurate or is conserved beyond the delay, the holder of data shall have a right to have data erased or, at least, its access blocked (Castro, 2005).

An exception to the requirement of free and informed consent of the holder of the data will occur whenever he/she is temporarily unable to consent – by being in coma or unconscious – and yet the treatment of personal data is mandatory in order to protect vital interest of the holder of data (art. 7 nr. 3 a) of Law 67/98). This would be the case in situations of monitoring persons in coma or in intensive care units (Castro, 2005).

Relevant exception to the prohibition of treatment of health data is the one of art. 7 nr. 4 of Law 67/98. According to this, the treatment of health data (although sensitive) may be admitted whenever necessary in terms of preventive care, medical diagnosis, medical care and medical treatment, provided that these are assured by a doctor or health care professional obliged to secrecy, and that the National Commission of Data Protection (CNPD) is notified and warranties for the security of information are ensured (Castro, 2005). The Portuguese National Commission of Data Protection has already stated that telemedicine operations are to be considered as treatment of data for the purposes of art. 7 nr. 4 (Authorization nr. 73/2000, published in 2000 by CNPD), and this recognition certainly keeps an open window on the development of telemedicine facilities, provided that the above referred requirements are respected. Anyway, this treatment of health data will only be possible whenever it is done by a health care professional or other person under obligation of secrecy. And data relating to health, sexual life, and even genetic data are required to be logically separated from other personal data, according to Law 67/98, article 15 nr. 3 (Castro, 2005).

Yet, even considering that the collection and treatment of such data may be not only admissible but even beneficial for the holder of the data, it must not forgotten the need to comply with some fundamental principles in the domain of personal data treatment, specially the one concerning to the finality of data collection and treatment: the finality must be known in advance, must be legal and legitimate, and the use of the data must comply with this finality (Castro, 2005).

Some difficulties could arise out of the fundamental rights of the holder of the data, specially the right to oblivion or right to be let alone, meaning that data must be kept only while it is necessary for the purposes of collection and treatment. In Portugal, the National Commission of Data Protection (CNPD) will determine the delay of use of the data according to the finalities of the treatment. After the course of the delay, the data must be deleted, thus being ensured the right to oblivion of the holder of the data (although CNPD might allow keeping data for statistical or scientific purposes) (Castro, 2005). Another relevant right of the holder of data that must be referred is to have the data deleted or its access blocked whenever data are no longer accurate or are kept beyond the fixed delay (art. 5 nr. 1 c) and art. 11 nr. 1 d) Law 67/98. Furthermore, it must always be kept in mind that the holder of the data "should always be informed of the presence of tags and readers, the purposes for which the data are collected and processed, who is the responsible controller, whether the data (and what kind of data) are stored, the means to access and rectify data, and whether the data will be made available to third parties" (Hert et al., 2008).

As a summary, we may emphasize that Directive 95/46/EC specifies important requirements relating to the quality of data, emphasizing that 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;
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 data were collected or for which they are further processed;

In Data Protection the main concern is with the control each individual may (or may not) have on its own data, through law and technology, especially through the so-called transparency-enhancing technologies (Hert et al., 2008). In this sense it is of the utmost importance a right that has been lately referred to by some legal doctrine, having in mind the fulfillment of the premises of informational self-determination: the right every individual has not to be subject to automatic individual decisions taken by application systems only (Castro, 2005).

The specifications and legal concerns are presented due to the obligation to regulate the data protection and transmission of personal data across the several services of the iGenda. The fact is that personal oriented systems that use sensitive information about the user must not be overlooked due to legal matters, personal protection and human rights. Thus the need to protect and secure the user data that flows in the system is crucial, as previously mentioned, so that the user may benefit of the services provided but being protected at the same time.

CONCLUSION AND CHALLENGES

As the population ageing paradigm shifts to another stance, aged population the persons tends to require more assistance and services that provide the proper response to their problems. The fact is that it is very difficult to provide human care services to all population, leaving the space to implement services and solutions that can assist users of the said solutions in their daily routine and activities, through an array of different and distinctive applications in different fields, such as the user home or even a hospital. To respond accordingly to the user needs the applications are heavily based upon user’s personal information, to create a digital profile, containing several aspects and information to provide the system with knowledge and with the necessary proactivity towards events and activities the user is or will be preforming.

Health Care Services currently require that personal and sensible data are shared between several persons and in some systems the information is also available to other users and relatives. Under Portuguese legal system, the treatment of health data (although sensitive) may be admitted whenever necessary in terms of preventive care, medical diagnosis, medical care and medical treatment, provided that these are assured by a doctor or health care professional obliged to secrecy. Thus being, telemedicine operations are to be considered and this recognition keeps an open window on the development of telemedicine facilities, provided that legal requirements are respected. Profiling and monitoring may thus become legal, but it is important to have always a look at the rights of the holder of the data in a perspective of informational self-determination. It must be absolutely required a total cooperation and participation of the user, with the only exceptions of situations in which the holder of the data is not able to consent (by being unconscious or in comma) and the treatment of personal data is mandatory in order to protect vital interest of the holder of data.

