

## DIGITAL TERRITORY: BUBBLES

Laurent Beslay and Hannu Hakala  
[Lbeslay@edps.cec.int](mailto:Lbeslay@edps.cec.int) & [Hannu.Hakala@vtt.fi](mailto:Hannu.Hakala@vtt.fi)

To be published in the Vision Book (2005)  
[http://europa.eu.int/information\\_society/topics/research/visionbook/index\\_en.htm](http://europa.eu.int/information_society/topics/research/visionbook/index_en.htm)

### INTRODUCTION

Digital territory is a vision. It introduces the notions of space and borders in future digitised everyday life. It is a place of information and communication.

Everyday life is experiencing a growing and ubiquitous digitisation, and each generation is more familiar with the digital data than the previous one.

Collected personal data are networked and thus remotely available. Simultaneously, the boundaries between traditionally distinct environments, for example, work, home, and school, are also disappearing as the private activities are brought into the public arena and vice versa. Although the distinction between private and public areas is not always clear-cut, people are aware of the boundaries between them, and of the grey zones, and take informed or intuitive decisions on how to act accordingly.

The vision promoting the implementation of a digital territory aims for a better clarification of all kinds of interactions in the future information society. Without digital boundaries, the fundamental notion of privacy or the feeling of *being at home* will not take place in the future information society.

Ambient intelligence is a vision that places human beings at the centre of future development of the knowledge-based society and information and communication technologies. These technologies will be embedded in everyday objects, and be almost invisible to those who use them, and the interfaces will be easy and natural to use.

Supported by technologies, the demarcation in digital territory between personal, private and public spaces will be decisive for its sustainability. Without digital boundaries, the information society will remain a parallel world, *a cyberspace* which was described by William Gibson [1].

To illustrate the vision of digital territory, the following sections describe the gradual digitised layers of everyday life space, where it is proposed to place digital boundaries. These range from the most intimate and private ones, just near to the skin, through limited family spaces and the virtual residence, to interactions of public and private spaces. The following examples intend illustrate the digitisation of the various physical territories. The primary concept is that of the bubble.

### THE NOTION OF TERRITORY AND ITS DIGITISATION

Personal space (understand privacy) is usually translated into physical distance from others. Depending on the context, someone may, for example, try to reduce the distance to a goddess

of beauty in a bar, to its minimum socially accepted (and even less) level, in order to *get* more information and eventually start a conversation to charm the goddess of beauty. But even when much closer, a real success considering the challenge, there is much valuable, and maybe forbidden, data that is not available, except in a digitised environment.

By claiming territoriality on a specific space, users tend to stabilise and to regulate the social systems, which surround them. Depending of the distances and the nature of these territorial changes, their owners have decreasing control. Altman defined three main categories of territory which will be useful to illustrate latter the different digital territories [2].

Closest to the person is the primary territory in which the individual has a complete control; it can be illustrated by the management of the individual's body and its relative nakedness. In the secondary territory the individual or a group has some control, ownership and regulatory power, but as a result of negotiations and transactions. Peoples' homes are clear examples of this secondary territory. This space has either been bought or rented, which gives the resident specific and personal rights on it, but it is still included in and regulated by a commonly established social, legal and even cultural framework. The public territory is characterised by a temporary quality and free access. Obviously, a public bathroom is a place that can be used freely, for a limited time, during which this space is completely private. These places are regulated by a public social contract.

By digitising this personal domain, but also its boundaries, the vision of digital territory offers the opportunity to introduce the notion of territory, property and space in a digital environment. The objective is to provide a tool that enables users to manage proximity and distance with others in this future ambient intelligence space, both in a legal and a social sense, as is the case in the physical world.

Ambient intelligence spaces will be a collection of technologies, infrastructures, applications and services across different ambient intelligence environments; car, home, the neighbourhood, the city, etc. This computing environment aims to facilitate and enhance peoples' everyday life by collecting a tremendous amount of data, analysing it, and providing an exclusive personalised environment better suited to the occupants. For example, a coffee cup may adopt specific colours depending on the temperature of the beverage, or the level of sugar accordingly to diet guidelines. The information and data needed for social or business transaction will follow people and be accessible everywhere.

