




## Digital Territories

Towards the protection of public and private space in a digital and Ambient Intelligence environment

**Authors: Barbara Daskala and Ioannis Maghiros**



EUR 22765 EN - 2007



***The mission of the IPTS is to provide customer-driven support to the EU policy-making process by researching science-based responses to policy challenges that have both a socio-economic and a scientific or technological dimension.***

European Commission  
Joint Research Centre  
Institute for Prospective Technological Studies

***Contact information***

Address: Edificio Expo. c/ Inca Garcilaso, s/n. E-41092 Seville (Spain)  
E-mail: [jrc-ipts-secretariat@ec.europa.eu](mailto:jrc-ipts-secretariat@ec.europa.eu)  
Tel.: +34 954488318  
Fax: +34 954488300  
<http://www.jrc.es>  
<http://www.jrc.ec.europa.eu>

***Legal Notice***

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

A great deal of additional information on the European Union is available on the Internet.  
It can be accessed through the Europa server  
<http://europa.eu/>

JRC PUBSY 7125

EUR 22765 EN  
ISBN 978-92-79-05653-6  
ISSN 1018-5593

Luxembourg: Office for Official Publications of the  
European Communities

© European Communities, 2007

Reproduction is authorised provided the source is  
acknowledged

*Printed in Spain*

# D1gital Territ0ries:

Towards the protection  
of public and private  
space in a digital and  
Ambient Intelligence  
environment

*Authors:*

Barbara Daskala and Ioannis Maghiros

**Institute for Prospective  
Technological Studies**

2007

## ■ Foreword

Technology influences positively the way we live, work and enjoy ourselves. It addresses emerging mobility requirements and information needs; however, at the same time, technology poses many risks already identified or new, that will have to be dealt with. Balancing security and privacy issues is fundamental in making the world of tomorrow acceptable, based on the technology-enabled democratic principles that we have come to understand and apply for years. The danger here is that users faced with increasing privacy intrusion will simply decide not to use the technologically-enabled services, thus impacting on the potential for growth, employment opportunities and living in digital world as a whole.

Considering that people have over the years mastered the art of using distance as an indicator to control the amount and type of personal data they wanted to share, IPTS has set out to study the concept of Digital Territories (DT) and assess the likelihood that it may be used to balance security and privacy needs in the digital world. Primarily, we tried to envision specific situations of personal data in a home environment, which is continuously stretched through the social needs of its constituent members. This resulted in the study of Virtual Residence, where measures to adequately protect personal data were studied, even in those cases where these data were stored in servers controlled by third parties. Then the concept of the bubble was created to denote a personal info-sphere surrounding the individual, which is used to restrict and / or allow the information coming in or going out of it; based on the idea of the bubble, the concept of territories of influence started to emerge.

Emerging concerns regarding security and privacy and the protection of personal data pointed at a need to further develop the identified concept of DT into a framework that would enable users to manage proximity and distance with others in the digital and the presumable ambient intelligence space. Thus, considering the concepts of private and public space on the one hand and physical and digital space on the other, and their interrelation, the DT concept was further developed. The objective was to provide a more systematic view on the blurring boundaries of public and private digital space, and thus assist towards tackling concerns of privacy, security and identity of people's online activities.

This report is an introduction to the concept and framework of the Digital Territories, attempting to prove its relevance and usefulness and arguing in favour of more research in this area.

***Ioannis Maghiros***

Action Leader - Techno Economic Foresight in the Information Society (TEFIS)  
Information Society Unit  
IPTS

## ■ Acknowledgements

The study on Digital Territories has been based on ideas developed at the Techno-Economic Foresight for Information Society (TEFIS) group of DG JRC IPTS' IS Unit.

The study on Virtual Residence (Annex I) has also been carried out by DG JRC IPTS staff by the Cyber-Security group; we would like to specifically acknowledge the efforts of Laurent Beslay and Yves Punie for conducting the research and authoring that study.

A number of experts external to the JRC also contributed to the creation of the Digital Territories concept; we would like to acknowledge the contribution of Dr Achileas Kameas of the Research Academic Computer Technology Institute (CTI) as well as of ATLANTIS Consulting for their efforts in authoring the Study on Digital Territories, which served as a background paper for our study, (Annex II).

Also, we would like to thank Laurent Beslay and Hannu Hakala for their contribution to the concept of the bubble.

Other experts participated in workshops or met with the authors on specific topics. Their names and affiliations are included in the list below.

Yves Punie (IPTS)	Achilles Kameas (Research Academic Computer Technology Institute - CTI)
Laurent Beslay (EDPS)	Nena Karagianni (Research Academic Computer Technology Institute - CTI)
Hannu Kakala (VTT)	Irene Mavromati (Research Academic Computer Technology Institute - CTI)
Serge Gutwirth (Vrije Universiteit Brussel)	Tonia Damvakeraki (Atlantis Consulting)
Gill Wildman (PLOT)	Foteini Psarra (Atlantis Consulting)
Marcus Kirsch (UNVOID.NET)	Effie Amanatidou (Atlantis Consulting)
Despina Papadopoulos (5050ltd.com)	Dr Rob Van Kranenburg (XS4ALL)
Bas Raijmakers (STBY & RCA)	Vagelis Papakonstantinou (Drakopoulos Law Firm)
Daniela Pirrone (COMUNE di PALERMO)	Vassilis Zorkadis (Greek Data Protection Authority)
Athina Stavridou (NTUA)	
Christian Becker (University of Stuttgart)	
Danny De Cock (Katholic University Leuven)	
Ganesh Sauba (Advantica Ltd)	

## ■ Table of contents

<b>EXECUTIVE SUMMARY.....</b>	<b>7</b>
<b>1. INTRODUCTION.....</b>	<b>11</b>
1.1. A new world.....	11
1.2. Peeping through the hole.....	12
1.3. Scope and structure of the report.....	13
<b>2. A NEW CONCEPT FOR A NEW WORLD: DIGITAL TERRITORIES.....</b>	<b>15</b>
2.1. Types of DT.....	16
2.1.1. Primary or personal.....	16
2.1.2. Secondary or group.....	16
2.1.3. Public.....	17
2.2. Basic DT components.....	18
2.2.1. The bubble.....	18
2.2.2. Borders and markers.....	19
2.2.3. Bridges.....	20
<b>3. A SPECIAL CASE – THE VIRTUAL RESIDENCE.....</b>	<b>21</b>
3.1. Smart home.....	22
3.2. Mobility.....	23
3.3. Online family life.....	23
<b>4. INTO PERSPECTIVE: WHY DT? .....</b>	<b>25</b>
4.1. Privacy and data protection considerations in the digital and Aml environment.....	25
4.2. Privacy protection laws, regulations and standards exist and are in effect.....	27
4.3. Enters DT... ..	28
4.3.1. DT in action I – the present: from simple Internet search to Social Networking and Web2.0.....	29
4.3.2. DT in action II – the future: RFID implants.....	32
4.4. Synthesis .....	33
<b>5. EPILOGUE.....</b>	<b>37</b>
5.1. Some considerations... ..	37
5.2. Next steps.....	37
<b>REFERENCES .....</b>	<b>39</b>
<b>ANNEX I: A VIRTUAL RESIDENCE IN AN AMBIENT INTELLIGENCE SPACE.....</b>	<b>41</b>
Executive summary.....	41
Introduction.....	43
Virtual Residence: Definition and Basics.....	48
Possible application fields for VR.....	59

<b>ANNEX II: STUDY ON DIGITAL TERRITORIES.....</b>	<b>69</b>
Executive summary.....	69
Introduction.....	72
Tools and approach for the study .....	74
Study methodology and work plan followed.....	76
Detailed introduction of the concept of digital territories .....	78
Key technologies for DT and emerging technologies involved .....	82
Boundaries and the management of distance and proximity .....	86
Bubble, a contextual data filter .....	90
Private and public spaces .....	94
Bridges between real and digital worlds .....	96
Legal and social framework .....	101
Security and privacy concerns .....	104
Mobility of citizens.....	111
Suggestions for raising awareness .....	114
Conclusions.....	114
References.....	115





## ■ Executive Summary

It seems that a whole new world is out there, a virtual or a 'digital' one, the Net, running almost in parallel to our normal physical world. The new world does not require our physical presence; individuals assume various different 'digital' identities, their 'digital' self becoming an extension of their physical one. We surf the net, search for information, socialise, transact and buy CDs or books or tickets; we leave many 'digital' traces behind us while doing so. At the same time, and because of this, the requirements for identification and authentication have increased in the digital environment. The collection, storage and exchange of sets of personal data, some of which may be sensitive, pose many new challenges to online identity and raise serious considerations regarding our privacy and protection of our personal data.

Extensive research and studies have been devoted to privacy during the last thirty years. Privacy may be defined in terms of the physical distance from others; it is an iterative, ever-changing 'boundary-regulation process in which a person or a group sometimes wants to be separated from others and sometimes wants to be in contact with others' [2]. In order to achieve the desired level of privacy, which is highly dynamic, a balance between public and private has to be reached. In the digital world, it appears that privacy is far easier to violate and far more difficult to protect: the default in cyberspace is more likely to be privacy invasive, thus always requiring appropriate action from the user. The advent of an Ambient Intelligence (Aml) environment, i.e. a vision of the future Information Society where people will be surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects (furniture, clothes, vehicles and smart materials), renders data protection and privacy issues even more difficult to address, especially when considering that the collection, storage and exchange of personal data are a requirement for such an environment to function properly.

Laws, regulations and international standards have already been gradually established, in order

to protect personal data. And yet these practices often prove to be inadequate towards ensuring the protection of our privacy and personal data in the digital space, since sometimes they cannot be enforced adequately or cannot keep up with rapid technological developments and social changes. Perhaps the existing legal framework may need to be improved to ensure the citizen's trust in the Information Society?

In this context and to address these considerations, IPTS has engaged in research on developing a concept that would allow individuals to manage distance and boundaries, the 'territories', in a social and legal sense, in this new space, while also providing a proper balance between security and privacy. The idea of 'territory' has been present in the physical space almost as long as human presence on earth. Legal rules and tacit socio-cultural norms and even traditions constitute the guidelines for people's understanding of what is private or public space or what is socially accepted as private or public space. Although the distinction is not always that clear, people have learnt to become aware of the boundaries between them and act accordingly.

At this point, the Digital Territories (DT) concept is brought forward to provide an appropriate way to protect privacy and personal data in the digital world, while promoting freedom of expression and enhancing collaboration and communication in public places of the digital world. It is considered equally important to protect the 'openness' of these public places in the digital world, as to protect the private space and personal data of an individual. Specific examples are drawn from present 'on-line' applications, namely Google, MySpace.com, Blogs and Wikis, as well as from potential future or emerging applications, which seem to raise even more concerns (e.g. RFID implants) to better describe the DT concept.

### **The benefits of DT**

DT as a concept provides a more systematic way to conceptually represent data and information flows, explicit or implicit user consent, as well

as map dynamically and flexibly the borders between private / public spaces and the 'grey' areas in between and thus becoming a systematic and analytical tool towards defining such boundaries.

DT as a framework could be also used to supplement appropriately the current legislation on privacy and data protection. It could contribute to mapping personal data sufficiently, thus rendering easier the task of its legal regulation and its enforcement. Software developers and service providers could also use the DT framework to design their products and services in such a way so that these merit being labelled as 'privacy-enhancing technologies'.

Moreover, DT could assist in promoting awareness of people regarding the privacy and security risks in the digital world, so that they could then decide what they should try to protect and what they do not need or cannot protect. It could also enhance users' awareness regarding the security practices that they would have to follow themselves in order to protect their data.

With regard to the use of surveillance and its social implications, the setting of boundaries in the digital sphere would provide a basis for consensual resolution. In this context, it could be used in the development of Aml products or services to enhance the offered level of security and privacy. Security and privacy requirements could be considered from the initial development phase ('privacy by design').

## DT – An overview of the concept

In the context of our study, we have identified three different types of digital territories (DT), according to the degree of control that individuals exercise on their data in the specific space and the relative duration of the individuals' claims to the space: Primary or Personal DT, Secondary or Group DT, and Public DT.

*Primary or Personal DT* relates to a person's digital space and encompasses the individual's digital identities as well as all digital personal data of a person (including any data which are generated by the person's on-line activities). The second DT type, the *Secondary or Group DT*, is a hybrid as it combines both the total and pervasive control allowed to participants in primary

territories and the almost-free use of public territories by all persons; it corresponds to groups of individuals that share common interests or purposes and hence it is also referred to as a group DT. Finally, the *Public DT* is a space where almost any individual has access and may exercise a low level of control. It is a kind of 'commons' in digital space, a free territory, open to the society members at large, fostering freedom of expression and open circulation of ideas and points of view.

We have also identified four DT components that are necessary in order to enable a functional DT: namely, bubbles, borders, markers and bridges. Firstly, the (digital) *bubble* is a dynamic personal info-sphere, or better data-sphere, since it basically 'holds' the person's personal data, and is used to set the borders, restricting and / or allowing data / information coming in or going out of it. The notion of bubble encompasses all the interfaces, formats, rights and agreements etc. needed for the management of personal data and informational interactions.

The size of the bubble may vary as a result of its information content, the form of interaction the individual wants to perform and the overall 'trust' assigned to the environment of the interaction. Using a cell-membrane analogy, the bubble has a two-way exchange with the environment – sometimes from the inside of the cell out to the environment and sometimes from the environment into the cell.

The second component of a DT, the *borders*, are seamless, fictitious lines that draw its perimeter, implementing the permissions set through the bubble. Therefore, these borders are always under negotiation and they adapt to different situation or spaces, they are also not autonomous but are set by the bubble; they thus change, decrease or increase, according to the 'will' of the bubble, and the boundaries that it wishes or is obliged to set.

The way of expressing and making boundaries visible, is by setting *markers*. In the physical world a marker would be the 'Keep Out!' sign placed in one's garden, informing other people that this is a private space where trespassing is not permitted. In digital space, it could be the log-in screens for accessing one's personal computer or it could be the 'private' tag put in one's folder.

The *bridge* is the fourth component of a DT. It differs from the other components in the sense that it is not a component per se, but provides the link between the physical and digital / virtual world. As the boundaries between these two worlds become blurrier with the development of new technologies in a future Aml environment, the concept of the bridge will become increasingly important in relation to the identification of the personal data-space and the drawing of the DT boundaries.

Furthermore, within the context of DT, IPTS has developed the concept of 'Virtual Residence' (VR), which projects the concept of a legally or through the adoption of social norms, protected 'residence' in the on-line, digital world. It relates to the individuals' lives and the personal data stored at home, which at times need to be remotely accessible from the digital world. VR is also an attempt to address the need for more privacy enhancing initiatives, at least in the 'home environment'. VR has been considered a special DT case, especially since it constitutes a first clear example of territory (physical and digital) that requires regulatory protection, and as such it has been studied separately. It is an attempt to identify alternative legislation to protect data of a personal nature, exactly as it is protected in our physical homes now. VR is a DT, made up by the integrated DTs of the 'home' residents who take turns in managing the 'shared' data, since in many cases more than one persons use the same physical infrastructures. VR could become the first DT application area, since current applications put additional pressure on taking relevant action and the issues posed are perceived as easier to address.

