Preface

INTRODUCTION

There is one particular wall posting on my Facebook account which always seems to make me stop and daydream. It is a post from my Friend Debbie, or should I say, it is actually her automatic Nike application which ‘posts’ telling me when she is starting her run and when she has finished (Figure 1). All her friends can then monitor her times and actual distance run. We also have the option of sending her messages as she runs....as if...

Anyhow, I am aware of course for years about such devices/gadgets/GPS apps from the fitness world - but it is the integration of this particular application which always makes me think of futuristic scenarios when we can tag other everyday chores and actions around the house. What if the vacuum cleaner has a network connection and broadcasts to the world whenever we clean “Kevin Curran has started to vacuum the kitchen......Kevin Curran has started in the hallway.....Kevin Curran has emptied the vacuum cleaner....” or “Kevin Curran has filled the cats dish”...Kevin Curran has broken the vase......Kevin Curran has finally taken a bath”....OK, we get the message. I guess what I wanted to bring into this piece is that data - even innocuous data such as this - even if we do not post it to social networking sites might actually be beneficial. I mean what would you call embedding a sensor in everyday objects? It really is a form of embedded business intelligence. Now, that term is overloaded in many ways, but such embedded broadcasting of activity could - if the right analytical tools/processes are applied - perhaps lead to addressing any inefficiencies in our life. Perhaps such data mining might really discover
that we run our lives inefficiently. By embedding activity monitoring into our everyday objects….perhaps we can indeed enrich our everyday lives.

There are some basic functions of Ambient Intelligence, one of which is context awareness. This is where the sensors are placed into the environment. They then communicate and help to identify movements and actions. For instance, audio, video, and data can be transferred wirelessly to devices within an Ambient Intelligent system, therefore enabling access to information and entertainment wirelessly. Finally, by doing everyday things such as talking, moving, and gestures, the users of an Ambient Intelligent environment can interact with their surroundings. By doing these daily activities, they are enabling a hands free type of interactivity with the surrounding environment (Aarts and Marzano, 2003).

The key to delivering ambient intelligence to users is being able to provide what is wanted, when, where, and how it is wanted. All aspects are important so that the user receives the right information, at the right time, and in the right way so that the person can make use of the information. Ambient Intelligence also can cater for those people who may have a disability such as the requirement of a hearing aid. However, user control is voluntary so they can decide what information they want and whether or not they want to receive it at any point (Basten et al., 2003).

Devices face temporary and unannounced loss of network connectivity when they move from one cell to another and are frequently required to react to changes in the environment, such as a change in context or a new location. The concepts of context and context-awareness have been central issues in Ambient Intelligent research for the last decade (Oh et al., 2007). Context-awareness has emerged as an important idea for achieving automatic behaviours in pervasive and predictive systems. For example, a system that senses a user’s condition, location, or physical actions and adapts to maximise user convenience is utilising context awareness. Initial research began by looking at context-aware systems more generally and independently of specific applications, including context middleware and toolkits from Dey et al. (1999). Everyday objects are being enhanced with sensing, processing, and communication abilities, and as a result, our everyday living is moving towards a higher degree of complexity. There is a need for context-aware Ambient Systems to continuously and implicitly adapt the environment to meet evolving user expectations. Up-to-date valid context information is the key requirement for successful transparent interaction. Methods of representing context awareness, context modeling, and acquisition techniques are of critical importance in the development of Context-Aware Ambient Systems. In fact, semantic technologies represent a very promising approach to solving many problems in ambient applications.

**AMBIENT INTELLIGENCE AND TECHNOLOGY IN TODAY’S WORLD**

Ubiquitous multimedia computing has awakened the passions of many of the research labs of the world due in part to the flourishing of wireless communication infrastructures such as 3G, WiMax, LTE, and RFID. So it was with great interest that I came across the article *Trends in Ubiquitous Multimedia Computing* (Lee and Chen, 2009). The focus of their research was to sift through surveys on various ubiquitous multimedia computing related topics in order to trace the latest development in this particular field. Factor Analysis, PFNeT, and context-based ontology were used (which is similar to Author Co-citation Analysis (ACA)). So in the resultant top 10 research trends in the UMC field by factor analysis, they found that #5 was *Context-aware workflow language based on Web services* and #6 was *Ambient intelligent systems*. (It may be worth noting that instead of searching all the papers in the citation index database, they limited the search to literature published in the citation data from ISI web in 2008. The
initial citation graph contained 15,708 document nodes and 17,292 citation arcs, and they removed papers with less than 3 citations so the graph was eventually built from 1,506 papers.