In the information society, the crucial issue will be to design this digital territory such that ancestral user-control over the distance with others will be preserved, otherwise the exercise of charm described above, will become a nightmare. Indeed, partly illustrated in the famous movie *Gattaca*, the beauty target can almost be scanned by the admirer's desires. Helped by enhanced sensors with real-time analysis capability, the DNA (deoxyribonucleic acid) compatibility of this goddess can be discovered. Using profiles stored in various databases, to which the admirer has access, it may be possible to determinate, before a single word is exchanged, if goddess of beauty is socially free, or not, or even far more detailed data.

## **BUBBLES**

A bubble is a temporary defined space that can be used to limit the information coming into and leaving the bubble in the digital domain. It constitutes a digitisation of the definition of

personal space described by the psychologist Robert Sommer [3] as a *soap bubble*. The vision of the bubble is defined to gather together all the interfaces, formats and agreements etc. needed for the management of personal, group and public data and informational interactions.

The functionality of a bubble can be understood through two examples. The first example is mobile telephones and the second is access rights to a mainframe computer.

In the case of mobile telephones, these include a selection mechanism for personal profiles. These are used to control the ringing tones of the telephone, thus decreasing or increasing the possibility to reach the user. The concept of a bubble can be used to control the communication of the bubble; that is to say, both incoming and outgoing data flows; in this case telephone calls, which can be silenced or amplified according to the set-up. In the case of access rights to a mainframe computer, these rights can have different levels, for example, administrator, user or visitor, providing them with different system functions. The owner of a bubble can act as the administrator for the access rights.

The Wireless World Research Forum has defined a reference model and its physical levels of connectivity, called spheres, which are needed for different levels of communication. These spheres provide the definition of interfaces for the real world. The concept of bubbles resembles the spheres, but is defining the information-interfacing concept for the user in the virtual world.