## Challenges and future steps

The four components described in the previous paragraphs are essential in implementing a functional DT. However, this implementation also raises certain challenges. For example, identifying effectively the boundaries of the private DTs is difficult as sometimes the boundaries between private and public space in the digital world are not analogous to that of the physical, since these two worlds have many differences. Further to this, it should be noted that sometimes seemingly (legally) un-regulated spaces as certain spaces of Internet have so far been, have provided the opportunity to communities of the Net for useful and

innovative creation and development of breakthrough solutions. For example, the open-source and free software movement create a space to facilitate the exchange of ideas and where freedom of expression is exercised and where control by its members is shared. Another challenge regards the balance between privacy and security: privacy of a citizen in the sense of protection against loss of control over his/her personal data when operating in the network, versus the 'ambient security standpoint', the network or society that needs to protect itself against users with malicious intentions.

Finally, in order to further gain more insight into the concept and supplement it appropriately, further research is considered necessary, which however should be conducted within a more systematic context. A feasibility study is proposed as a next step towards such a research, in order to assess the viability of the idea; it may constitute a preliminary analysis in the course of this study so as to ascertain its appropriateness and its likelihood to succeed. It may also provide an analysis of possible alternatives as to how to proceed with the study of the concept, in order to further gain more insight into the concept and supplement it appropriately.



## ■ 1. Introduction

### 1.1. A new world

While standing from a distance observing people go around, hurrying to their work and going about their everyday tasks, at home or going out, one may think that nothing has changed over the years; and yet it has. Our lives, we have become increasingly 'digital', communicating with our clients, family and friends remotely via new sophisticated devices, shopping 'on-line', taking notes on our smart pocket PDAs. If we look closely, most of the people around use a product of digital technology, be it an 'old' mobile phone or a cutting-edge technology gadget.

Moreover, we have learnt to take for granted this digital part of our lives oblivious to the underlying infrastructure, the thousands of small and big networks around us; we do not take notice and most of the times we are not able anyway, since digital communications take place seamlessly across borders. Castells (2001) rightly likens Internet to the electrical grid and the electric engine; it has become the 'fabric of our lives' [8], a basic necessity for most people in the developed world, and despite it being expensive in some countries, it is still being extensively used by an ever growing percentage of their population. People go 'on-line', surf the 'Net', search for information, socialise, talk with friends, check e-mails, buy CDs or books or tickets.

We are therefore faced with changes affecting our society deeply and the way it operates. Negroponte (1995) accurately forecasted that we are faced with a gradual change from atoms to bits, an irrevocable and unstoppable process [28], which leads to what is defined as the information age and the rise of the network society, also identified by Castells [7]. The Internet is the technological basis and information lies at the centre of the network, hence the term Information Age. The term Infor-

mation / Knowledge Society is introduced to signal the objective to advance from a networked society towards a society where information is the prime resource thus dubbed 'Information Society'.

'The Net', 'on-line', 'digital', 'virtual', 'cyberspace'<sup>1</sup> are the main terms used interchangeably to basically denote this alternate space / world running in parallel to the 'physical' world.

Undeniably this new world has affected time and space, having shifted the focus from place to persons, especially through the use of mobile devices. The new world does not require our physical presence; individuals may socialise over the internet but they do not take their physical bodies there: their bodies remain at the chair in front of the computer [26]. What is most important is that on-line they assume various different 'digital' identities, their 'digital' self becoming an extension of their physical one.

Individuals sit behind their screens and they transact or relate to other people online; either way they need to identify themselves to on-line services, or other 'persons' or third parties etc. in order to be granted the right to proceed with whatever it is they want to do. The requirements for identification and authentication have undoubtedly increased in the digital environment: people have multiple digital identities (e.g. one identity in an on-line shop where they buy books and CDs, etc and a different one when buying shares on-line). The collection, storage and administration of sets of personal data, some of which may be sensitive, pose many new challenges to online identity.

On the one hand, individuals wish to maintain the simplicity of transacting in relative anonymity just as they do in the crowded streets and shops of a big city; 'anonymous' cash facilitates their diverse needs. On the other hand, on-

<sup>1</sup> The term 'cyberspace' was coined by the novelist William Gibson in his novel *Neuromancer* (1984). For John Barlow of the Electronic Frontier Foundation, cyberspace is the place 'where you exist when talking on the phone' (Rucker et al. 1993: 78) and according to Featherstone and Burrows, cyberspace is a generic term referring to a whole group of technologies, all of which have the ability to simulate environments within which humans can interact (Featherstone and Burrows 1998 [1995] quoted in [26]). Or put more simply: in this new space the exchange of information is in the form of a software code; this creates cyberspace [26].



line service providers require some form of identification, primarily so as to better serve their clientele, but also so that commercial liability can be exercised. In addition, the governments and states wish to protect their citizens and create a state of security and trust, where identity is a significant building block. As a result, identification requirements in this emerging new world require 'handling with care'. Society needs to embrace new skills to enable it to master emerging risks and make the most of emerging opportunities. All the more so as the world we live in continues to evolve as a matter of course.

## 1.2. Peeping through the hole

It is argued that the extreme sophistication of ICTs and emerging technologies may create a future environment, where computing will be literally everywhere, so that we won't even realise when we use it. Such an environment has been for some time now referred to as Ambient Intelligence (Aml); the term was first introduced by the Information Society Technologies Advisory Group (ISTAG) in 1999 and regards 'a set of properties of an environment that we are in the process of creating'. It basically refers to a vision of the future Information Society where people will be surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects (furniture, clothes, vehicles and smart materials); such an environment will be capable of recognising and responding to the presence of different individuals in a seamless, unobtrusive and often invisible way. It is however important to note here that ISTAG (2002) abstains from defining the term more tightly, since they deem important that Aml remains an 'emerging property' and that Aml should be treated as an 'imagined concept' and not as a set of specified requirements [20].

Moreover, Aml can only be fully developed by following a holistic approach, encompassing technical, economic and societal activities. It should not just consider the technology, but the complete innovation supply-chain from science to end-users, and should take into account the various features of the academic, industrial and ad-

ministrative environment facilitating or hindering the realisation of the Aml vision. (ISTAG 2003: 12-13).<sup>2</sup>

In Aml, human beings are placed at the centre of future development of the knowledge-based society; its main objective and expected result is ultimately empowered users in terms of added convenience, safety and security, as well as time and cost savings. Aml technology has the potential to positively impact the way we work, move, enjoy and live. It would also contribute towards economic growth, foster business and knowledge opportunities as well as efficient services, and most importantly increase the employment opportunities for people. Aml is expected to enhance the use and the protection of our digital identities, with the development of appropriate technologies.

Aml may be a vision, but considering some current technology applications, it does not appear to be very far away. The Radio Frequency Identification (RFID) technology for example already provides a 'bridge' between the physical and the virtual world, linking physical objects to information in digital format, which is stored in databases and remotely accessible through the Net. It is therefore even more necessary, while building the Aml environment, to raise awareness as to its opportunities and threats in advance, so that people become more 'intelligent' regarding the use of technology. In an Aml world, the need for identification increase even more, as we will need to identify ourselves many times a day in order to use Aml services. The identification and authentication process in many cases will occur as a result of a conscious, deliberate decision on our part; however, most importantly it may also happen automatically, without any intervention on our part [1]. Our identity today may be based on an accumulation of our identity attributes and identifiers, but tomorrow it may regard such elements as where we have been, the services we have used, the things we have done: an accretion of our preferences and behavioural characteristics [1], enabling thus identification and authentication of people through *profiling*.

Profiling will undoubtedly be a requirement for the Aml environment to function properly;

<sup>2</sup> See for a more extensive discussion of the Aml vision: Punie, Y. (2005) 'The future of Ambient Intelligence in Europe: The need for more Everyday Life', COMMUNICATIONS & STRATEGIES, no. 57, 1st quarter 2005, pp.141-165. [ART: 92216]

however at the same time, it raises serious challenges and poses new risks especially regarding security and privacy, since it will require an enormous amount of behavioural, personal and even biological data that would need to be collected, stored and exchanged. Today's concerns about potential abuses of privacy rights can only get worse since technology is progressing faster than the policy-building process that might otherwise assuage these concerns. Apparently living in an Aml space would require a proper balance between a complex diversity of interests and values related to freedom of speech, access to information, protection of the individual sphere, trust, security, protection against discrimination, protection of identity, and protection against intrusions by public and private actors [8]. In this context, the protection of this data is deemed very important. Towards addressing this issue, a new framework has to be developed that would enable 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 [2]. The sections that follow present this concept, which has been defined as 'Digital Territories'.

### 1.3. Scope and structure of the report

As already stated above, the increasing proliferation of personal data in the digital space and the importance of electronic identification as we move towards an Aml environment, has raised the need for a concept that would allow individuals to manage distance and boundaries in the social and legal sense in this new space, and that would also provide a proper balance between security and privacy. IPTS has been engaged in research on this topic since 2002, when a study was initiated on issues related to Aml space and technologies and the concept of 'Virtual Residence' (VR), as well as the balance between security and privacy in the everyday life of the citizen. This study led to a draft report (annexed in this report at Annex 1): this in turn led to a project for further studying the concept of Digital Territories (DT); the results of this project and the corresponding report can be found in Annex 2.

Subsequently, IPTS further explored and extended the concept of Digital Territories and has developed this report, based on the findings of the

two previous reports. The study of the DT concept presents particular difficulties for the researcher. At first, one has to identify current threats and extrapolate future threats, arising from the deployment of emerging technologies. Even more difficult is developing a logical structure to address the challenges which could be technologically implemented. In the course of this study, we have focused on the concepts of physical and digital world in conjunction with the notions of public, private (or personal) space, and especially their transition when these two spaces are projected to the digital world. As part of this activity, focused as it is on Aml space, IPTS envisages contributing in shaping the requirements, definition, conception and development of specific security, trust and privacy technologies and infrastructures, and the policy framework needed for the future management of privacy and identity in the European Information Society.

As a result, the presentation of the concept itself has preceded the justification of its development, because having first a basic understanding of what the concept entails, would make it easier to comprehend the necessity for its development; especially in the context of a future Aml environment. The report is structured as follows:

In Chapter 2, the DT concept is presented in detail, framing its associated terms and defining its basic layers and components.

In Chapter 3, the concept of Virtual Residence (VR) is defined and presented in more detail. VR is considered a special case / example of a DT, and it has also been studied separately.

In Chapter 4, we provide the context within which the DT concept was conceived and developed, the primary drivers that led to its creation. In order to explain the context better, as well as the DT approach itself, we provide some practical examples for the application of DT in present and near future digital services. It should be noted that the presentation of the concept itself has preceded the justification of its development, because having first a basic understanding of what the concept entails, would make it easier to comprehend the necessity for its development; especially in the context of a future Aml environment.

In the final chapter, possible benefits of the DT approach are identified, as well as further con-

siderations related to the application of the DT concept. Also, proposals are made regarding the next steps that could be taken regarding further analysis of the DT concept.

The two background studies / reports on Virtual Residence and DT, used in the making of this report, are annexed in Annexes I and II, respectively. In some sections of this report, we make references to the Annexes, where more information may be provided on a particular issue.

At this point, it should be noted that in the course of our analysis, we refer to examples of both current/present and potential future situations. However, although the full benefits from the application of the concept are anticipated in the future, we had to develop it considering current and emerging situations. Besides, it is possible to apply DT quite effectively to present situations as well; however, its strength lies in its ability to be used in a future Aml environment, where the complexity of the environment multiplies the challenges.



## ■ 2. A new concept for a new world: DIGITAL TERRITORIES

The notion of 'territory' is present in the physical space almost as long as human presence on earth. Legal rules, tacit socio-cultural norms and even traditions constitute the guidelines for people's understanding of what is private or public space or of what is socially accepted as private or public space. Although the distinction between the two spaces is not always that clear, people are aware that boundaries do exist and they act accordingly. The fenced private lawn, the 'keep out' sign on someone's private lawn, the questioning look given to strangers in a neighbourhood bar, and the urban gang's respect for the turf of other gangs are just a few examples of the 'intuitive validity of the idea of territory' [2] in the physical space.

Territory is defined as more distant, somewhat removed from the immediate person, and it involves use of places and objects in the environment [2]. Territorial behaviour is a self/other boundary-regulation mechanism that involves personalisation of or marking of a place or object and communication that it is 'owned' or claimed to be 'owned' by a person or a group. This place can be also referred to as a 'personal space', another mechanism used to regulate interpersonal interaction. Personal space is often translated as 'physical distance from others' and refers to the 'invisible bubble', an invisible area surrounding the human body – intrusion into this space by others leads to discomfort or anxiety [2]. Undoubtedly, we all need a personal space and we learn how to manage it from a very young age, e.g. sharing toys for toddlers, the 'no entry' sign on teenager's door etc.

According to Irwin Altman (1978), both territorial behaviour and personal space act as mechanisms used to regulate interpersonal interaction and to achieve a desired level of privacy [2]. Privacy is conceived of as an interpersonal boundary process by which a person or group regulates interaction with others. It is well accepted that the closer you physically get to a person, the more intimate (private) data you are likely to share with this person. If someone comes too close to us, vi-

olating our personal space and our territory, we may react by stepping back or push the other person back. If we feel we have too much privacy and we are isolated, we may approach a person to talk or we may smile at someone encouragingly in order to engage in conversation, thus intending to put an end to our isolation. The relation between personal space, territory and privacy – in this case the control over the amount and quality of personal information that individuals wish to exchange – is strong and dynamic in nature. Often unconsciously, we set boundaries in order to protect our territory / personal space; this may be manifested by a sign on a door or even a gesture, a word or a facial expression.

So far, the aforementioned facts are well accepted; however, they pertain more to the physical space. It seems that in the digital space, protecting one's privacy and personal data are much more complicated than shrugging off an undesirable touch. Without underestimating the already complicated nature of privacy, personal space and personal data in the physical space, it seems however that it gets even more complex in the digital space. It has already been mentioned that in such an environment, there are many serious new challenges and considerations with regard to privacy and protection of personal data, which only seem to increase as we proceed towards a more digitised and technologically sophisticated 'smart' environment. It seems that using the notions of territories and personal space in the case of digital world, may provide us with a better way to map out and conceive the personal space and the management of personal data and privacy in the new digital world. The need for such an attempt is further analysed in section 4 of this report.