Even considering the need for a compliance of the systems with the above referred rights and warranties of the holder of data, it is important not to forget the risks of what is now called “dataveillance” (Clarke 1988) “the massive collection, aggregation and algorithmic analysis of data on everyone and everything” and of profiling, allowing the gathering of data and construction of knowledge about citizen-consumers in order to achieve certain purposes (Hert et al., 2008). It is furthermore necessary to distinguish between privacy and data protection issues, between what (Hert et al., 2008) call opacity and transparency tools. Thus being, it is important to understand that law requires enforcement and a major role may be played on this issue by technology itself – for this, there is a need of both privacy-enhancing technologies and transparency-enhancing technologies (Hert et al., 2008). On this issue, it might be interesting to consider that while technology certainly brings along many threats to privacy and data protection, it may also be questioned whether or not technology should be itself considered as part of the solution for enhancing privacy and data protection regulations. As Jane Winn puts it "Just as technical standards make networked communications possible, increasing the risk that data may be processed without regard to the requirements of data protection law, they may also lower the cost of compliance with data protection laws and increase access to privacy-enhancing technologies" (Winn, 2009). In this sense, it is certainly wise to approach the newest threats to human rights of privacy and data protection through a clear distinction between the different but complementary roles that both Law and Technology have to play in this context.

REFERENCES

Adam, T., & Evans, D. B. (2006). Determinants of variation in the cost of inpatient stays versus outpatient visits in hospitals: a multi-country analysis. Social science medicine, 63(7), 1700-1710.

Baltussen, R., Adams, T., Torres, T. T., Hutubessy, R., Acharya, A., Evans, D., & Murray, C. (2003). Making Choices in Health: WHO Guide to Cost-Effectiveness Analysis (p. 312). World Health Organisation (WHO).

Carneiro, D., Novais, P., Costa, R., Gomes, P., & Neves, José. (2009). EMon: Embodied Monitorization. Proceedings of the European Conference on Ambient Intelligence, 133-142. Springer-Verlag. doi:10.1007/978-3-642-05408-2_17

Castro, C. S. e. (2005). Direito da Informática, Privacidade e Dados Pessoais (p. 374). Edições Almedina.

Charness, N. (2008). Aging and Human Performance. Human Factors The Journal of the Human Factors and Ergonomics Society, 50(3), 548-555. Human Factors and Ergonomics Society. doi:10.1518/001872008X312161

Chisholm, D., & Evans, D. B. (2007). Economic evaluation in health: saving money or improving care? Journal of Medical Economics, 10(3), 325-337. doi:10.3111/13696990701605235

Corchado, E., Arroyo, A., & Tricio, V. (2010). Soft computing models to identify typical meteorological days. Logic Journal of IGPL, 19(2), 373-383. doi:10.1093/jigpal/jzq035

Costa, R., Novais, P., Lima, L., Carneiro, D., Samico, D., Oliveira, J., Machado, J., et al. (2009). VirtualECare: Intelligent Assisted Living. Electronic Healthcare First International Conference Ehealth 2008 London September 89 2008 Revised Selected Papers (p. 138). Springer. Retrieved from http://www.springerlink.com/index/q72k12653361lk83.pdf

Costa, Â., & Novais, P. (2011). An Intelligent Multi-Agent Memory Assistant. In L. Bos, L. Goldschmidt, G. Verhenneman, & K. Yogesan (Eds.), Handbook of Digital Homecare - Successes and Failures (1st ed., pp. 197-221). Springer. Retrieved from http://www.springerlink.com/content/xv07367n45354013/

Costa, Â., Novais, P., Corchado, J. M., & Neves, José. (2011). Increased performance and better patient attendance in an hospital with the use of smart agendas. Logic Journal of IGPL. doi:10.1093/jigpal/jzr021

la Cueva, M. D., & Lucas, P. (1993). Informática e protección de datos personales. Centro de Estudios Constitucionales.

DeLong, R. P. (2003). Interoperability & Sensor Fusion. Naval Engineers Journal, 115(2), 89-104. doi:10.1111/j.1559-3584.2003.tb00207.x

Farinho, D. M. S. (2006). Intimidade da Vida Privada e Media no Ciberespaço (p. 108). Almedina.