The Context Aware trends in UMC that were discovered were m-health, which includes health information systems, clinical bioinformatics, ubiquitous computing in health care, clinical decision support, patient access medical records, smart house for older persons, and more. Other context aware areas included context-awareness applications, context-aware computing technology in intelligent decision-making, context-aware product bundling architecture, context-aware comparative shopping, context-management services, context-aware adaptive information system, context aware proactive service, and context-aware migratory service.

The reason I highlight the areas above is because I believe context awareness and ambient intelligence will move up the top 10 trends chart should this exercise be repeated year on year. In fact, it is obvious just from this issue alone, the importance of context in our ambient intelligent platforms. As we are aware, “Context refers to the conditions in which something exists or occurs,” and what better area of computer science to address this than the world of ambient intelligence?

While still talking about context: jokes rely on context. There are gags that a comedian would never tell on TV but go down as a treat on stage to live audiences. Also, the jokes you share with your friends on the bus may not be appreciated as much in front of the church on a Sunday morning. Yes, context… In fact, there was a recent attempt quantify the funniest joke ever told. The most interesting outcome was the differences revealed along cultural, age, and gender lines. Men tended to enjoy more aggressive jokes, along with the so-called dirty joke featuring sexual or scatological references, while women preferred clever wordplay or puns. They did reach a compromise with regards the funniest joke ever told and it went like this “A couple of New Jersey hunters are out in the woods when one of them falls to the ground. He doesn’t seem to be breathing; his eyes are rolled back in his head. The other guy whips out his cell phone and calls the emergency services. He gasps to the operator, “My friend is dead! What can I do?” The operator, in a calm soothing voice says, “Just take it easy. I can help. First, let’s make sure he’s dead.” There is a silence, then a shot is heard. The guy’s voice comes back on the line. He says: “OK, now what?”

To be serious again for a moment, ambient, pervasive, and ubiquitous computing are seen as a drastic shift for computing systems. In reality, networked computing resources should become invisible to users and simply provide them with the right services at the right time. Latest evolutions in both the computing and the networking domains have been remarkable. Handheld user devices, such as smartphones, now embed computing resources that make them comparable to desktop computers of the previous decade. Wireless networks become ubiquitous and offer overlapping coverage and alternative attractive features. Sensors become embedded in most user devices but also in any imaginable object of the physical environment. While the above offer a powerful substrate, ambient computing has still a long way to go before becoming truly ad hoc (Georgantas and Issarny, 2010).

The significance that Ambient Intelligence (AmI) has acquired in recent years requires the development of innovative solutions. In this sense, the development of AmI-based systems requires the creation of increasingly complex and flexible applications. The use of context-aware technologies is an essential aspect in these developments in order to perceive stimuli from the context and react upon it autonomously (Alonso et al., 2011).

Another technology which is beginning to have a positive impact in Ambient Intelligence research is Augmented Reality. Augmented Reality (AR) is a technology that provides the user with a real time 3D enhanced perception of a physical environment with addition virtual elements either virtual scenery,
information regarding surroundings, other contextual information, and also capable of hiding or replacing real structures. With Augmented Reality applications becoming more advanced, the ways the technology can be viably used is increasing. Augmented Reality has been used for gaming several times with varying results. AR systems are seen by some as an important part of the ambient intelligence landscape. It is also used to good effect in the domestic, industrial, scientific, medicinal, and military sectors, which may benefit future ambient intelligent systems (Curran et al., 2011).

Future smart environments will be able to observe behavior, and to understand and anticipate it. It has been less emphasized, however, that once this form of ambient intelligence will be achieved, humans will be able to exploit it in new ways: i.e. by performing actions while knowing and expecting that the environment will notice and understand what we are doing. Our behavior - and its physical traces - will thus become a “message,” a “signal” sent to the environment itself in order to obtain collaboration, although remaining a concrete practical action, not symbolic gestures or mimics. The theory of this form of intentional (or functional, non-intended) communication is crucial for the future human-environment interaction (as for human-robot interaction (Castelfranchi et al., 2010).

There is currently a move towards integrating commonsense reasoning and understanding capabilities as the key elements in bridging the gap between idiot savant systems and real Ambient Intelligence systems. Since the appearance of the Ambient Intelligence paradigm, as an evolution of the Ubiquitous Computing, a great deal of the research efforts in this field have been mainly aimed at anticipating user actions and needs, out of a prefixed set. However, Ambient Intelligence is not just constrained to user behaviour pattern matching, but to wisely supervise the whole environment, satisfying those unforeseen requirements or needs, by means of rational decisions (Santofimia et al., 2010).