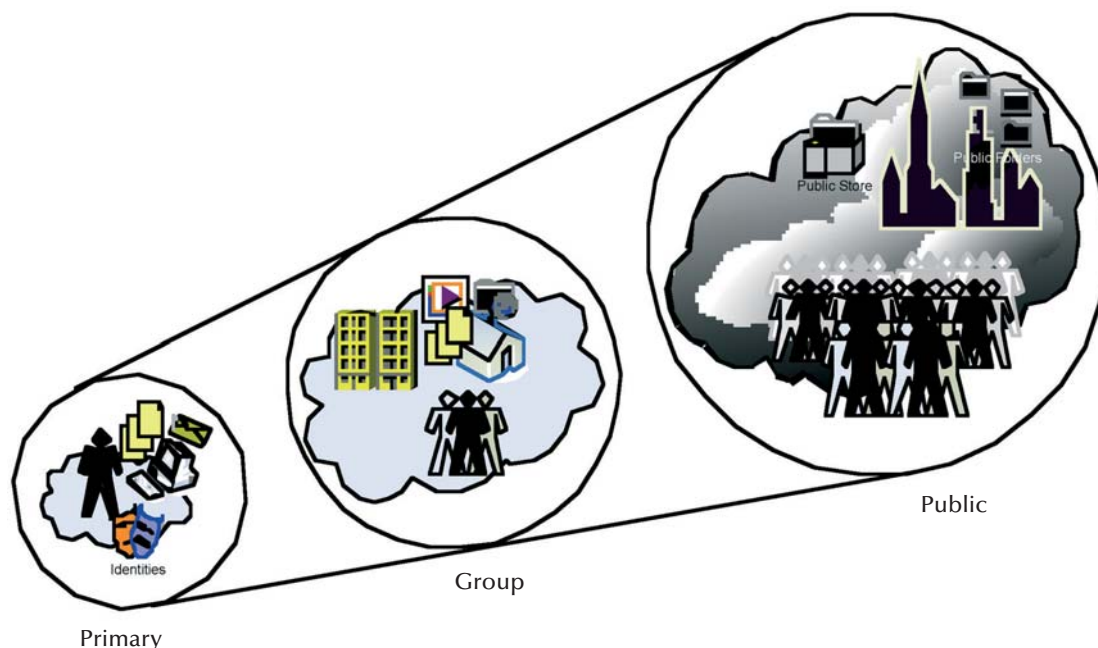
In the framework of our study on the Digital Territories (DT) concept, we have identified three types of Digital Territories, as well as four basic components, which are further analysed in the sections that follow. Also, more information on the DT components may be found in Annex I.

## 2.1. Types of DT

Based on Altman's approach regarding territoriality and personal space in the physical world, we have identified three major types of digital territories: *Primary* or *personal*, *secondary* or *group* and *public*. The distinction among these types of territories was based on (1) the degree of control

and use that its owners should have, (2) relative duration of owners' claims to the space and (3) considering the other two criteria, the number of individuals that would be able to exert control over the DT. The three types / dimensions are depicted in Figure 1 and a more detailed presentation of the three types follows in the paragraphs below.

■ Figure 1: The three types of DT



### 2.1.1. Primary or personal

In the physical world, personal space is literally 'attached' to the self [2]; it refers to an area, a 'breathing room' with invisible boundaries surrounding the person's body, separating him/her from others [2].

In the digital world, the primary digital territory (DT) regards a person's digital personal space; in this study, we consider the primary digital territory as a digital personal space.<sup>3</sup> As depicted in Figure 1, this digital personal space encompasses all the personal data of an individual in electronic (digital format), as well as the person's digital identities and 'on-line' activities. As such, the personal DT aims at achieving a desired level of privacy, while facilitating the performance of the required tasks. Within this 'space' the individual exercises

full control over his or her data and actively decides on who to grant access and to what part of the data ('partial e-identity'), e.g. different profiles for online banking, messaging or tax declaration or even when one creates more than one user profiles and appropriately configures one's home PC with an Internet connection (e.g. administrator, personal, guest-enabled user accounts).

### 2.1.2. Secondary or group

The secondary or group DT has elements of public access, considering that it is 'used' by two or more persons, but at the same time its owners enjoy a certain degree of control, however not to the same degree as over their personal DT [2]. This type of DT encompasses both the total and pervasive control allowed by participants in primary ter-

<sup>3</sup> In contrast to the physical space, where territory usually implies a fixed, geographically immobile region, whereas personal space is carried everywhere one goes [2].

ritories and the shared use of public territories allowed to all participants sharing the same 'space'. It basically relates to groups of individuals that share interests or purposes; hence we refer to it also as a group DT. A very characteristic example of this type of DT is the home, considering it in an Aml environment, where a family may share various physical access nodes, storage space, digital tools and where events may take place within a closed system. Another example, though with somewhat different features from the 'digital home', is the workplace environment. In this environment, there are well established rules that go beyond the *netiquette*<sup>4</sup> on the sharing of common resources; a collection of written and unwritten rules apply, which are very much dependent on culture, that shape behaviour, e.g. fraud may be interpreted differently as there is usually a collusive tendency on the part of the employees and / or the employers.

Basic DT components such as borders and markers (see 2.2.) can coincide with those of the personal DTs of the individuals that have formed this group DT. However, it is possible that borders overlap and may result in conflicts between the members of the group DT, as for example it may occur in a moderated online forum or list where a moderator has determined the netiquette but some members do not comply with it, or as well when the content of data are shared between two or more members. In case of potential conflict, solutions would be needed in order to resolve the issues and allow an agreeable relationship between them; the aim is to preserve the continuation of DT's existence for as long as it is considered necessary.

The duration of the group DT is not fixed; it varies from situation to situation and it basically depends on the type of common interests and purposes that have brought the individuals together. Considering a home environment: it may consist for example of a family of five members, namely the two parents, the two kids and a grandparent; a situation which may change, when the kids grow up and leave their family home or when the grandparent passes away. Friends of the family may also share this DT limited by time and cultural factors;

however, not all members share the same level of control or quantity of data exchange, as is the case for example with messenger contacts and use of Skype with videoconference facilities.

Also, in some cases of secondary or group DTs, an owner / moderator may be assigned, who will be responsible for moderating the DT. In an internet community for example, i.e. a private *blog* or other on-line forum, where people can log-in and express their opinion in the context of a discussion or want to request information about something, someone is defined as a moderator, the DT 'owner' being responsible for it, making sure that all participants abide by the community rules of conduct [6]. This can also be the case with a temporary DT that has to be identified in the event for example of a crime. The police while conducting an investigation on a committed crime would identify a secondary DT of a more temporary nature that would encompass the DTs of all the people involved in the crime scene, for which a police officer would be the responsible / owner. Also, typically restricted access web-sites are of this DT type.

### 2.1.3. Public

The third category of DT is an extension of the group DT and has the most temporary quality of the three; almost any individual has free access and a certain (mostly low level) degree of control to this DT. It is a kind of 'commons' in digital space, a free territory, open to society at large. In the physical world it could be for example a beach, a street or a park, while in the digital one, it could be a publicly available on-line / non-moderated forum, an on-line newspaper offering digital space for individuals' comments, a public web-page offering free open-source software to download or the publicly accessible zone of exhibition sites, where people provide comments on exhibits. It could also be identified as 'other than private and group', in the sense that whatever is not private or under other access restrictions, is public.

The duration of the public DT cannot be pre-defined and it varies. In the Internet there are still many public spaces with indefinite duration, i.e.

<sup>4</sup> 'Network etiquette', a catch-all term for the conventions of politeness and respect recognized on Usenet, in mailing lists, in live chat systems, and on other electronic forums such as Internet message boards (Wikipedia, available at: <http://en.wikipedia.org/wiki/Netiquette>)

all sites where access is not restricted through the use of any form of eID and where some level of interaction is allowed. However, market and technology forces are pushing towards the creation of 'privatised' spaces, where access is restricted and the actions and transactions of individuals are monitored [30]. The flow of information about personal movements and transactions in both the physical and digital world can result in a resource system that a number of organizations or individuals can 'appropriate' and use for their benefit. In response to such privatisation, there have already been made proposals in order to legally and/or technically create 'public spaces' on the Internet (Kline 1996; Gey 1998; Goldstone 1998) [30].

In such a public DT, the equivalent of open physical space, anonymity is sought in general. However, this is very difficult to achieve, all the more so in tomorrow's Aml world, since profiling would render anonymity almost impossible. It is thus necessary to establish roles and guidelines that would allow profiling in public DTs, while at the same time protecting the deserved privacy of the individual.

Towards this direction, the public DT is identified as an 'open' space that promotes freedom of expression, online collaboration and communication, extending 'the reach of an individual voice beyond that of what is possible in physical space' [30].

At this point it should be noted that the three DT types could coexist for the same service / application. Considering for example the case of YouTube,<sup>5</sup> every user has:

- a) His/her own primary DT, encompassing their personal information which they agreed to share when they signed up for a YouTube account, their uploaded videos and the information<sup>6</sup> that appears in their *Channel*.
- b) At the same time, a public DT may also be identified, when the users exercise their

rights and view the videos uploaded by other YouTube users (which have not been made private) even without having a YouTube account, i.e. anonymously.

- c) Finally, group DTs could be identified through the creation of *streams*<sup>7</sup> or the categorization of users into groups, according to the type of videos they upload.

## 2.2. Basic DT components

In the course of this study, we have identified four DT components that are necessary in order to enable a functional DT: bubbles, borders, markers and bridges are presented in the paragraphs that follow (for further information on each DT component, you can also refer to Annex I). Each DT type encompasses these four components; however certain differences may be noted in the specific function of these components in each DT dimension.

### 2.2.1. The bubble

The first component of the primary DT is the (digital) 'bubble', a dynamic personal info-sphere, or better data-sphere, since it basically 'holds' the person's personal data, and is used to setting the borders, restricting and / or allowing data / information coming in or going out of it. The bubble concept clusters together all the interfaces, formats, rights and agreements etc. needed for the management of personal data and informational interactions [2]. The size of the bubble may vary as a result of its information content, the form of interaction the individual wants to perform and the overall 'trust' assigned to the environment of the interaction. For example, when transacting in the framework of 'on-line' banking, using a secure line and data encryption, the bubble can grow as needed by the application, while when exchanging messages over a non-secure Bluetooth connection with a friend, it could be limited in size.

<sup>5</sup> YouTube allows people to easily upload and share video clips on [www.youtube.com](http://www.youtube.com) and across the Internet through websites, mobile devices, blogs, and email (<http://www.youtube.com/t/about>).

<sup>6</sup> This information refers to their profile showing their personal information, some of which may be considered private and made available only to certain users (e.g. identified as friends, family etc.)

<sup>7</sup> YouTube rooms created to interact with other users while sharing videos. Everyone who's part of each room can chat with each other in real time as the videos play and add videos from their Favorites, QuickList, or by pasting in links. Streams have two basic areas: the video (on the left) and the chat (on the right) (YouTube Help Center).



A bubble may contain current as well as past information related to its owner. For example, in a work environment it contains information specific to the various transactions that the owner has executed in the past. Moreover, the bubble actually generates and defines the boundaries / borders of DT (the second basic DT component, presented in the next section), in the sense that the borders are changed every time the bubble and its size changes to adapt to a new situation.

Using a cell-membrane analogy, the bubble has a two-way exchange with the environment – sometimes from the inside of the cell out to the environment and sometimes from the environment into the cell [2]. In this context it can be tuned to function differently depending on the following criteria / features:

**The direction of the movement of data:** *outward* and *inward* filtering. Outward filtering is based on which personal information (stored within the bubble), people want to or have to provide to external parties. The information flow towards the bubble (inward filtering) is controlled based on information needs and requests, and while negotiating the amount of personal information needed or assessing the trustworthiness of the counterpart; it also happens when bubbles ‘meet’, ‘touch’ or ‘overlap’ [6], which in the digital world means every time there is a request for information exchange.

**Classification of the personal data.** This is a procedure that most of us routinely use, which most of the times is done unconsciously and is not always structured that aims at protecting our privacy, according to our standards. In the context of the DT framework, this classification of data (whether of personal nature or not) stands in the centre of the bubble’s function, and promotes the awareness of people on performing this very important task. The categories that usually are used are the following:

- **Private:** data that is exclusively personal and we want it to remain so. The challenge here is that while in the physical world we understand the underlying mechanisms and can effectively protect ourselves, in the digital world, this is not so easy and this is the reason why phishing and pharming scams are so successful

- **Confidential / restricted:** data that could be shared with very few people or given to very few organisations, in order to receive a service
- **Public:** data which could be easier disclosed even to a public space

Such a classification is of course flexible, meaning that the classification types or criteria used may vary for each individual or external environment (e.g. security or privacy protection levels offered by the external environment, whether it is accessible by everyone, etc.).

**Time and spatial factors.** The filtering of data may vary also with time or space (physical and digital). Inward or outward filtering rules may change for example when an individual is using his personal PC or a public one (e.g. in the Internet café), or when he or she is using an instant messenger or an open-to-the-public blog.

While chatting in an Instant Messenger, we can filter our incoming requests for communication, by rejecting contacts by strangers, while accepting invitation to ‘talk’ with friends; in both cases, we have complete control over our bubble, but we adapt our bubble differently according to our preferences. It is thus evident that the bubble can be used to filter and select data, according to our wishes and reactions to external stimuli. It may also be intelligent in the sense that it may decide on our behalf based on these pre-defined preferences.

### 2.2.2. Borders and markers

The borders of a DT allow it to have an end and a beginning; they are seamless, fictitious lines that draw its perimeter, implementing the permissions set through the bubble. Therefore, these borders are always under negotiation and they adapt to different situation or spaces. As in physical space, the borders of a DT convey the idea of ownership of a place [2]; controlling of these borders is essential in the process of personalisation. When they are crossed, normally people will experience an invasion of privacy [25], feeling that their control over their interaction with the external environment is inadequate [2].

As already mentioned in the previous paragraph, the borders are not autonomous but are set

by the bubble; they thus change, decrease or increase, according to the 'will' of the bubble, and the boundaries that it wishes to set. Moreover, as bubbles may 'meet', 'touch' or 'overlap', the borders may shift or blur to adapt to the new environment.

The way of expressing and making boundaries visible is setting **markers**. In the physical world a marker would be the 'Keep Out!' sign placed in one's garden, informing other people that this is a private space where trespassing is not permitted and where it may be even legally prosecuted, e.g. common in the United States, even if no fence has been built around the garden. In digital space, it could be the log-in screens for accessing one's personal computer or it could be the 'private' tag put in one's folder. It is also the ability to turn-on or off the Bluetooth connection of one's mobile or the 'killing' or 'putting to sleep' of an RFID sensor. It is however currently most of the times difficult for individuals to put markers in their everyday communications and activities in the digital space. They more or less rely on markers and other relevant protective measures set by private companies and organisations' (e.g. the log-in required to enter to someone's profile in an online store or application). In this case, 'privacy by design' and 'Privacy Enhancing Technologies' take up a new meaning, since it is the choices given by the software that determine the control exercised over the outcome of the process. It is thus very important to think of the code, the technology that facilitates selection as a regulatory instrument.

### 2.2.3. Bridges

The bridge is the fourth component of a DT; however, it is not always brought into the definition of DT, as it is a component of a rather different and more complicated nature. Basically, it differs from the other components in the sense that

it is not a component per se, but it provides the link between the physical and digital / virtual world. For example, a bridge can be an RFID tag, which contains a link to information about the object that embeds it, thus providing a link between a physical entity (object) and its virtual history and 'bridging' in a way the physical and the digital world.<sup>8</sup> With the advent of more advanced technologies, bridges are of course expected to become more sophisticated, for example through the introduction of sensors in the home environment. Bridges introduce new ways of storing and accessing related information and thus have implications on the function of the bubble.