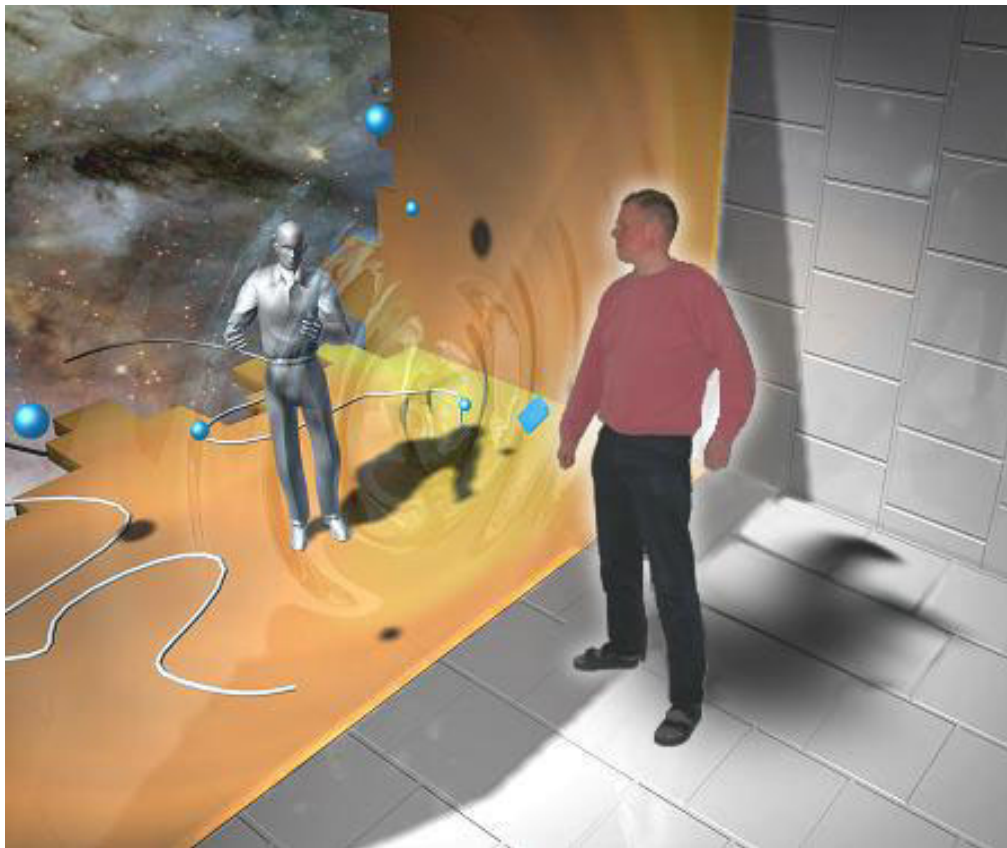


Figure 1: Vision, hearing, taste, etc. But what more can be *received* if additional sensors and ambient intelligence systems are available to assist people?

The bubble concept can be used to make filtering and selection of data. This contextual activity can be based on privacy, personalisation, priority, location, membership, ambience, circumstances, and time. The bubble may be described as a semi-transparent membrane that can be tuned to function differently depending on the direction of the movement of data. Filtering outwards is based on what people want to tell to external parties about information being stored inside the bubble, or about themselves. Information flow into the bubble is tuned based on information needs and requests.

A bubble can be created whenever it necessary for personal, community or global use. The bubbles can be shared between individuals or groups, for example, common bubbles for people having similar hobbies or bubbles for working teams. Bubbles can be seen both as a way to share views and experiences, but also as a means to limit the access rights of everybody in proper way. Sharing of views can be widened not only to expressions of the present time, but also to the past. It can be seen as sharing personal images with others; images can be watched as moments in time, recording major milestones, or images can be used as a means of personal expression.

The number of existing bubbles is not restricted, but will probably be naturally limited. This can be compared to the number of email folders, which depends very much of the ways of using them. The bubbles can be used as a manageable concept for various interfacing occasions; surfaces of the bubbles can be interpreted as a means of communication for all inputs and outputs. This emotional content has both spatial and temporal aspects.

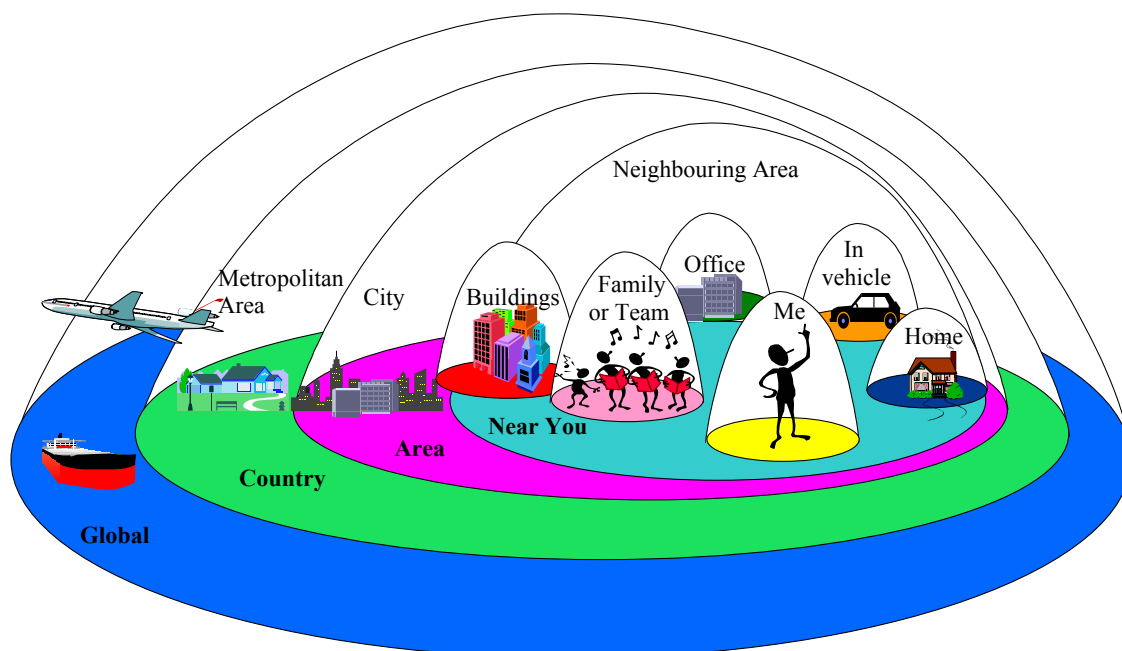


Figure 2: The environment can be seen as bubbles on different levels

In this vision of digital territory, identification smart tags (extremely tiny chips that can communicate with the outside world usually called RFID tag) have been massively spread and