**AMBIENT INTELLIGENCE AND THE FUTURE**

Recently, some of the media picked up on the story of the Los Angeles-based woman who is claiming damages from Google because she was injured while taking a “safe” route recommended by Google Maps. Yes, you did read that correctly. According to her claim, she sustained injuries and “emotional suffering” from the accident, which occurred after she following directions on her BlackBerry. The Californian woman claimed she used Google Maps to chart an approximately two-mile course in an upscale Utah ski town and Google Maps led her to a four-lane highway without sidewalks that she claims was “not reasonably safe for pedestrians” and “as a direct and proximate cause of... Google’s careless, reckless, and negligent providing of unsafe directions... was led onto a dangerous highway and was thereby stricken by a motor vehicle, causing her to suffer severe permanent physical, emotional and mental injuries...” Let me remind you that this woman is in her twenties. This was not a school kid.

One may believe this is an isolated incident and unlikely to reoccur.....but is it? In other words, are we as developers/architects of automated systems to think of every potential misuse of our systems in the future by people (however stupid they may appear)? The first thing that comes to mind after this incident is that the end-user license agreement (EULA) for any location determination technologies will now contain a significant number of extra lines. Even on that issue, does anyone read EULAs anymore? And were they ever even a waiver of responsibility anyhow? I mean, if someone writes a piece of code and then hides a line in the EULA which states that they can snoop at any time on the information contained in a person’s online account, does that allow them to do this or do the data protection laws
of that jurisdiction supersede those lines? Also, what about those lines of disclaimers added to email messages - what is that about?

What I am hoping to highlight here is the blind reliance on system output in lieu of common sense. This, in fact, could have major repercussions in the Ambient Intelligence world. Without stating the obvious, our systems’ main focus is on supplementing human knowledge/assisting in daily living. Few of our systems output hard and fast “correct” decisions. No, our systems are aids in daily life, and therefore, are prone to misinterpretation. If we were to take the above case (which I must make clear has had no decision as yet in a court of law) as a marker for the future, then none of us could ever release a product out into the wild. Therefore, let us hope that common sense prevails in the ruling, and in the meantime, please do test that last module that you coded!

Cloud computing has still got traction behind it especially now with Apple moving into the arena with the iCloud service (Ihnatko, 2011). Cloud relies on distributed architectures which centralise server resources on a scalable platform so as to provide on demand computing resources and services. There still, however, remain concerns over security risks that have been highlighted in the last twelve months with sensational breaches of systems belonging to giants such as Sony.

In future multimedia systems, seamless access to application services on different devices available to users in their vicinity will be commonplace. The availability of these services will change as the mobile user moves, but current 3G multimedia systems do not support access to multiple applications operating on multiple different devices in the context of a session or indeed seamless device session handover.

THE NEED TO CLASSIFY DATA

Classifying data is becoming a critical IT activity for the purposes of implementing the optimal data solution to store and protect data throughout its lifetime. It could become an important aspect of future Ambient Intelligent Systems. Developing a data classification methodology for a business involves establishing criteria for classes of data or application based on its value to the business. Four distinct levels of classifying data or applications are commonly used: mission-critical data, vital data, sensitive data, and non-critical data. Determining these levels takes some cooperative effort within the business and when completed, enables the most cost-effective storage and data protection solutions to be implemented. Data classification levels also identify which backup and recovery or business resumption solution is best suited for each level to meet the RPO (Recovery Point Objective) and RTO (Recovery Time Objective) requirements. Other considerations include availability, length of data retention, service levels and performance requirements, and overall costs.

Information is an extremely valuable asset to any organization and like all valuable assets; it should be protected from threats. Data classification can be defined by its strategic role in enhancing the protection of information assets while enabling proper access to them and the resource components that must be engaged to ensure its effectiveness. Forward-looking organisations that align data classification schemes with enterprise objectives are more likely to translate this strategy into reduced costs of doing business, revenue enhancement, and ultimately, shareholder value. As a strategic process, data classification either protects an organization’s information assets from harm, or enables access to information assets in a manner that supports the objectives of the organization.