Since today the difference between digital and physical spaces is more or less clear, its importance as a component of a DT may not be quite apparent. However, as the boundaries between these two worlds become blurrier with the development of new technologies, in a future Aml environment the concept of the bridge will become increasingly important and will play an important role in the identification of the personal data-space and the drawing of the DT boundaries. Bridges are expected to have a considerable impact especially on our perceptions of both physical and digital space; they allow a brief or not so brief 'cross-over' to digital space, and in an Aml environment these transitions would happen automatically and subconsciously. It is also important to mention here that in such a world, the concept of DT will be more holistic in nature, encompassing data and other information not only of the digital space but from the physical space as well.

As the infrastructure becomes of 'age' and information as a resource is increasingly more valuable, our information needs in the physical world combined with always-on, seamlessly communicating networked devices will increase enormously, rendering the understanding, building and crossing of bridges more important.

<sup>8</sup> An example of bridging that has already raised considerable concerns is the broadcasting of advertisements to all mobile phones that are in range – identified through mobile technology location-based services. A more futuristic example is the one described by Hollywood movie 'Minority Report' where the lead actor is automatically identified and targeted with advertising as he enters a shopping mall.

### ■ 3. A special case – the virtual residence

Aml space is foreseen to require a high degree of surveillance and profiling data, in order to function properly, so as to offer high quality and personalised services to the citizens. On the other hand, this increased surveillance raises many concerns, from violations of privacy to feelings of frustration and anxiety experienced by individuals. In physical space, the home is conceived as a private place, a protected sphere delimited by the walls of a physical house meant to protect the family from outside threats and where individuals want to feel completely relaxed and comfortable. Is there a digital equivalent of the house so that our data can reside in relative safety with the maximum convenience in managing them possible? A photo album kept in a cupboard of our living-room is supposed to be only viewable by the members of the household, including the friends and relations that may see it. A digital family photo album however, sometimes available and even searchable over the Internet usually is not equally well protected; a good example is the case of *mySpace.com* presented in more detail in section 4.3.1.2, or that of *Flickr* ([www.flickr.com](http://www.flickr.com)) and *YouTube* ([www.youtube.com](http://www.youtube.com)), Web2.0 applications which allow for online storing, sorting, sharing but most importantly searching of photos and videos.<sup>9</sup> To the same effect, a not well configured Google desktop (see also section 4.3.1.1) on the Personal Computer at home, may result to the disclosure of private family data to the public or unauthorised individuals. In addition to these concerns, the idea of being surrounded by devices and sensors that would constantly monitor most of the individuals' movements or actions within their own personal sanctuary would not be very welcome; to be more specific, what will not be welcome is the risk that the data of all the home sensors may be compromised and / or abused, since the existence of this data would be indispen-

sable in order for the Aml devices to function properly.

IPTS has initially coined the concept of Virtual Residence (VR)<sup>10</sup> aiming at raising awareness on such concerns over security, privacy and identity of living and working in a future Information Society in Europe inspired by the vision of Ambient Intelligence. The term 'virtual residence' basically projects the concept of a protected 'residence' in the on-line, digital world; this protection could be either legal or in the form of social norms and 'netiquette'. It is an attempt to identify alternative legislation to protect data of a personal nature, exactly as it is protected in our physical homes now. It relates to the individuals' lives and the personal data stored at home, which at times need to be remotely accessible from the digital world. In this context, VR is considered a DT; it is categorised as a secondary or group DT, and is made up by the integrated DTs of the 'home' residents who take turns in managing the 'family' data, since in many cases more than one persons share the same physical infrastructures. In the case for example of a single-person household, VR may fall into the first type of DT, namely the primary DT. It thus constitutes a first clear example of territory (physical and digital) that requires regulatory protection.

VR is considered a special DT case and has been studied separately.<sup>11</sup> The VR provides the opportunity of encompassing all the personal and family data, from family photos and videos to recipes and other documentation etc. This information, whether located in personal computers inside the physical house or in public servers, should be considered private and be adequately protected. As our lives, homes, cars, neighbourhoods, cities and other environments become increasingly digitized and connected, the information that will

<sup>9</sup> On-line services such as Flickr, mySpace and YouTube have known huge success over the past few years. They provide a space where people can easily exchange information and share photos, videos, interests with other people, facilitating the on-line communication and making it more fun; and all that normally at no additional charge (apart from the fixed cost of Internet access and adequate equipment), in terms of money.

<sup>10</sup> The publication where the term was coined: Beslay, L. & Punie, Y. (2002), 'The virtual residence: Identity, privacy and security', The IPTS Report, Special Issue on Identity and Privacy, No. 67, September 2002, 17-23

<sup>11</sup> For further information on VR, you can also refer to IPTS' special report on VR in Annex I of this report.

be gathered, and stored would regard not only basic personal identification data such as age, sex and location, but also information on personal events (past and current), working documents, family albums (pictures, video, chat) and even shopping preferences, and medical and financial records.

Three basic elements / dimensions of VR are identified and are presented in the paragraphs that follow. It should be noted however that since VR is a type of DT, these elements / dimensions and their analysis pertain also to the general discussion on DTs.

### 3.1. Smart home

The increasingly connected home of the ‘future’ and its domestic infrastructures are one of the ‘nodes’ in the network(ed) society. The smart home of the future would among other things contain many sensors embedded in the home environment and in home objects. These tiny sensors will be connected in sensor networks which would be able to monitor everyday activities in ways that are completely invisible<sup>12</sup> to the people being monitored; which should be performed only under user consent, otherwise it is illegal (e.g. spying on the nanny of one’s kids when not at home is illegal, although it has been noticed that many people do it anyway). The potential risks of privacy invasive monitoring and surveillance are many. However, for every sensor, a different debate should be held – as argued by researchers involved in the US based Georgia Tech Aware Home<sup>13</sup> – on where (and where not) to install a sensor in the smart home, and for what purpose the sensor information can or cannot be used. There are sensors that may be used to detect physical activity (e.g. a person entering a room, a temperature change, an object being moved) and which therefore do not necessarily collect personal information. Sensors can also safeguard privacy through anonymity but coupled with other data, especially identification data (e.g. video camera) they may become privacy

invasive (e.g. identifying and storing who moved the object).

Natural borders could easily be crossed in the smart home where rooms are equipped with sensors. Other people are able to know – remotely, if they wish – who is in the home, in which room, with whom (other inhabitants and/or visitors), at what time, and also, maybe, what one is doing. It is easy to argue that people can opt out by not installing, activating or using these features, but the situation is more complicated since services are expected to provide added value. For example, monitoring the most private spaces of the home such as the bathroom might even be worthwhile, for medical purposes such as preventive medical care for the elderly. Also in the case of parental control, when parents are able to view and control their children’s movements and actions physically within the house, as well as their children’s online activities in the digital space; the risk here is that the data collected and used to the benefit of the individual, who happily grants agreement, are corrupted or abused by an outside attacker.

It is argued that in physical space, boundaries of the home environment should not only provide appropriate protection from the outside world, but also within the home environment; physical boundaries and access options should be established among family members as well, allowing them to come together or not, depending on the circumstances [2]). This is also a consideration in digital space, where the digital borders would have to be set in such a way as to facilitate interaction and appropriate control, whereas at the same time respecting individuals’ privacy levels, as for example in the case of parents protecting their office from their kids sneaking into it, or the worried father reading his child’s diary, in order to identify any possible danger his child might be running.

However, the increasing need for mobility and remote access to data coupled with the new wireless technologies that facilitate such access,

<sup>12</sup> A fundamental characteristic of Aml is indeed that computing capabilities move to the background and become invisible, hence R&D programs such as ‘the disappearing computer’, an EU funded activity in Future and Emerging Technologies (FET) of the IST research program. <http://www.disappearing-computer.net>

<sup>13</sup> Gooley, C. & Saponas, T. (n.d.) Privacy issues of the Aware Home. Paper on the Georgia Tech Aware Home project. <http://www.thegooley.com>; See also <http://www.awarehome.gatech.edu>.



have 'extended' the home environment outside its visible physical borders, making it mobile and 'always-on'.

### 3.2. Mobility

Just as the notion of legal and social protection of the physical residence has evolved to encompass other (mobile) spaces such as the car, and just as people move through time and space, so VR should be seen as a mobile and dynamic concept travelling through different Aml environments (home, work, school, leisure, neighbourhood, city). The Aml space indicates a seamless connectivity and interoperability between these different environments [20]. This would mean that people can (and should be able to) access their virtual residence as a protected private space from any other protected public and private space. This follows the sociological trend, enabled by ICTs (e.g. mobile phones), of the blurring of traditionally distinct spheres of living (e.g. home and work), as for example in the case of a parent travelling for work, but being able to remotely access private data stored in his/her home PC at home over the Internet.

Mobility in Aml space not only implies the movement of people but also the movement of personal data in cyberspace via things such as caches, cookies, liquid software<sup>14</sup> and downloadable applications. Therefore, it seems to be necessary to envisage online extensions of the virtual private space that encompass intelligent agents. These agents move through time and cyberspace by 'encapsulating' personal data to carry out requests for their real life counterparts. Some intelligent agents, for example those used in online travel shopping, compare the discounted airfares offered by major airlines and are able to book them online, having received the users' consent. In order to find the best flight ticket corresponding to the user's specific criteria, the intelligent agent has to 'go' through numerous web sites comparing the user's personal data with the travelling information offered. This example illustrates how on-

line personal information belonging to someone's private space may spread around in online public spaces, without the owner knowing about it. It indicates also the blurring of boundaries between online public and private spaces in the future Aml space.

### 3.3. Online family life

'Online family life' concerns Internet activities that relate to living in a physical residence, i.e. the online lives of people, families, and households. In an intelligent home environment, more and more personal information will be gathered, stored and possibly accessed by or disclosed to third party sources, service-providers, institutions and/or other people. This information encompasses not only basic personal identification data such as age, sex and location but also information and content such as events information (past, current and future), working documents, family albums (pictures, video, chat) and even shopping, medical and financial records.

Standard Internet search facilities can today be used to gather information about where people live and work and what their interests are. This raises the question of whether personal information on the Internet is public, since the Internet is a public network [33].

There are possibilities for individuals to control or restrict the flow of personal information but the market in personal information tends to place the burden and cost of this on the citizen. Since information about people is a resource for organizations, they might collect as much as they can unless internal or external costs become too high. Organizations are unlikely to act unilaterally to make their practices less privacy invasive. Unless choices are easy, obvious and cheap, people will probably go with the default position and that is, in cyberspace, more likely to be privacy invasive [30]. As a result, the privacy level available online is less than that which is required by the norms of society and people's stated preferences [30].

<sup>14</sup> Liquid software is software that easily 'flows' from machine to machine. It is proposed as a new way of constructing computerized networked systems.



## ■ 4. Into perspective: why DT?

The DT concept has been coined for a purpose: in order to address the privacy, security and identity issues / concerns in a new reality. The presentation of the concept itself has preceded the justification of its development, because having first a basic understanding of what the concept entails, would make it easier to comprehend the necessity for its development; especially in the context of a future Aml environment. In the paragraphs that follow, we present in detail the background of this study, proposing the need for a new concept and finally showing why its use addresses serious challenges and may result to our benefit.

First, we will attempt to present briefly privacy and data protection considerations as these are widely accepted today, as well as in the near future. We would then present very briefly the main elements of the existing privacy protection framework to finally set the scene for the DT concept and in what way it could be used to improve on the current situation.

### 4.1. Privacy and data protection considerations in the digital and Aml environment

Extensive research and studies have been devoted to privacy during the last thirty years. Privacy may be defined in terms of the physical distance from others; it is an iterative, ever-changing 'boundary-regulation process in which a person or a group sometimes wants to be separated from others and sometimes wants to be in contact with others' [2]. In this context, it is basically a dialectic process in the sense that forces to co-exist with others and forces to be left on your own are simultaneously present, with one force dominating at one time and the other being stronger at an-

other [2]. During the last century we have witnessed a change in society with respect to privacy. From the village situation where society was open / transparent, where everyone knew everything about everyone else (not much space for privacy), to the city situation where no one knows anymore who one's neighbour is.<sup>15</sup> Society has managed successfully this change and it is part of the basic know-how we have on managing our privacy. At the same time, other forces, such as social norms, state enforced regulations, also act on the individuals' privacy. In order to achieve the desired level of privacy, which is highly dynamic, a balance between all forces present has to be reached. In the physical world, people have acquired over the years the knowledge to perform such a process.

The notion of privacy is unstable, complex and difficult to describe [1]. The expectation of privacy differs for each stakeholder (individuals, governments and private industry), as well as according to age, gender, culture, location, family history, income, educational level and many other factors [17]. Moreover, privacy is usually tied up to the private or individual good, while its value for the 'common good' has received somewhat less attention<sup>16</sup> [30].

In the context of the rapid technological developments and the advent of the Information Society, new issues regarding privacy have emerged. It seems that privacy in the digital world is far easier to be violated and far more difficult to be protected, as we leave 'digital' traces when surfing. The default in cyberspace is more likely to be privacy invasive [30], thus always requiring appropriate action from the user. Consider for example when upon installing a programme or signing-up for an on-line service, you are automatically subscribed to newsletters or services, and you are then informed that you should go to the respective web-

<sup>15</sup> There are closed societies and tribes e.g. in Africa or Latin America, where people's everyday life and whereabouts are known to everyone else in the village [7]. This however has changed their perception of privacy in their cultures, and they have adjusted their social behaviour accordingly.

<sup>16</sup> According to Regan (2002), privacy encompasses the following three values: (a) **Common value** – all individuals value some degree of privacy and have some common perceptions about privacy, (b) **Public value** – it has a value not just to the individual as an individual or to all individuals in common but also to the democratic political system and (c) **Collective value** – technology and market forces are making it hard for any person to have privacy without all persons having a similar minimum level of privacy.

site and request to be unsubscribed. The opt-out possibility is thus most of the times made more difficult and requires extra effort on the part of the user, as well as technical knowledge in most of the cases. To make matters worse, the user is often not aware of the amount and the type of information (e.g. IP address, cookies, web-tracking, cache, search terms etc.) that is captured as one surfs the net or performing other online activities, thus making it more difficult to opt-out or to protect one's privacy.

Further analysis is based on the identification of the major threats to privacy and the agents of these threats. The threats are mostly generated as a result of a conflict of interests, because of different expectations and requirements of privacy among all stakeholders (governments, citizens, industry):

- **Government, state and law enforcement agencies:** Governments collect, process and store significant amounts of citizens' personal data and also monitor and survey their citizens. Their basic motivation has to do with tackling tax evasion or providing better public services, but basically to provide national security and protect the country and the citizens from potential external and internal threats. As Regan (2002) puts it, the risk society requires surveillance as a way of managing risk [30]; however, surveillance requires increasing information so as to minimise risks that exist generally or which are posed by particular individuals. Nevertheless, the knowledge produced by the surveillance systems sometimes produces new uncertainties leading to more surveillance and collection of more information [30]. Often security measures were proven to be rather ineffective<sup>17</sup> and citizens have a perception of security that is not aligned with the enforced security protection they benefit from.
- **Private sector:** Companies and organizations need personal data, in order to be able to provide more personalised services to customers, as well as to deal with customer churn. They also require personal data, such as web-site

searches, visits etc. to determine customer's preferences and for profiling. Moreover, employers need to monitor and survey employees' activities in the workplace. Citizens are willing to part with their data, if they benefit from more personalised products; however, they feel betrayed when private entities misuse or abuse their personal data in order to gain profit.