embedded in a multitude of items of everyday life. If these tags represent a great source of knowledge for the user to be better informed about their nearby environment, they may also, if precautions are not taken, communicate a lot of sensitive information about the user. The implementation of bubble of communication and information may therefore help in a better control of the data delivered by the tags to avoid privacy invasive measures. If the tags are not allowed to communicate their information, under specific conditions, outside the bubble defined by the user, this will take care of the issue of access rights to the tag's information. Security threats may then be avoided: a mobile tag reader can not inform thieves of the potential value of goods and money (European Central Bank has planned to embed smart tag in euro bank notes) carried by their target, because of the opacity of the bubble for this specific data. Users can then create and manage their own digital boundaries.

A further idea related to this identification tags vision, can be built with user devices acting as tags themselves. The input and output capability of the user devices would be based on the semi-transparency of the bubbles, where users have access rights either defined by themselves, or through group memberships.

## **VIRTUAL RESIDENCE**

The vision of virtual residence can be seen as a virtual representation of the smart home. It may be used as a mental map to manage security and privacy, both remotely and from within the home. The physical and traditional residence constitutes a legal sanctuary, and protects the citizen, at least in democratic countries, from outside interference or invasive measures. In some countries, citizens are even allowed to shoot someone who places a foot inside the boundaries of the home.

With the advent of the information society and its digitisation effects, values protected by the inviolability of the domicile will also need protection outside the physical limitation of the house, and therefore requires the implementation of a virtual residence with digital boundaries as an extension of the legal sanctuary constituted by the home. Indeed, the digitisation of the everyday life environment tends to blur the borders defining the home (grass, fences etc.). When the home network is connected to the Internet, the domain under consideration is no longer the home.

The problem is that in the online world, there are very few social and legal indicators of what constitutes a private space. There are no clear labels to help Internet user estimate where private digital territories start or end, nor are there social norms, such as the *netiquette*, to discourage people from entering private online spaces without authorisation. This lack of indicators not only implies technological challenges, but also urges for clarifications of the social and legal framework of the new ambient intelligence space.

The vision of virtual residence is therefore proposed as a means of tackling new concerns about identity, privacy and security within an ambient intelligence space that encompasses both physical, online and virtual lives, and the embedding of computing in everyday devices. It consists therefore, of the following three elements: the future ambient intelligent and connected home considered as the main platform of the virtual residence vision, the online lives of people, families, households and their virtual representation and mobility and interoperability between different ambient intelligence environments or ambient intelligence spaces.

The future intelligent home will contain many smart devices able to sense activity and to communicate this information to other appliances, people and networks, both within the home and outside the home. Within the home, domestic infrastructures can be regarded as the backbone of all these connections. It consists of wired, wireless and mobile technologies, amongst others.

This smart home will have complex and intertwined networks to increase the connectivity, the interaction, and the *intelligence* of home devices and services. Security issues will be at the heart of this development. In most cases, the inhabitants of the smart home will not be able to effectively administrate these networks and their potential failures because of their complexity. An external service provider will probably carry out residential network administration, and as a result, domestic networks will be extended beyond the physical boundaries of the residence.

The above highlights the need to define a new digital territory, that is to say, a virtual residence that will encompass external network administration, be it automated or human driven. Because of the extent of interconnectivity of home networks and devices, disruptions will affect the whole network and will therefore, become *critical*. The criticality of the residence is of course also the result of the growing dependency of the smart home's inhabitants on networked home facilities and applications.