Gawinecki, M., & Frackowiak, G. (2008). Multi-Agent Systems with JADE: A Guide with Extensive Study. IEEE Distributed Systems Online, 9(3), 4-4. doi:10.1109/MDSO.2008.9

Geda, Y. E., Roberts, R. O., Knopman, D. S., Petersen, R. C., Christianson, T. J. H., Pankratz, V. S., Smith, G. E., et al. (2008). Prevalence of neuropsychiatric symptoms in mild cognitive impairment and normal cognitive aging: population-based study. Archives of General Psychiatry, 65(10), 1193-1198. Retrieved from http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2575648&tool=pmcentrez&rendertype=abstract

Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., & González Fuster, G. (2008). Legal safeguards for privacy and data protection in ambient intelligence. Personal and Ubiquitous Computing, 13(6), 435-444. doi:10.1007/s00779-008-0211-6

Hodges, S., Williams, L., Berry, E., Izadi, S., Srinivasan, J., Bulter, A., Smyth, G., et al. (2006). SenseCam: a retrospective memory aid. UbiComp 2006 Ubiquitous Computing (Vol. 4206, pp. 177 - 193). Springer Verlag. Retrieved from http://eprints.soton.ac.uk/55428/

Janeiro, D. B. (2002). La protección de datos de carácter personal en el derecho comunitario. Anuario da Facultade de Dereito da Universidade da Coruña, 133-156.

Jiang, J., Geven, A., & Zhang, S. (2009). HERMES: A FP7 Funded Project towards Computer-Aided Memory Management Via Intelligent Computations. 3rd Symposium of Ubiquitous Computing and Ambient Intelligence 2008 (pp. 249–253). Springer. Retrieved from http://www.springerlink.com/index/t6u276605n5h6v1h.pdf

Miguel, C. R. (2004). El Derecho a la Protección de los Datos Personales en la Carta de Derechos Fundamentales de la Unión Europea. Temas de direito da informática e da internet (pp. 17-71). Coimbra Editora. Retrieved from http://books.google.com/books?id=ZYxyPgAACAAJ

Moreno, A., Valls, A., & Viejo, A. (2006). Using JADE-LEAP to implement agents in mobile devices. Development. Retrieved from http://jade.tilab.com/papers/EXP/02Moreno.pdf

Nations, U. (2009). World Population Ageing. Population English Edition, 7(4), 750. doi:10.2307/1524882

Nehmer, J., Becker, M., Karshmer, A., & Lamm, R. (2006). Living assistance systems: an ambient intelligence approach. Proceedings of the 28th international conference on Software engineering, 43-50. ACM. doi:10.1145/1134285.1134293

Nice. (2011). Supporting people with dementia and their carers in health and social care. Dementia, 2006(March), 1-56. National Institute for Clinical Excellence. Retrieved from http://www.nice.org.uk/nicemedia/live/10998/30318/30318.pdf

Novais, P., Costa, Â., & Costa, R. (2010). Collaborative Group Support in E-Health. 9th IEEE/ACIS International, 177-182. Yamagata, Japan. doi:10.1109/ICIS.2010.105

Robinson, L., Bamford, C., Beyer, F., Clark, A., Dickinson, C., Emmet, C., Exley, C., et al. (2010). Patient preferences for future care - how can Advance Care Planning become embedded into dementia care: a study protocol. BMC Geriatrics, 10, 2. BioMed Central. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/20067613

Rouvroy, A. (2008). Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence. Studies in Ethics Law and Technology, 2(1), Article 3. doi:10.2202/1941-6008.1001

Rouvroy, A., & Poullet, Y. (2009). The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In S. Gutwirth, Y. Poullet, P. Hert, C. Terwangne, & S. Nouwt (Eds.), Reinventing Data Protection? (pp. 45-76). Springer Netherlands. Retrieved from http://dx.doi.org/10.1007/978-1-4020-9498-9_2

Rubel, P., Fayn, J., Simon-Chautemps, L., Atoui, H., Ohlsson, M., Telisson, D., Adami, S., et al. (2004). New paradigms in telemedicine: ambient intelligence, wearable, pervasive and personalized. Studies In Health Technology And Informatics, 108(pp 123-132), 123-132. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/15718638

TimesTeam. (2010). Inpatient and Outpatients Waiting Lists.

Triantafyllidis, A., Koutkias, V., Chouvarda, I., & Maglaveras, N. (2008). An open and reconfigurable wireless sensor network for pervasive health monitoring. Methods of Information in Medicine, 47(3), 229-234. IEEE. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/18473089

Tucker, G. (1995). Age-Associated Memory Loss: Prevalence and Implications. Journal Watch Psychiatry.

Winn, J. K. (2009). Reinventing Data Protection? (S. Gutwirth, Y. Poullet, P. Hert, C. Terwangne, & S. Nouwt, Eds.) (pp. 191-206). Dordrecht: Springer Netherlands. doi:10.1007/978-1-4020-9498-9