- **Individuals:** A real threat is posed by malicious on-line users and crackers who want for example to abuse identity information and perform financial transactions on our name to their benefit. Citizens feel extremely vulnerable to such attacks all the more so as there is no one willing to take responsibility as to the outcome, since it is rather difficult to enforce liability. Taking this to an extreme, even we sometimes become a threat agent when we agree to sacrifice our privacy in return for receiving better service or other provision, either because we are not aware of the risks or we simply are given no other choice. It is also possible that people would willingly do with less privacy, either because the concept of privacy is changing or because they voluntarily want to share their private data or files ('user-generated content'<sup>18</sup>) with other users or friends in an on-line service, such as YouTube, MySpace.com etc.

The potential advent of the Aml environment renders data protection and privacy issues even more difficult to address. The collection, storage and exchange of personal data are a requirement for such an environment to function properly, which will lead to more 'profiling', a practice which is inherent to Aml [1]. Moreover, it is expected that people will be under constant surveillance ('transparent'), which is a prerequisite in Aml, as the monitoring and surveillance capabilities of new technologies may be massively extended.

In addition, a very important challenge that Aml presents regarding privacy and data protection is the identification of what to protect, namely which data or information is qualified as personal and has to be adequately protected as such and

<sup>17</sup> A very typical example of this, is that increasing the street light intensity is a more effective measure than the 4 million closed-circuit cameras (CCTVs) in operation in London, monitoring a typical London resident around 300 times a day [21].

<sup>18</sup> User-generated content refers to various kinds of media content that is produced or primarily influenced by end-users; as opposed to traditional media producers, licensed broadcasters, and production companies ([http://en.wikipedia.org/wiki/User-generated\\_content](http://en.wikipedia.org/wiki/User-generated_content)).

which is public and may be disclosed. The distinction between the two areas, public and private, is becoming increasingly complicated and the borders between the two will only get more difficult to define, especially since there are many grey areas between the two. A characteristic example of blurred boundaries between online public and private spaces in the future Aml space is that of 'intelligent agents', which 'encapsulate' personal data to carry out requests for their real life counterparts, such as in the case of online travel shopping, where the intelligent agent has to 'go' through numerous web sites comparing the user's preferences with the travelling information offered.

## 4.2. Privacy protection laws, regulations and standards exist and are in effect

As more personal data are being collected, stored and processed, with or sometimes without our knowledge and/or consent, there is more pressure to share this information. Such problems are well-known and the current legislative framework is providing a certain level of protection. However, emerging technologies may exacerbate the problems.

The right to protection of private life constitutes a relatively new concept in the development of contemporary law. Laws, regulations and international standards have been gradually established in order to regulate as much as possible these new issues, and protect personal data. The right to respect a person's family life is established in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Towards addressing more concretely the issues of data protection, the European Commission issued two Directives of crucial importance for the further development of data protection in Europe, namely Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data<sup>19</sup> and on the free movement of such data, and Directive 97/66/EC on privacy and electronic communications.

Every private company is required to have a privacy policy, and to maintain a personal data filing system; all persons are entitled to know what personal data are being kept in the systems of companies or government agencies. Most private companies that collect personal data are required to undergo compliance audits to ensure they comply with the current privacy regulations (e.g. Data Protection Acts) and security best practices.

However, data protection legislation does not distinguish between personal data that affects or does not affect private life. The central notion in this area of law is personal data, meaning any information relating to an identified or identifiable individual [9]. Data protection, although it recognises the existence of a special category of sensitive data, is built up on the idea that all data can be abused, including the more ordinary data, such as names and addresses. We may consider for example that while the processing of sensitive data about the ethnic / origin category of some people may be rightfully prohibited, the processing of a simple list of the names of these people that can also convey the same information as the sensitive data, is not equally restricted, since these data are considered ordinary.

Moreover, compliance with the regulatory regime often proves to be inadequate towards ensuring the protection of our privacy and personal data in the digital space, since often there is not enough transparency about the outcome of such activities. For example, despite the fact that companies and organisations are often required by law or regulations to perform compliance audits regarding data protection, in practice often there is no guarantee that such an audit has been performed thoroughly (or indeed at all) and its results are valid and reliable.

Current legislation about privacy and data protection cannot always keep up with rapid technological developments and social changes; it understandably lags behind and it takes more time for it to reflect these changes. In the meantime, there are bound to be issues and dimensions that remain rather elusive and are not covered by law.

<sup>19</sup> According to the Directive of the European Parliament and European Council 'On the protection of individuals with regard to the protection of personal data and on the free movement of such data' (1995), **personal data** means 'any information relating to an identified or identifiable natural person ('data subject')'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity' [11]



The increased digitisation of our lives, not only of our data, may not be fully reflected in the current privacy and data protection legislation. We are living in an Information Society, where 'being digital' is more than the mere electronic processing of personal data: it encompasses a distinct on-line life, a natural person having multiple different digital identities in the digital world. The proliferation of the amount of electronic personal data exchanged in this digital space, the nature of our digital activities and transactions online create many new challenges and considerations that are some times far more complicated to be appropriately addressed. For example, while searching for an article in Google, are the search terms used to be considered as data to be protected? Who is the actual owner of such personal data and should they be protected according to the data protection legislation or do they belong to Google which can dispose of them according to their will? Moreover, a growing number of emerging technologies, such as location-based services, third generation mobile telephones, closed circuit television (CCTV), biometrics, RFIDs etc. tend to establish links and bridges between a specific physical location and digitised knowledge and information [2]. With the diffusion of new technologies and the integration of Aml technology into everyday life, the boundaries between physical and digital space will become increasingly difficult to distinguish and may eventually disappear [6]. Considering all these issues, are the current privacy laws, regulations and international standards enough to protect the citizen's privacy and personal data in digital space as well? In what way can the framework be adequately modified to ensure the citizen's trust in the Information and Knowledge Society?

### 4.3. Enters DT...

In order to provide an answer to the questions raised at the end of the previous section (4.2), IPTS has engaged in related research and identified the need for a new approach and framework that would address these issues. What is at stake here is life in the future as everything indicates the convergence of physical and digital worlds into one. To this effect, the concept of DT provides a systematic and analytical framework towards defining the boundaries of personal and public digital space. The conceptual representation that could be made will

allow thinking beyond technical solutions [6]; it could then actually help address the challenging issues of privacy, security and identity. DT framework could provide answers to these questions, identifying the digital territories of the individuals, their private digital spaces to be protected. Once defined, they could be more efficiently protected, primarily, by enabling the definition and implementation of appropriate supporting legislation in combination with appropriate technological architecture.

Regan's (2002) assertion that privacy is not only of value to the individual but also to society in general [30] becomes a central idea in DT and its conception. It is widely acknowledged and recommended that in order to protect privacy, individuals should be given 'opt-out' alternatives. However, as we have argued elsewhere in this report, individuals are less likely to make choices towards protecting their privacy unless these choices are relatively easy to perform, obvious and low cost. What is the use of the possibility to unsubscribe from a service given to a basic user of PC and Internet, when he does not really understand what he is being informed about or how to perform the un-subscription? The company offering this service is legally 'covered' and complies with the laws and regulations of data protection; however, the level of privacy offered to this individual is insufficient. To quote Regan (2002), relying on individual decisions to protect privacy in a context where business logic pushes so aggressively to the opposite direction will result in less privacy than would be optimal from a collective standpoint [30].

Another factor to take into account is that not everything is privacy, not everything should be kept strictly private, limiting the ground of free expression, communication and creativity. As presented in chapter 2, we have identified three different dimensions of DT, in order to capture as many different aspects of the issue as possible; the first one pertains more to the personal space, closer to the individual and at the same time closer to the dominating perception of privacy, while the second and mostly the third one consider the more public aspect and common value of privacy, coupled with the consideration that 'public spaces' in the digital world should also be preserved and adequately protected. Further to this, we have introduced into this study the concept of 'commons' in the cyberspace. Internet zoning seems to be inevitable [22][30], in the sense that in the digital

space there are areas that are definitely more private than others, and some areas that are public. It is considered equally important to protect the 'openness' of these public places as to protect the private space and personal data of an individual.

Thus, DT could help reveal conflict situations and help raise consensus as to adequate sustainable solutions. The DT concept and especially its application will be better presented through specific examples; consequently, some DT examples have been developed to this effect and are presented in the following paragraphs. A number of questions that emerge are introduced and finally a synthesis section binds it all together and highlights the foreseen benefits.

#### 4.3.1. DT in Action I – the present: from simple Internet search to social networking and Web2.0

Up until some years ago, the average user used the Internet to find information or even perform the financial transactions; the first example of application of DT will be emerging Google services. However, recently, people use the Internet to socialise, communicate and collaborate with other people. Internet applications offering this possibility are known as online social networks and are becoming increasingly popular.<sup>20</sup> Also, far more sophisticated web applications have emerged, and many are talking about the advent of the Web2.0. platform, a concept initially coined by O'Reilly and MediaLive International in a conference brainstorming session in 2004 [29]. One of the most prominent issues regarding Web2.0 applications is that it facilitates users to share content (personal files, videos, music etc) with their family, friends and other people, nowadays referred to as 'user-generated content'. Based on the perception of privacy we had so far, it may seem that people are willing to 'settle' for less privacy; however, it may as well be that the privacy requirements of people have changed, and that the privacy concept needs to be revisited and redefined to match today's requirements. At any rate, in this case the DT concept could be suitable, since it allows users to decide whether to share their personal data and

files, and if yes with whom, through the classification process performed in the context of the bubble, as presented in paragraph 2.2.1 of this report.

In this context, social networking and the Web2.0 platform lie at the centre of today's digital life, and give rise to many identity and privacy considerations; hence they have been selected as characteristic and representative services for applying DT. Two more examples from this area of widely diffused services will be used to apply DT: namely MySpace and blogging. It should be noted however that the applications that have been selected as examples are indicative only and thus by no means exhaustive; there are certainly more applications or services that could provide good examples of application of DT.

##### 4.3.1.1. To Google or not to Google?

Google has built on top of its search engine, notably one of the more widely used, a variety of online services and applications. The *Google Desktop* solution is a value-added universal search utility, which enables an advanced 'Search Across Computers' feature to provide the users with the possibility to search their documents and view web pages across all their computers. The issue arising here is that according to Google's Desktop Privacy Policy, by enabling the advanced features of the product, information about the web-sites visited and other information (such as the number of searches one does and the time it takes to see the results) will be sent to Google.<sup>21</sup>

This feature of Google, although very useful to most users, poses a challenge when considering user-privacy protection, such that the Electronic Frontier Foundation (EFF) urges consumers not to use this feature. Assuming that Google is in a position to protect all the protected data from misuse, this feature will make their personal data more vulnerable to subpoenas from the government and possibly private litigants. In case Google is unable to secure this information, it will expose them to unauthorised access by crackers and/or other malicious users who have been able to obtain a user's Google password [3].

<sup>20</sup> [http://en.wikipedia.org/wiki/Social\\_network#Internet\\_social\\_networks](http://en.wikipedia.org/wiki/Social_network#Internet_social_networks)

<sup>21</sup> Google's Privacy Policy available at: <http://desktop.google.com/privacypolicy.html>

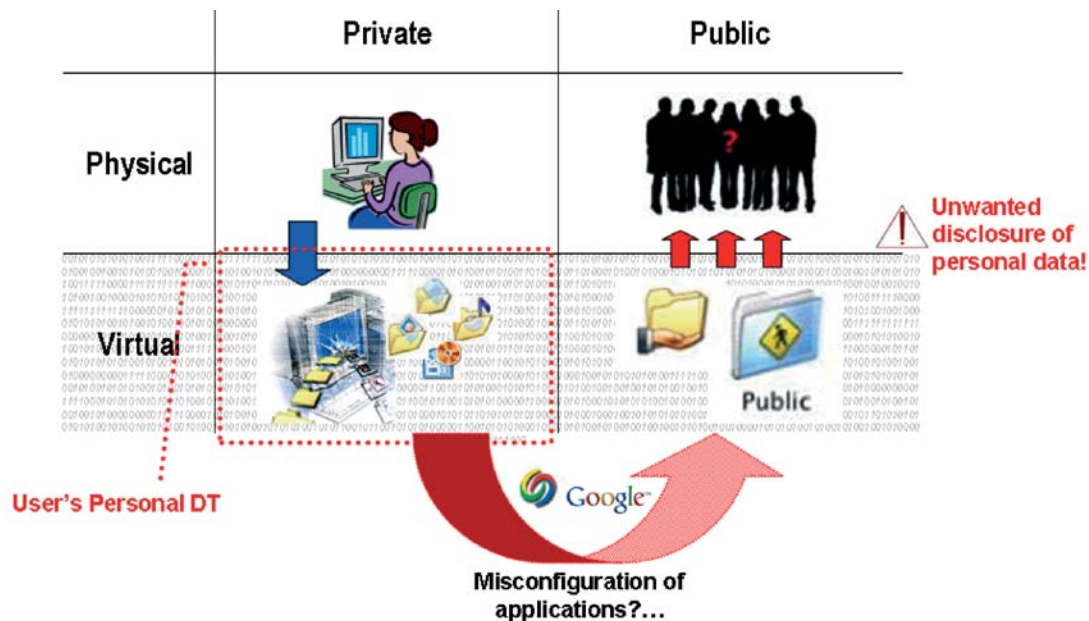
Also, given the recent US Department of Justice's subpoena to Google, it seems that it will not be very long since the entire search history of an individual, since it is being stored in Google<sup>22</sup> servers, will be subpoenaed by the police, lawyers or attorneys to be used as evidence in the court of law. For example, this information apparently has been used quite recently as evidence to convict a man in North Carolina in November 2005; apparently, the search terms 'neck', 'snap', 'break' and 'hold' were found in his computer search history, terms which it seems he had searched for in Google before his wife was killed [26]. The main issue here is that data collected by Google may be used for purposes other than the original ones, e.g. leading to conclusions or incriminating someone without having further evidence.

The user's files (documents, photos, videos etc.) are normally kept in the user's Personal Computer. The potential erroneous configuration of software utilities, such as in the case of Google Desktop, may allow this personal data, which in the physical space may be for example kept in a cupboard in a person's room, to be publicly disclosed and available to other (unauthorised) indi-

viduals in the digital space, through the Google servers and the Internet (See Figure 2).

The data that Google keeps are namely:<sup>23</sup> web requests, Internet Protocol address, browser type, browser language, the date and time of the user's request and one or more cookies that may uniquely identify the user's browser. Google asserts in its Privacy Policy that appropriate security measures are taken to protect against unauthorized access, alteration, disclosure or destruction of data. A number of questions emerge as to the degree the combination of security safeguards and privacy protection legislation is enough today and in the near future to provide efficient protection. Such questions are: Will users trust Google with their personal data, which would be stored in its publicly accessible servers? Are current technical security solutions (e.g. Virtual Private Networks, encryption, and security protocols), self-regulation guidelines or third-party attestations adequate in order to deserve user's trust? Under what conditions could we trust Google with our personal data, which would be stored in publicly accessible servers? Do end users have any control over their own personal data and should they?