A monitoring system will be needed to conduct remote diagnostics. Future intrusion detection systems will be based both on network and physical sensors. Alarm functions will be a key element of the domestic critical infrastructure management. This latest example illustrates also the future bridge between the physical and the digital and their growing interdependency.

Virtual residence will also be used to represent the online private space of people, families or households in the information society and may enable the creation of new ways of living in cyberspace. Legal framework on music (CD) or movies (DVD) for instance, expects that these are used only for private listening and viewing, that is to say, only inside the family circle. A person can watch a purchased DVD wherever they like, at home, in the car, at work, in a hotel, as long as the person carries the disk with them.

In the future, it is expected that digital storage of entertainment and large bandwidth will increase considerably and that viewing or listening will therefore not be restricted to use of the actual disk. It is easy to imagine the digital storage of family entertainment on a family computer, which is accessible not only in the home, but also outside from any location. Virtual residence will be the virtual space repository where all the family private and commercial entertainment is stored. This will grant legal and social access to its use by the members of the family, who may be at different locations, for example at university, or in a hotel room, eating in a restaurant, etc.

Finally, the notion of physical *residence* has evolved, in some countries to encompass other mobile spaces such as the car. Thus, virtual residences and associated software that may be located in various places in cyberspace also need to be seen as a mobile and dynamic concept travelling through different ambient intelligence environments.

## PRIVACY, SECURITY AND IDENTITY

When the French philosopher Jean-Paul Sartre declared “l’enfer c’est les autres!” (meaning “hell is the others!”), he did not suspect that his claim would be so consolidated and potentially implemented by the advent of the information society where everyone tends to become naked, not only physically (through powerful and tiny sensors), but digitally as well, when all personal data are under the permanent and pervasive scrutiny of others.

The construction of this vision is motivated by major issues like privacy, security and identity, which may be raised from the digitisation of everyday life. The building process of this digital world may indeed generate mainly two kinds of threats for the respect of privacy, identity and security of the users.

The first is a lack of digital territoriality and therefore no protective boundaries. Four borders can be identified [4], and the crossing of one or more of these borders usually implies that people feel that their privacy is invaded. These borders are *natural borders*; *social borders*; *spatial or temporal borders or both*; and *ephemeral or transitory borders*. If these borders are quite well defined in the physical world, the digital environment is still characterised by the absence of these borders, which means that any abuse or violation of these borders can even not be noticed.

The second threat is a multiplication of invisible and uncontrolled bridges between the real and the digital environments. A growing number of emerging technologies, such as location-based services, fourth generation mobile telephones, closed circuit television, biometrics, etc., tend to establish links and bridges between a specific physical location and digitised knowledge and information. If the added value for the user is obvious, the potential new threats are not always highlighted. The following example describes a *positive* application of these bridges.

People are continuously creating their own views of the surroundings, but they are not really able to share these views with others. When being able to reference the real world with the digital space, tools and methods will be available that can be used for sharing these views with others. One idea to illustrate this is the concept of virtual notes; in the future people will be able to leave virtual yellow Post-It stickers where they want to. The only difference is in the visibility; they can be *seen* by everybody, or only those who are allowed, or those who are able to see them. The picture shown in Figure 1 illustrates the idea. People entering the house are all able to see the notice board, but not all the stickers.



Figure 3: Selective notice board

## **PUBLIC SPACES AND PRIVATE SPACES**

The digitisation process of the information society also concerns public spaces. Public territory is seen as a free access space with a temporary quality. It offers the user a limited jurisdiction in term of time and space. When a telephone call is made from a public telephone box, the users obtain jurisdiction of this territory for the time of the call. They control the access rights in this public place for a brief period of time and for a particular purpose.

The marking of private space is used to express that an individual has the right to do with that particular space what he/she wants. Core parts of this private space is kept either inside the second skin (wearable computing device), or at the most they are shared among the family, that is to say, they constitute the inside information of the family bubble (residence). Some parts of this private space may be published temporarily to all the residents of a community, that is to say, made public, which is similar to, for example, arranging an open meeting at home for everybody in a neighbourhood.