Public organisations by tradition have understood the need for data classification as a tool for protecting information from outside interests. Sectors such as government departments (most of the time)
have well established schemes of protective marking that applies from state secrets to information that would cause only embarrassment if lost. The problem, however, is that processes that have worked well in the past are failing to meet today’s demands. A key problem is the sheer amount of information being generated and the ease by which this can be shared and distributed without ownership attributes attached. The mind-set of the “Facebook generation” is as widespread in the public sector as in the private, and they expect easy access to and sharing of data. For instance, in 2007, the loss of a HMRC CD containing the personal details of every person in Britain with a child under 16 went missing in the post. It was greeted with astonishment and anger by the public, however for those working in the sector, the only real amazement was that it did not happen earlier. Public sector data security policies have tended to prioritise confidentiality at the expense of availability and data integrity. This can often detract from system usability; however, there is also an increasing need to store personally identifiable information. A lot of this data has not fit within existing data classification regimes, and notably, there has been little tendency to consider the impact of the gathering of large quantities of such information. As a consequence, many systems at the lower end of data sensitivity have not had adequate safeguards in place. Those public sector data breaches, such as the HMRC incident, have provided a catalyst for widespread improvements. Many public sector bodies now place a premium on the establishment of a risk management culture aimed at rebuilding the public’s confidence in the storage and management of their sensitive data. Personal data can now be expected to receive the same treatment previously reserved for higher levels of classification. The UK Government has recently published a Security Policy Framework that outlines a set of new minimum mandatory measures including reporting and compliance mechanisms, which supersedes the protectively marked Manual of Protective Security. This underlines a new level of openness, as well as illustrating the increasing similarity in data and risks to data across the public and private sectors. A public domain Information Assurance Maturity Model has also been published, which provides a practical framework for IA compliance consistent with and building upon existing standards and regulation relevant to the private sector, such as ISO 27001 and the UK Data Protection Act.

The implementation of Ambient Intelligent environments, other new technologies, and rapid connectivity to external parties has led to increased risks to an organisation’s information assets. Information that is more valuable than ever before is more accessible and easier to divert. Organisations that fail to address the broader security issues that accompany this change will have insufficient controls in place to minimize risks. These risks could lead to significant financial, legal difficulties and reputation risk for these organisations. Appropriate preventive, detective, and corrective controls in the form of policies, standards, procedures, organisational structures, or software/technology functions, and monitoring mechanisms are therefore required to minimise the risks associated with the confidentiality, integrity, and availability of information assets within an organisation. These aspects of security should be the underpinnings of any ICT security program. The move to the cloud will be important. The move within the EU at present to enforce safe harbour and address the grey area of data domicile will usher in a greater awareness of data classification. It is also possible that due to the multi-tenant nature of a cloud platform, organisations will also pay greater attention to the data lifecycle phases and ensure that aspects such as data destruction is provided and auditable as part of the service. The very fact that an organisation is allowing confidential important information to leave the company network should lead them to examine how they can robustly protect that data and the answer can be simply an effective data classification strategy.
There are three main reasons to adopt data classification: 1) Tagging data allows it to be found more easily, 2) It helps to remove duplicated information, which helps to cut storage and backup costs, and 3) It can meet legal and regulatory requirements for retrieving specific information within a set timeframe, and this is often the motivation behind implementing data classification technology. Any organisation wishing to benefit from these 3 reasons is most likely to go down the data classification route. Consequently, any organisations that place little emphasis on information retrieval speeds, data duplication, and legal requirements are less likely to see the need to visit the arena of data classification. Common inhibitors to going down the data classification route are that the tools, processes, experience, and leadership are absent in many organisations to effectively classify data and to make potentially difficult choices. A policy-driven data classification approach provides an automated method to enforce the assignment of correct levels. There are various data classification tools available today, and each should be reviewed to determine their product focus meets the business requirements. In truth, modern organisations can be overwhelmed with redundant data, including relational and non-relational, much of which is redundant and varying in quality; therefore, plans must be in place to source most important data and document it along with business rules. Once this metadata is in place, then classification taxonomies can be used to tag assets of varying types, in terms of their business relevance.

Another danger is defining access requirements. It can be difficult for any organisation to understand exactly who has a clear need to use the information during regular business operations, who needs access only for support and maintenance purposes, and finally, who will periodically audit operations to prevent fraud and security incidents and detect performance anomalies. Industry standards recommend that the information owner should be ultimately accountable for whatever happens with the information. This therefore needs to be supported by a formal approval and authorization mechanism. Of course, unique requirements will be identified depending on how distributed each information system actually is, the different user profiles, and the selected access control solution. A single repository controlling global access is desirable, but not always viable from a business standpoint, while local groups granting access and synchronizing with each other periodically will require uniform approval criteria and validation procedures among the authorizing parties to ensure consistency.