■ Figure 2: DT – The Google example



<sup>22</sup> Preparing to defend a controversial Internet pornography law in court, the Justice Department has demanded search logs from Google, Microsoft, Yahoo and America Online. For more information: [http://news.com.com/FAQ+What+does+the+Google+subpoena+mean/2100-1029\\_3-6029042.html?tag=nl](http://news.com.com/FAQ+What+does+the+Google+subpoena+mean/2100-1029_3-6029042.html?tag=nl)

<sup>23</sup> Google's Privacy Policy and Frequently Asked Questions available at: <http://www.google.com/privacypolicy.html> and [http://www.google.com/intl/en/privacy\\_faq.html](http://www.google.com/intl/en/privacy_faq.html)



Furthermore, there are many indications that future services would add even more to these considerations. Google, Inc. is speculating to offer a new service GDrive, which, if Google's present plans materialise, will offer an 'infinite storage' service, that 'will provide anyone (who trusts Google with their data) a universally accessible network share that will span across computers, operating systems and even devices' [13]. Such a service would of course facilitate a lot the data and information exchange and would be very convenient for the end-users. However, and despite this not being a reality yet, many issues and concerns are already raised especially with regard to the privacy and the security of the user's personal data. Considering the VR concept and the increased need for mobility, would it not be nice if the data in the GDrive were appropriately protected as if it was located in a server at home?

#### 4.3.1.2. MySpace.com

Not yet as widespread and famous as Google, however equally interesting is the case of MySpace.com, an online service that allows its members (and there are around 100 million of users<sup>24</sup>) to set up unique personal profiles that can be linked together supporting networks of friends. According to MySpace.com privacy policy, the information collected is user submitted, is compliant to data protection legislation (regarding information such as name, email address and age) and is used in order to authenticate users and to send notifications to those users relating to the MySpace.com service.<sup>25</sup>

It is apparent that MySpace.com has taken precautions towards ensuring its users' privacy: but is it enough? Especially considering that the information submitted by its users may be shared with third-parties to provide more relevant services and advertisements to members; user IP addresses are also recorded for security and monitoring purposes.<sup>26</sup> Even more interesting is that the disclosure of this information to third-parties may be

deemed necessary, in order to '(1) conform to legal requirements or to respond to a subpoena, search warrant or other legal process; or (2) enforce MySpace.com Terms of Use Agreement or to protect the company's rights; or (3) protect the safety of members of the public and users of the service.'<sup>27</sup> In this case, a user's personal data may be disclosed to third parties, without his knowledge and/or consent, since it is considered that he / she had already agreed to it, in order to use the services of mySpace.com.

#### 4.3.1.3. Blogs and Wikis

Other Web 2.0 hype applications are *blogs* and *wikis*. A *blog* is a personal home page in journal style, an online diary, to which people can invite their family, friends etc. to participate, sharing ideas, images, music, videos and more. A *wiki* is a type of Web site that allows the visitors themselves to easily add, remove, and otherwise edit and change some available content, typically without the need for registration [38]; it is thus considered a breakthrough in online collaborative authoring.

*Blogs* and *wikis* undoubtedly facilitate communication and collaboration between friends, peers or colleagues. It is foreseen that blog syndication may change the way traditional media exist today. Especially *wikis* promote the free expression and the development of open source and free software. A characteristic example is that of Madridpedia (<http://www.madridpedia.com/>) which aspires to be the main on-line point of reference for information on Madrid and all the Community of Madrid. *Wikis* but mostly *blogs* may contain personal data and information about an individual, which could be disclosed to unauthorised individuals, given the low levels of security and privacy protection implemented so far. *Blogs* and *wikis* are not considered most of the times an exclusively private space, as for example would be the Account Information space in an online store, which contains also financial details. They are private spaces, upon which individuals may exercise a

<sup>24</sup> According to Wikipedia, the 100 millionth account was created on the 9th of August 2006 ([http://en.wikipedia.org/wiki/MySpace#\\_note-MySpace100Millionth\\_Profile](http://en.wikipedia.org/wiki/MySpace#_note-MySpace100Millionth_Profile))

<sup>25</sup> MySpace.com also collects other profile data including but not limited to: personal interests, gender, age, education and occupation in order to assist users in finding and communicating with each other. MySpace.com also logs non-personally-identifiable information including IP address, profile information, aggregate user data, and browser type, from users and visitors to the site, in order to manage the website, track usage and improve the website services.

<sup>26</sup> Taken from MySpace.com Privacy Policy, available at: <http://collect.myspace.com/misc/privacy.html?z=1>

<sup>27</sup> Ibid.

certain amount of control; or they could be moderated spaces or even considered public spaces.

In this context, DT and its three types could be used to map and draw the boundaries, so as to protect the private space and data of an individual wherever this is appropriate; but also to allow for public interaction and exchange of ideas, by maintaining the 'openness' of public spaces, supporting freedom of expression and adequately protecting these spaces. As already stated in Chapter 2, the DT concept aims at offering a more comprehensive protection: it considers personal and public spaces, as well as spaces that have both personal and public elements, including data that are neither private nor public.

From the previous examples, it is clear that current applications raise many considerations and pose new challenges. The future, especially when considering an Aml environment, seems to raise even more concerns, more complex and difficult to address. In the following section, an example of a possible future application is provided, namely the RFID implants, which has already started to be implemented experimentally in certain cases.

#### 4.3.2. DT in action II – the future: RFID implants

Just like surgery has expanded from a pure health environment to other domains to contribute to aesthetics and well-being, implants are likely to be employed beyond the pure medical area. Some implants may soon leave the arena of helping impairments, towards compensating for natural decline of senses or even to enhance human capabilities. In this dynamic environment, implants may merge with sensors or actuators, which are currently not employed for humans. In October 2004 the first RFID implant, called VeriChip,<sup>28</sup> obtained approval for medical use from US Food and Drug Administration. It operates at a low frequency (134.2 kHz), it can be read from 3 inches (7,6 cm) [34] and contains only a unique identification number. Any other information about a person is not stored in the implant itself, but in a

centralized database, from where personal information can be retrieved using as a key the user's ID number.

A prime application of VeriChip is in the health care area, the so-called VeriMed system.<sup>29</sup> This RFID implant offers a unique identification number to every patient and is apparently enjoying the rapid adoption of a number of hospitals [35]. In addition to this commercial product, some people have non-FDA approved devices implanted. For these implants, RFID tags are used which were originally manufactured for industry or supply chain purposes. For example, Kevin Warwick, a professor of cybernetics at the University of Reading, has implanted an RFID chip that allows a computer to detect his presence in the workplace (Department of Cybernetics at the University of Reading) and automatically opens a door, switches on and off the lights, heaters and computers<sup>30</sup> [32]. However, RFID implants have been also commercially used for fun purposes, as in the case of the Baja Beach club in Barcelona ([www.bajabeach.es](http://www.bajabeach.es)), which provides its VIP clients with the opportunity to implant themselves, in order to enter the club without any identification, get access to the VIP special area of the club and without having to carry any cash for paying.

Serious social, privacy and ethical concerns have already been raised with regard to the use of RFID implants for the identification and authentication of people. Especially with regard to privacy, RFID implants may pose serious risks, since they permit easy and instantaneous identification and authentication of individuals, often unbeknownst to them. Tracking of people thus becomes easier and in the context of an Aml environment with increased surveillance and profiling requirements, it may result in the Orwellian prophecies becoming a reality. However, in some cases implants may provide the appropriate level of security protection when for example, parents are implanting their kids with RFID chips in order to be able to track them down easily in case of abduction.

A number of questions again emerge, such as: Are the data inside the RFID chip personal data? Are there any specific requirements to be set re-

<sup>28</sup> VeriChip is produced by American company with the same name (subsidiary of Applied Digital), [www.verichipcorp.com](http://www.verichipcorp.com). VeriMed is a name of system for patient identification based on VeriChip.

<sup>29</sup> Website of VeriMed system is available at: [www.verimedinfo.com](http://www.verimedinfo.com). The site provides description of system, demo and is used to login for patients and physicals.

<sup>30</sup> *What happens when a man is merged with a computer?* Available at Kevin Warwick web-site: <http://www.kevinwarwick.com/Cyborg1.htm>

garding the protection of these data? When is it considered that the protection of these data has been violated? These are only a few of the questions / considerations that begin to arise with the introduction of this technology. DT's role in this particular example would be initially to define the individual's primary DT, identifying the borders and classifying the data and the identity that constitutes the 'digital bubble'. The classification of this data will then determine the protective measures that need to be taken, and under what circumstances this protection may be lowered, so as to allow law enforcement to act

#### 4.4. Synthesis

Considering all the above analysis and the examples, we have identified basic uses of DT and in brief the benefits that all stakeholders (individuals, state / government and industry) may expect from its implementation. We will now attempt to justify the need for further development of DTs.

To begin with, the DT concept provides a more systematic way to conceptually represent data and information flows, user consent, as well as borders between private / public spaces and their 'grey' areas in between. In this respect, it could be argued that an individual's personal information or data in electronic format stored either in the person's personal computer or public servers, falls within the user's personal DT, and should be classified, controlled and protected accordingly. Of course as it is noted elsewhere, it is not that simple and straightforward to identify these boundaries; it is exactly because of that, that DT concept is dynamic and flexible, providing at the same time a systematic and analytical tool towards defining these boundaries. Once personal data and digital identities in digital space are identified in the DT, it is then easier to classify personal data. The classification of data is a very important practice, since it provides a first step for risk management, and thus enables appropriate management of data and identification of possible risks regarding this data. It is then easier and more efficient to identify possible controls to address the risks.

In this context and having defined more or less the boundaries and identified the personal data and identities to be protected, a conceptual representation could be made that will allow

thinking beyond technological solutions; it could then actually help addressing the serious considerations of privacy, security and identity. What should privacy laws protect? Do the data threads left at our ISPs' servers or the search terms used during a Google search constitute our personal data and thus should they be protected? The DT framework could address these questions, identifying the digital territories of the individuals, their private digital spaces to be protected thus assisting towards appropriately supplementing the current legislation on privacy and data protection. In this context, DT can also be used to help make better laws and also assist in enforcing these laws. Given that personal data are sufficiently mapped, thus knowing what and how to protect, it is perhaps easier and more efficient for related laws and regulations to be developed based on that information.

Moreover, notions of legitimate or reasonable expectations of privacy basically turn on two criteria: individuals conveying a sense that they expect privacy, and society recognising the individuals' right to privacy [30]. However, the first criterion requires knowledgeable individuals or at least individuals that are aware of the privacy and security risks that their every-day digital life would entail. DT could assist in promoting this awareness, so that individuals could then know what they should try to protect and what they do not need or cannot protect. It could also enhance users' awareness regarding the security practices that they would have to follow themselves in order to protect their data.

Society can be as secure as its weakest link; often proved to be the human element. Without the security awareness of people, IT security or indeed Privacy Enhancing Technologies (PET) could not possibly provide the full level of protection needed (as in the example of a user who does not understand what it means to unsubscribe from an 'on-line' service, or even how to proceed with it). By implementing DT, people may become more aware of the risks and thus 'advanced' users of the new technologies, taking advantage of the additional opportunities that are currently being offered by these new technologies. It is noted however that the most important factors towards enhancing people's awareness on these issues is education and digital literacy, without which it will not be possible to achieve such an objective.

With regard to the use of surveillance and its social implications, the setting of boundaries in the digital sphere would provide a basis for consensual resolution. Spying physically into someone's everyday activities and/or house is considered at least inappropriate and annoying, and most people would feel scared, angry and would sooner or later somehow express their objections to it. Unfortunately, the same situation on the Net is not treated likewise. For one thing, as mentioned before, in the digital world, there are no markers or social norms that would assist Internet users in distinguishing between private and public space; in addition, an average user does not even realise when he/she is being spied upon, either because of his/her ignorance (low level of digital literacy and relevant knowledge) or lack of appropriate transparency in software utilities and applications, that often do not provide any information on the specific actions a program or Internet application performs. Electronic shadowing has become a serious issue, making the traceability of our everyday activity easier: GPS tracking, CCTVs, RFID technology, localisation through mobile telephones recorded at telecommunication companies and credit card payments in various shops, are only a few examples of technologies that can be used to this effect. Nowadays every citizen is recorded into approximately 500 files, and while it is advocated that all these quite invasive monitoring activities are done to the benefit of the larger community (i.e. localisation of criminals or terrorists or even personalisation of services), they may easily be (and often are) misused [26]. Moreover, the ability to link all this data into a single picture of our everyday activities on-line and off-line, only makes matters worse.

In this context, DT could also be used in the development of specific security software, appropriately alerting the user of potential monitoring actions. The operating rules should be open, transparent and well understood by everybody without the presence of hidden solutions that people are unaware of which are or out of their control [26]. It could be also argued that proper legislation could be put in place, stimulating software companies to disclose all actions that their software applications perform on the users' computers; the latter is also a requirement for effective multi-lateral security.

Moreover, DT could be used in the development of Aml products or services to enhance the

offered level of security and privacy to the benefit of suppliers, as well as end users. Security and privacy requirements could be considered from the initial development phase ('privacy by design'); thus fully integrating them into the product or solution under development, instead of adopting corrective and probably not very effective measures *a posteriori*, when the first problems would have already begun to appear [6], as a matter of precaution in every situation.

Another use of DT is obvious when considering the special case of VR. In the VR, the challenges emerge both inside the 'Smart Home' environment and outside of it and threats could come from 'friends' as well as 'foes': the typical power struggle among family members is on the one hand supported by emerging surveillance technologies (parents surveying their kids or their baby-sitter), but on the other hand it is also prone to abuse (which may be also facilitated by technology) by allowing third parties to make use of collected material in unforeseen ways, for example, when attacking the common infrastructure through its weakest link. At the same time, the mobility induced requirements of the residents raise questions as to whether the home infrastructure can be 'kept' safe and secure within the legally protected physical walls of the 'smart home'. As a result, more issues emerge that require applying a DT model to ensure the necessary level of protection for lowering the barriers towards adopting a digital life style. Moreover, VR could be a priority to address since current applications put additional pressure on taking relevant action and the issues posed are earlier and easier perceived by the individuals. Besides, it may be easier to solve as the existing legislation regarding the protection of the physical residence is more explicit (the borders and markers of the different DTs (personal or group) could be easier to define in the context of the residence. As such, VR could very well become the first application of DT. However, it should be noted that it will not be until the application of DT to public spaces bears fruit that the real benefits from DT could be appreciated.

A summary of all the aforementioned uses and benefits of DT that we have identified in relation to each stakeholder: individuals, industry / market and governments / state is presented below:



**Individuals** – Obviously, the identification of personal data and identities in the digital space that should be appropriately protected is very important for individuals, keeping them informed and aware of what they need to protect and also helping them understand the operation of the digital space better. The identification of group DTs provides many benefits as to data management in a space as VR for example, while the identification of public DTs, promotes collaboration between individuals and provides room for free expression and creativity. In this context, intervals will have a clearer picture of what to expect in terms of privacy and personal data in the digital space and to know when their privacy is being violated and when to respect another individual's personal space.