The difference between private and public space is defined clearly on some occasions, like concerts or theatrical performances. The audience has the right to share the experience, that is to say, be there and enjoy, but can not make recording or take pictures. There are other cases where the borderline is not this clear. The concert may not be arranged on a commercial basis, but still there is no right for those attending to make a recording of the performance and to sell

it without permission. Many of the issues near the borderline between private and public spaces are such that their uses require some kind of negotiation or agreement between the users of the spaces and the owners of the rights of the spaces. The grey zone is then defined as specific territory where a negotiation or transaction is required to obtain the jurisdiction of the targeted space.

Real world locations can be used to access both private and public virtual spaces. Figure 4 illustrates one scenario, where several people have different access rights to the public notice board. Some of the people may *see* only the information that is accessible to everybody, but at the same time some of them may have their own private information delivered through the same channel, and that information is only *visible* to them.



Figure 4: Viewing information through common notice board with personalisation possibilities through selectivity

The interactions between public and private spaces in the future digital world and the significant role of digital territory can be also illustrated with the controversial example of a crime in the street.

Imaging that a murder has been committed in the street in front of a house. Alerted by the emergency service, the police arrived on the crime scene few minutes after the tragic event and undertook the investigation by collecting evidence and testimonies. Up to this point, the description of this scene is absolutely traditional.

Now, consider what happens within the vision of a digital territory. To obtain maximum information, the police not only define the physical boundaries of the crime scene with the well-known plastic tape, but also the digital boundaries surrounding the crime. They create a bubble around the victim, an information sphere or *infosphere*. This digital crime space encompasses other peoples' digital territories, such as the personal bubble of the citizens who were in the street. This defines information from devices such as mobile telephones with *always on* cameras, wearable computers with detection facilities and proximity

communication systems, etc. It also encompasses the houses in the street near the crime scene, and therefore the virtual residences near to where the crime took place. These include residential gateway systems, intrusion detection agents, etc. Finally, the infosphere also encompasses the digital part of the public space constituted by the street, including thermal sensors, closed circuit televisions, global positioning systems of public transport, etc.

All these territories have collected and stored, with their sensors, a huge amount of data, which may be useful for the detection of the offender. The clear drawing of several and specific digital boundaries and territories, and of course, the democratic nature of the country where the crime took place, will permit the preservation and respect of the fundamental rights of the owners of these territories. At the same time, the police will have access to the data only under specific conditions and may be with a particular process, for example to protect the identity of the witnesses or the legal sanctuary nature of the virtual residence as part of the residence.



Figure 5: Bubble used at a crime scene

## CONCLUSIONS

In relation to the growing ubiquitous position of the Internet, it is already becoming clear that people today contrast the online with the offline to a much lesser extent. This was typically the case for the first generation of the Internet. In the same way as the information society will be embedded in society at large. The individual, the nearby environment, the physical residence, bubbles, and virtual residence, may become intertwined, paradoxically perhaps, by establishing clear indicators and boundaries for the digital territory.

By defining digital borders, the vision of digital territory creates a continuum between the physical world and its digitised counterpart. The construction of digital boundaries consolidates the gateways already established between these two worlds. This paradox will be catalysed by the implementation of a growing number of bridges between the two environments. Location-based services, radio frequency identification tags, body implants, ambient intelligence sensors, etc. will permit the implementation of a trustworthy environment and therefore the domestication of the ambient intelligence space by the individual. The vision will facilitate the transition through a traditional society that coexists with an information society, to a single society whose citizens have accepted and adopted the fusion of physical and digital realities.

In this future society, people will still be able to control and manage distance from others with new tools provided by ambient intelligence space technologies.

## REFERENCES

[1] William Gibson *Neuromancer*, Ace edition, July 1984.

[2] Altman, I. *The Environment and Social Behaviour*, Brooks / Cole Monterrey, 1975.

[3] Sommer, R. *Personal Space: The Behavioral Basis of Design*, Prentice Hall Trade, June 1969.

[4] Marx, G.T. Murky conceptual waters: the Public and the Private, *Ethics and Information Technology*, Vol. 3, No. 3, pp. 157-169, 2001.