A critical factor for success is that the classification scheme should clearly express the association between the data and their supporting business processes. Once meaningful terminology is employed in the classification scheme, a secondary capability should evolve seamlessly. This capability is the mapping and expression of security characteristics such as ownership, liability, and control of data. Here then, the security characteristics flow directly from the business process, rather than being derived from unrelated criteria. It is also critical that the business requirements start with a high-level business impact analysis so that they recognize critical business information. This can be done using questionnaires or interviewing key users to identify the business processes and unstructured information such as e-mails or spreadsheets that are most likely to impact the organisation. The key success factor in a data classification scheme is that classes of information are properly defined and related to process owners, easily communicated to all stakeholders, and clearly convey a business value to the organization, while expressing the need for hard, technical internal controls that IT understands.

Policies and processes are crucial. Ensuring that data classification schema are implemented requires storage administrators and end-users to agree on classification criteria. Policies can then be established to enforce the criteria on an on-going basis. A clear owner for the data classification process greatly facilitates the effort, class assignment process, and prioritization. Businesses can get bogged down in the assignment process if a clear leader is not established. With the advent of more advanced storage
management tools and information lifecycle management initiatives, the classification of data and information becomes critical to establish initial data placement and on-going automated management. The ingredients for a successful data classification implementation include a policy-engine and a tiered storage hierarchy. It is important to educate the workforce that the classification of data and documents is essential to differentiate between that which is of little value and that which is highly sensitive and confidential. When data is stored, whether received, created, or amended, it should always be classified into an appropriate sensitivity level. For many organisations, a simple 5 scale grade with categories such as Top Secret, Highly Confidential, Proprietary, Internal Use Only, and Public should suffice. It can, in reality, be difficult to convince decision makers in an organisation of the wisdom of investment in security measures such as data classification. Most organisations, when implementing the necessary security and control mechanisms, face a number of issues as security investments are justified against hypothetical losses, and communicating risks and benefits of security investments to nontechnical stakeholders can be difficult.

CONCLUSION

Ambient Intelligence is an evolution of technology, communication, and awareness towards human-computer interaction. Ambient Intelligence is the environment of computing, networking technology, and interfaces. It has the awareness of specific characteristics of human presence and personality. It deals with the needs of users, should be capable of responding intelligently, and may even engage in intelligent dialogue. Ambient Intelligence should not be visible to the user unless necessary. It is also crucial that interaction should be of minimal effort to the user, easy to understand, and therefore an enjoyable experience. Ambient Intelligence is being adapted to build smart systems to guide human activities in critical domains, such as healthcare, ambient assisted living, and disaster recovery. However, the practical application to such domains generally calls for stringent dependability requirements, since the failure of even a single component may cause dangerous loss or hazard to people and machineries. Despite these concerns, there is still little understanding on dependability issues in Ambient Intelligent systems and on possible solutions. There is, however, some work underway to build innovative architectural solutions to such issues, based on the use of runtime verification techniques (Cinque et al., 2010).

The evolution and convergence of information, communication, and networking technologies has established a framework for the adoption of ambient, ubiquitous computing in every aspect of life. Ambient Intelligence offers the real possibility of a revolutionary change in the way services are delivered. The AmI vision imagines ambient environments, enriched with assistive technology that can make necessary resources available to users in everyday life. Access to accurate information is important, and the pervasive nature of AmI technology ensures that users have constant access to up-to-date information regardless of their location (Kosta et al. 2010).

Ambient intelligent systems are context-aware and adaptive, providing contextually relevant information that is personalised to the user. This allows people to quickly hone in on the information they need to make informed decisions in time-critical situations. Digital location maps, communication tools, and messaging services support the numerous interactions that occur within people’s daily lives. The success of Ambient Intelligence will depend on how secure it can be made. Information retrieval must be user-led, and privacy must be protected to avoid any violations of the public’s rights. Ambient intelligence should be invisible, unobtrusive, but still in our consciousness (Riva et al. 2005). The ultimate goal for
Ambient Intelligence must, therefore, be user empowerment with the creation of universally accessible services, supporting authorised users in a transparent and effective way. This new technology has the potential to radically energise existing services by harnessing information and using it to its best effect, empowering users, and allowing them to focus more on what is really important in their daily lives.

*Kevin Curran*
*University of Ulster, UK*

**REFERENCES**