**Market / industry** – By all means, the concept of DT is very focused on the welfare of individuals and their protection from possible violations of their privacy in the digital space. However, it is considered that the protection of personal data and privacy could become easier for Industry as the DT concept has been developed to be implemented also by industry. Companies may use DT in order to include the privacy requirements in the development of their software ('privacy by design'), thus rendering their products more at-

tractive and easier to use with confidence. Moreover, companies may use DTs when developing their security management documentation (security policy, standards and procedures) or their privacy policy, to comply with privacy and data protection regulations. Specific seals could be used to signal compliance. It could also help them to define better policies in the workplace, respecting the employees' right to privacy, while securing their business.

**Government / state** – The importance of the role of government / state in privacy and data protection has been advocated for years now. As mentioned in the benefits above, the DT concept, by appropriately identifying boundaries between private and public places in the digital sphere, could assist towards crafting new more efficient and easier to enforce laws and regulations or towards appropriately updating the existing ones.

Finally, it should be mentioned that security and privacy protection are indispensable for building citizens' confidence in the Information Society. The DT concept by providing an appropriate approach to safeguard privacy and personal space in the digital world, could assist towards enhancing this trust and confidence of the user for the emerging Aml environment.



## ■ 5. Epilogue

### 5.1. Some considerations...

Despite its many foreseen benefits as presented in the previous section, the DT concept has certain limitations and gives rise to many questions when contemplating its further application. To begin with, there is a perceived difficulty in identifying effectively the boundaries of the private DTs, and certainly sometimes it is not that helpful to directly project from the physical space, because the two spaces have many differences. It is said that the freedom of one person ends where that of another's begins, and this should also be applied to DTs. In this sense, it should be considered that the residence boundaries cannot be only set and operated by the owner of the residence: they are both an individual and a collective concern.

Further to this, it should be noted that sometimes seemingly<sup>31</sup> (legally) un-regulated spaces as certain spaces of Internet have so far been, have provided the opportunity to communities of the Net for useful and innovative creation and development of breakthrough solutions, such as open-source and free software movement, as well as facilitated the exchange of ideas and freedom of expression. In a way this should be considered and respected: care should be taken not to 'over-regulate', eliminating thus opportunities of free expression and innovation. The suggestion of 'building a commons' in cyberspace has been introduced in the debates about intellectual property online from those concerned about maintaining the free flow of ideas [30]. Lessig, among others, advocates an 'intellectual commons', more or less a space promoting free exchange of ideas and collaboration, rather than a 'propertisation of ideas', the latter being more likely to emerge if notions of property dominate [22]. To this effect, we have already considered a third dimension / type of DT, the public DT, highlighting the importance of this concern; nevertheless, we wanted to emphasise even more its significance and at the same time the difficulty

of preserving a fair amount of control and protection over private / personal and public spaces, and whatever lies in between.

Another challenge regards the balance between privacy and security: privacy of a citizen in the sense of protection against loss of control over his/her personal data when operating in the network, versus the 'ambient security standpoint', the network or society that needs to protect itself against users with malicious intentions [26]. The drawing of boundaries should be performed in a way that people's privacy is appropriately protected, while also eliminating any opportunities for malicious activities, thus ensuring security as well. The quest towards attaining this balance would be always a very crucial objective not only of DT, but in general in the context of a Secure Information Society.

### 5.2. Next steps

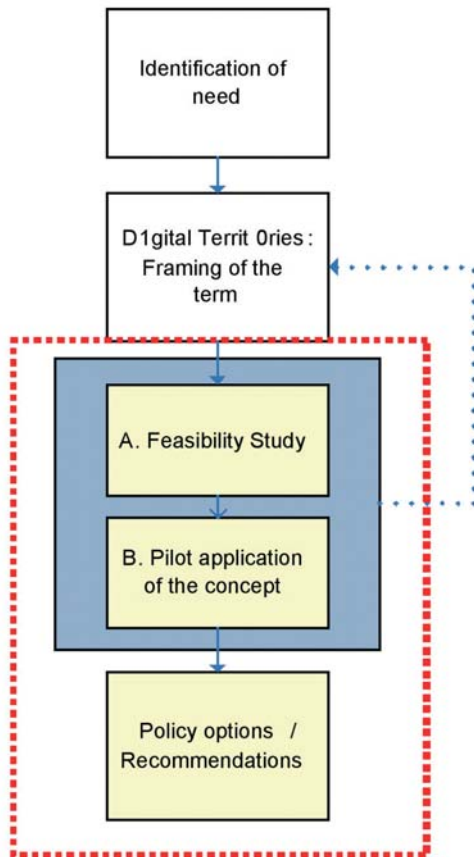
As already presented in the previous sections, a need was identified for systematic mapping of the personal digital space and on-line identities of individuals. To address this need the DT concept was developed and its basic components and associated terms were defined and analysed, as presented in this report. The DT framework would allow individuals to manage distance and boundaries, 'territories' in the social and legal sense in this new space, and that would also provide a proper balance between security and privacy.

At this point, in order to further gain more insight into the concept and supplement it appropriately, further research is considered necessary, which however should be conducted within a more systematic context. A feasibility study is proposed as a next step towards such a research, in order to assess the viability of the implementation of the DT concept. A feasibility study is normally used to assess the economic viability of a venture;

<sup>31</sup> We say 'seemingly', because most of these communities are regulated by informal rules / conventions by which their members have to abide

for example, in the case of setting up a new business, introducing a new product or developing an information system. In this case, it may constitute a preliminary analysis in the course of this study so as to ascertain its appropriateness and its likelihood to succeed. It may also provide an analysis of possible alternatives as to how to proceed with the study of the concept.

■ Figure 3



Following the feasibility study, we consider important to proceed with a pilot application of the concept, in order to test the concept in practice. Ideally, the concept will be tested against an Aml application; in order to do this it is important to co-operate with research institutes / manufacturers that are now developing Aml applications (e.g. RFID in the health area appears to be a suitable application domain). The involvement of users from the beginning of the process is also deemed very crucial. It is expected that the results of the feasibility study and the pilot application will provide feedback on the DT approach, so that there will be a need to review it and make appropriate additions or modifications. As mentioned in a previous chapter, VR could be the first application of DT, since it might a priority given that current applications put additional pressure on taking relevant action and also that it might be easier to apply. However, it should be noted that it will not be until the application of DT to public spaces that the real benefits from DT could be appreciated.

Finally, having established a concrete and structured approach on DT, some recommendations and policy options will be made towards addressing the identified issues.



## ■ References

1. Ahonen, P., Alahuhta, P., Daskala, B., De Hert, P., Delaitre, S., Friedewald, M., Gutwirth, S., Lindner, R., Maghiros, I., Mosci-broda, A., Punie, A., Schreurs, W., Verlinden, M., Vildjiounaite, E., Wright, D. (2006) *Safeguards in a World of Ambient Intelligence (SWAMI)*. Available at: <http://swami.jrc.es/pages/documents/SWAMI D4-final.pdf>
2. Altman, I. (1975) *The environment and social behaviour: privacy, personal space, territory, crowding*. Brooks/Cole Publishing Company
3. Bankston, K. (2006) *Google Copies Your Hard Drive - Government Smiles in Anticipation*. Electronic Frontier Foundation, February 09, 2006, available at: [http://www.eff.org/news/archives/2006\\_02.php](http://www.eff.org/news/archives/2006_02.php)
4. Beslay, L & Hakala, H (2003) *Digital Territory: Bubble in European Visions for the Knowledge Age - A quest for new horizon in the information society*, Kidd, PT (Ed.), Cheshire Henbury, 2007
5. Bohn, J., Coroam?, V., Langheinrich, M., Mat-tern, F. Rohs, M. (2003). *Disappearing Com-puters Everywhere – Living in a world of smart everyday objects*, Paper for the EMTEL Con-ference
6. Bray, H. (2006) *Google subpoena roils the Web – US effort raises privacy issues*. The Boston Globe, 21 January 2006. Available at: [www.boston.com/news/nation/articles/2006/01/21/google\\_subpoena\\_roils\\_the\\_web](http://www.boston.com/news/nation/articles/2006/01/21/google_subpoena_roils_the_web)
7. Castells, M (2000) *The information age: Econ-omy, Society and Culture Volume I – The rise of the network society*. Blackwell
8. Castells, M (2001) *The Internet Galaxy: Re-flections on the Internet, Business and Soci-ety*. Oxford University Press
9. Clements, B., Maghiros, I., Beslay, L., Cen-teno, C., Punie, Y. & Rodriguez, C. (2003) *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*. Report to the European Parliament Committee on Citizen's Freedoms and Rights, Justice and Home Affairs (LIBE), IPTS-JRC, July 2003, EUR 2083 EN
10. Daskala, B. & Maghiros, I (2006) *D1gital Ter-ritOries*. Proceedings of the 2nd IET Interna-tional Conference on Intelligent Environments, July 2006, Vol.2, 221-226
11. Directive 1995/46/EC of the European Parlia-ment and of the Council of 24 October 1995 on the *protection of individuals with regard to the processing of personal data and on the free movement of such data*. Official Journal L 281, 23/11/1995, pp. 31- 39
12. Elisson, C. (2002) *Home network Security*. Intel Technology Journal, Vol. 6, Issue 4, No-vember 2002, 37-48
13. Garrett, R (2006) *Google GDrive is not a rumor*. Googling Google blog, 3 March 2006 <http://blogs.zdnet.com/Google/?p=121>
14. Garfinkel, S (2004) *The Pure Software Act of 2006*. The Net Effect Column Series, April 7, 2004, Technology Review
15. Gibson, W (1984) *Neuromancer*. New York: Ace Books.
16. Google web-site, 'Search Across Computers' feature. Available at: <http://desktop.google.com/features.html#searchr-emote>
17. Gutwirth, S. (2002) *Privacy and the Informa-tion Age*. Rowman & Littlefield Publishers
18. Hudson, A. (1999) *Beyond the borders: Glob-alisation, sovereignty and extra-territoriality in 'Boundaries, Territory and Postmodernity'*, Frank Cass Publishers
19. i2010 - Communication from the Commis-sion to the Council, The European Parliament, The European Economic And Social Commit-tee And The Committee Of The Regions, *Challenges for the European Information Soci-ety beyond 2005*. 19 November 2004, COM(2004) 757

20. IST Advisory Group Working Group Report (2002) *Strategic orientations and priorities for IST in FP 6*, Report of the IST Advisory Group, EC: Luxembourg. [www.cordis.lu/ist/istag](http://www.cordis.lu/ist/istag)
21. IST Advisory Group Working Group Report (2003) *Ambient Intelligence: from vision to reality [For participation – in society & business]*. Available at: [ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-ist2003\\_consolidated\\_report.pdf](ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-ist2003_consolidated_report.pdf)
22. Jordan, M. (2006) *Electronic Eye Grows Wider in Britain*. The Washington Post, 7 January 2006
23. Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York NY: Basic Books
24. Lyon, D. (2001) *Facing the future: Seeking ethics for everyday surveillance*. Ethics and Information Technology, Vol. 3, pp.171-181
25. Marx, GT (2001) *Murky conceptual waters: the Public and the Private*. Ethics and Information Technology, Vol. 3, No. 3, pp.157-169
26. McCullagh, D (2006) *FAQ: When Google is not your friend*. C/Net News.com, 12 April 2006. Available at: [http://news.com.com/FAQ+What+does+the+Google+subpoena+mean/2100-1029\\_3-6029042.html?tag=nl](http://news.com.com/FAQ+What+does+the+Google+subpoena+mean/2100-1029_3-6029042.html?tag=nl)
27. Nayar, P. K. (2004) *Virtual worlds – Culture and politics in the age of cybertechnology*. Sage Publications
28. Negroponte, N. (1995) *Being Digital*. Vintage Books, New York
29. O'Reilly, T (2005) *What is Web 2.0 – Design Patterns and Business Models for the Next Generation of Software*. Published on O'Reilly [www.oreilly.com](http://www.oreilly.com), 30 September 2005
30. Regan, P. M. (2002) *Privacy as a common good in the digital world*. Information, Communication & Society, Vol. 5, No. 3, pp. 382-405
31. Riguidel, M, Martinelli, F et al. (2006) *Security, Dependability and Trust*. Beyond-the-Horizon, Thematic Group 3, Report for public consultation
32. Rotter, P., Compañó, R. & Daskala, B. (2006) *Will passwords, biometrics and identity cards disappear? RFID implants – new opportunities and challenges for identification and authentication of people*. Forthcoming paper (December 2006)
33. Tavinim H.T. & Grodzinsky, F.S. (2002) *Cyberstalking, personal privacy and moral responsibility*. Ethics and Information Technology, 4, 123-132
34. VeriChip Corporation (2006) *VeriMed patient identification. Procedure for VeriMed™ System Use*. Available at: <http://www.verimed-info.com/files/VeriMed%20ER%20Protocol.pdf>
35. VeriChip Corporation (2006) *97 Healthcare Facilities Have Now Agreed to Implement the VeriMed Patient Identification System*. Available at: <http://www.verichipcorp.com/news/1145900688>
36. Webb, S. (2001) *Avatar Culture – Narrative, power and identity in virtual home environments*. Information, Communication & Society, Vol. 4, No. 4, pp. 560-594
37. Wellman, B. (2002) *Physical space and cyberplace – The rise of networked individualism in 'Community Informatics – Shaping computer-mediated social relations'*, Routledge
38. Wikipedia (2006) *Wiki*. Available at: <http://en.wikipedia.org/wiki/Wiki>

## ■ ANNEX I: A virtual residence in an ambient intelligence space

### 1. Executive summary

Ambient Intelligence (Aml) refers to a vision of the future Information Society where humans will be surrounded by intelligent interfaces. They will be supported by computing and networking technology that is everywhere - embedded, for example, in everyday objects such as furniture, clothes, vehicles, roads and smart materials. Computing capabilities will be ubiquitous (not only inside computing devices), connected, and always on, enabling people and devices to interact with each other and with the environment. Computer devices will become increasingly small and cheap, easily interconnected and easy to use. Though many benefits are expected from Aml, there is also widespread concern about their potential use for monitoring, surveillance, data searches and data mining. In such an environment, and as our lives, homes, cars, neighbourhoods, cities and most other environments become increasingly digitized and connected, more and more personal information will be gathered, stored and possibly accessed by or disclosed to third parties such as service-providers, institutions and/or other individuals. This information encompasses not only basic personal identification data such as age, sex and location but also information and content such as events information (past, current and future), working documents, family albums (pictures, video, chat) and even shopping, medical and financial records.

In this context, IPTS has coined the concept of Virtual Residence (VR) to raise concerns over security, privacy and identity of digital living and working, as well as to help develop solutions to the future privacy, security and identity problems of living and working in an Information Society inspired by the vision of Ambient Intelligence (Aml). The concept of VR deliberately takes the citizen's residence as the starting point for discussing the need for a future virtual residence, which will be considered as a legal and social sanctuary. It is the objective of this report to lay down the foundations for the future development of Virtual Residence or of another similar concept under a different name. Developing such a concept is of vital importance,

if the emerging Ambient Intelligence environment is to become widely accepted and serve the individuals in their everyday life.

The 'Virtual Residence' (VR) consists of the following three elements: (a) The future intelligent/connected home (computing embedded in everyday objects connected via domestic infrastructures); (b) The online lives of people, families, households; and (c) Mobility and interoperability between different Aml environments (Cf. Aml Space). 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. The concept of virtual residence can be seen as a virtual representation of the smart home. It could be used as a mental map to manage security and privacy, both remotely and from within the home.

Moreover, the concept of VR deliberately takes the citizen's current physical-world-residence – which is legally recognised and protected – as the starting point for discussing the need for a future virtual residence, which will be considered as a private Digital Territory and thus as a legal and social sanctuary. The protection of the *material/physical* home is one of the oldest human rights and it is still enshrined in international human rights law and in national constitutions. Although the notion of home as a sanctuary might hide the tensions, struggles and inequalities (e.g. gender) that occur in the lives of many families, its symbolic meaning as a private space cannot be underestimated. The home is more than a certain physical environment; it is also about feeling at ease and being comfortable. The idea of non-interference in order to 'manage' his/her relational, civil and political life as a free human being is regarded as crucial in a democratic constitutional state. Values protected by the inviolability of the home therefore might need to be extended to the virtual world, hence the notion of virtual residence. This argument urges that ethical and normative

questions be raised and that societal choices be made that go beyond procedural data protection rules.

The concepts of territoriality, proximity and personal space have been studied extensively in the past, from many different angles and in many different ways. It is our purpose in this report, to demonstrate that these concepts are crucial to understanding the privacy, security and identity implications of VR. Social relations are managed, amongst others, via proximity and distance to others. The physical barriers of proximity that regulated access to persons and to personal information in traditional societies are disappearing in an Ambient Intelligence environment. This is related to territoriality.

A residence is by definition a limited territory designed by boundaries. These limitations permit to express and enforce specific rules which are implemented exclusively in this dedicated space. In the physical world, the borders of everyday life spaces are characterised by great diversity but they are the result of socio-cultural, legal and/or economic rules and motivations. Fences are commonly used to establish the borders of a residence for instance, but depending on the social context, it might be less tolerated or more dangerous to cross the open grass of a US residence than crossing the gate of a European one. In both cases however, indicators or markers are available to inform others where public space ends and private property starts.

Today, 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 users judge 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 clarification of the social and legal framework of this new Aml space. Virtual residence could be used to represent the online private space of people, families or households in Ambient Intelligence and it could enable the creation of new ways of living in cyberspace. It could be a mental model and virtual space on its own for dealing with the definition of public and private in the online world and thus for managing personal identities, privacy and security.

The physical barriers of proximity that restricted access to the personal information in traditional societies are disappearing in an Ambient Intelligence environment, not only where this information is networked and thus remotely available, but also where the boundaries between traditionally distinct environments (e.g. work, home, school) are disappearing as the private sphere is brought into the public sphere and vice versa. Although the distinction between private and public spaces 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. Socio-cultural norms, habits and legal rules provide the guidelines for people’s assessment of what is a private or a public space. The complex interrelationship between what is regarded as public or as private – affected by ICTs and in the future even more by Aml – is inherently related to issues of privacy and security. In the physical world, personal privacy is typically protected, both legally and socially, by the notions of ‘domicile’ and ‘residence’. These are carefully developed and recognized concepts that have even evolved to encompass other (mobile) spaces such as the car. Indeed, in some countries the interior of a car benefits from the same legal protection as the private domicile.

At this point, it should be noted that one important concern today is that there are very little indicators for what is public and private in the digital realm. Not only are there privacy concerns about accessing private spaces that have no clear indicators or that give no prior indication that they are private, but there are also concerns about the digital footprints people will leave behind in the future Aml Space. Internet users, especially newcomers, typically assume that their activities in cyberspace are private since no one in physical space is observing them as they use their computers. Another issue is that of storage, which lies at the core of the Virtual Residence concept. The increased digitisation of our everyday lives means that more and more data on our activities will become available in digital format.

Finally, certain application areas and examples of VR may be drawn. These relate to the application fields of e-entertainment/culture/leisure/education, e-government, e-health and smart home. These examples are presented in the final chapter of the report.



At this point, it should be noted that this report has been developed internally by IPTS and has not been officially published. Also, the research conducted led IPTS further investigate the context of Digital territories (DT); therefore, no definitive conclusions or policy options were reached regarding VR, and thus none are being elaborated in this report.

## 2. Introduction

### Virtual residence

As our lives, homes, cars, neighbourhoods, cities and other environments become increasingly digitized and connected, more and more personal information will be gathered, stored and possibly accessed by or disclosed to third party sources, service-providers, institutions and/or other people. This information encompasses not only basic personal identification data such as age, sex and location but also information and content such as events information (past, current and future), working documents, family albums (pictures, video, chat) and even shopping, medical and financial records.

IPTS has coined the concept of Virtual Residence (VR) to help develop solutions to the future privacy, security and identity problems of living and working in an Information Society inspired by the vision of Ambient Intelligence (Aml). The concept of VR deliberately takes the citizen's current residence as the starting point for discussing the need for a future virtual residence, which will be considered as a private Digital Territory and thus as a legal and social sanctuary. In the physical world, concepts of residence and domicile are carefully developed and recognised. The argument is that a comparable level of sophistication will be needed for people to accept and trust their increasingly digitized residential everyday life activities. Virtual Residence could provide for that.

VR would satisfy the need for people to feel at home in their future intelligent environment by representing their multiple identities (legally and socially), while respecting their privacy and secur-

ing their personal data and safety. VR consists of the following three elements:

- The increasingly connected future home and its domestic infrastructures will be one of the 'nodes' in the network society.
- Internet activities that relate to living in a physical residence, i.e. the online lives of people, families, and households.
- An extension of the physically located residence to cyberspace permitting, therefore, a greater mobility and interoperability between different Aml environments.
- The concept of virtual residence could help to:
- Tackle concerns of identity, privacy and security within the smart home and outside, and also for peoples' personal online activities.
- Contribute to a better perception and consideration of a citizen's personal digital territory.
- Tackle the blurring boundaries between what is public and private in the online world and especially the crossing of these boundaries.
- Extend the citizen's personal digital territory through time and space.

### Ambient intelligence

Ambient Intelligence (Aml) refers to a vision of the future Information Society where humans will be surrounded by intelligent interfaces. They will be supported by computing and networking technology that is everywhere - embedded, for example, in everyday objects such as furniture, clothes, vehicles, roads and smart materials. Computing capabilities will be ubiquitous (not only inside computing devices), connected, and always on, enabling people and devices to interact with each other and with the environment. Computer devices will become increasingly small and cheap, easily interconnected and easy to use. Smart devices will also be able to sense, think and communicate.<sup>32</sup>

The ISTAG<sup>33</sup> vision on Aml describes an environment that is intelligent and aware of the specific characteristics of human presence and

<sup>32</sup> ISTAG (2001) Scenarios for Ambient Intelligence in 2010, IPTS-ISTAG, EC: Luxembourg. <http://www.cordis.lu/ist/istag>

<sup>33</sup> ISTAG is the Information Society Advisory Group, a group of experts from both academia and industry advising the IST (Information Society Technology) program of the European Commission: <http://www.cordis.lu/ist/istag.htm>

personalities, takes care of human needs and is capable of responding intelligently to spoken or gestured wishes. It can even engage in intelligent dialogue. Right from the start, ISTAG explicitly sets people at the centre of development, not the technologies. According to the Aml scenarios for 2010, people (not just 'users', 'consumers' or 'employees') are at the forefront of the Information Society. The vision of people benefiting from services and applications whilst supported by new technologies in the background and of people interacting via intelligent user interfaces was essential to the ISTAG (ISTAG 2001: 3). The advisory group also warns that there is a potential risk of loss of control in such an environment and stresses the importance of giving ordinary people control over Aml and the ways in which its systems services and interfaces are implemented.

Aml represents a paradigmatic shift in computing towards 'human centred computing' whereby computing moves to the background in support of human interactions. Today, Aml is still more of a vision of the future than a reality but it is already a key concept in the EU FP6 IST program for the period 2002-2006.<sup>34</sup> According to its 2003 revising and updating of the Aml vision, ISTAG believes it is not necessary to define the term Aml more tightly. It should be regarded and promoted as an 'emerging property' rather than as a set of specified requirements. Moreover, Aml can only be fully developed by a holistic approach, encompassing technical, economic and societal research. It should not just consider the technology, but the complete innovation supply-chain from science to end-users, and should take into account the various features of the academic, industrial and administrative environment facilitating or hindering the realisation of the Aml vision. (ISTAG 2003: 12-13).<sup>35</sup>

Though many benefits are expected from Aml, there is also widespread concern about their potential use for monitoring, surveillance, data searches and mining. The general acceptance of these technologies requires high levels of trust; and the security of the underlying infrastructure will be

expected to protect citizens from various types of intrusion while collaborating with law enforcement requirements and maintaining their dynamically managed private (family and friends) and wider community interaction.

The concept of 'Virtual Residence' is proposed as a means of identifying and tackling concerns about identity, privacy and security within Ambient Intelligence, from the point of view of citizens' everyday living environment.

## Ambient intelligence space

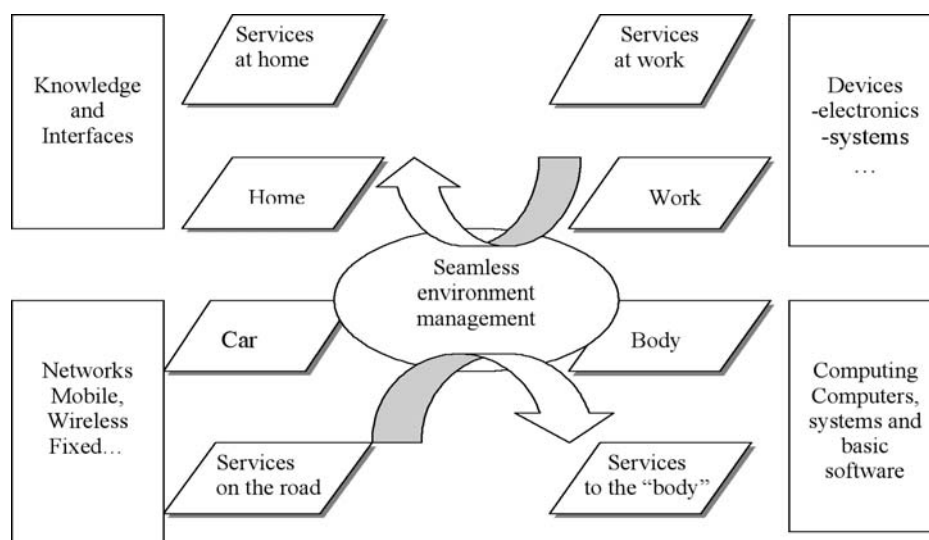
In 2002, ISTAG introduced the notion of Ambient Intelligent Space. The individual moves through different Aml environments such as home, work, school, car, etc. while expecting seamless services. The collection of all facilities and capabilities to enable seamlessness is called the 'Ambient Intelligence Space' (ISTAG 2002). The Aml Space is composed of collaborative (location or social based) sub-spaces, of devices (including sensor and actuator systems), services (including their interfaces) and the connecting networks. The Aml space is not just the collection of its component parts, but involves genuine integration and migration between them. It is precisely the seamless interconnection and integration of these various environments and the management of the required interoperability that constitutes the Aml Space. As such it spans all the different spheres of everyday life by migrating between technologies, services and users.

The Aml Space should contain applications and services that actively support humans in achieving specific tasks. It should interact with the user, model and know user behaviour, control security aspects to ensure the privacy and security of the transferred personal data and deal with authorisation, key and rights management. It should also ensure the quality of services as perceived by the user. As such, the Aml Space is not just a technical space. The IST Advisory Group believes that realising the Aml space will be no trivial task.

<sup>34</sup> European Commission (EC) (2002) Information Society Technologies. A thematic priority for Research and Development under the Specific Programme 'Integrating and strengthening the European Research Area' in the Community sixth Framework Programme, IST Priority, WP 2003-2004, EC: Luxembourg. <http://www.cordis.lu/ist>

<sup>35</sup> See for a more extensive discussion of the Aml vision: Punie, Y. (2003) A social and technological view on Ambient Intelligence in Everyday Life: What bends the trend?, European Media, Technology and Everyday Life Research Network, EMTEL2 Key Deliverable Work Package 2, September 2003, EC DG-JRC, IPTS, Sevilla. [EUR 20975]

■ Figure: Ambient Intelligence Space<sup>36</sup>



Crucial issues are availability and protection of copyrights, privacy and security of personal data, regulations and open standards, and viable business models. It is precisely the connection and integration of the different Aml environments described above that raises most concern over balancing privacy and security. Moreover, ISTAG<sup>37</sup> argues that this Aml Space will require a new security paradigm that is different from the security approaches that are deployed today (see next section). Another core challenge for this Aml Space, as regards security and privacy, consists in managing the blurring boundaries between what are regarded as (open) public spaces and (protected) private spaces, as will also be explained below.

ISTAG elaborates on the need for a new security paradigm and mindset for the future Ambient Intelligence Space in its paper on trust, dependability, security and privacy for IST in FP6. Security will become an increasing concern because of the scale of Aml (millions of connected devices and people), the foreseen mobility needs (which introduces more vulnerability than in a static world), its heterogeneity (in contrast with closed, co-designed systems), its complexity of hardware and software (introducing the dependability challenge) and its distribution of knowledge and resources (co-operation and interconnection).

In the future Aml Space, people will participate in a multiplicity of parallel, overlapping and evolving relationships (one-to-one, one-to-many, many-to-many) of which some will be very short-lived and on the spot, others will be temporary and moving through time and space and others that will be long-lasting but very flexible and dynamic. As a result, the parameters for this new paradigm are change, dynamism, de-centralization (distributed), flexibility, mobility, heterogeneity, temporality and context-dependency, in contrast with present day security parameters that are relatively stable, well defined and consistent. In a sense, this new approach reflects better our real-world interactions based on trust and confidence but it challenges present day computerized security.<sup>38</sup>

### The need for virtual residence

IPTS has coined the concept of Virtual Residence (VR) to raise concerns over security, privacy and identity of living and working in the future Information Society in Europe inspired by the vision of Ambient Intelligence. The objective of the VR project is to identify and discuss future risks and opportunities for Aml in everyday life, in terms of identity, privacy and security. This should contribute to informing Europe's decision-makers

<sup>36</sup> Source: ISTAG (2002a) Strategic orientations and priorities for IST in FP 6, Report of the IST Advisory Group, p.16, EC: Luxembourg, June 2002. <http://www.cordis.lu/ist/istag>

<sup>37</sup> ISTAG (2002b) Trust, dependability, security and privacy for IST in FP 6, Report of the IST Advisory Group, EC: Luxembourg, June 2002, p.9. <http://www.cordis.lu/ist/istag>

<sup>38</sup> ISTAG, 2002b: 6-12.

about the possible implications of Ambient Intelligence in Europe and help them identify the issues and bottlenecks for realising the future information society.

Ultimately it is the objective of European RTD, in particular in the field of IST, to contribute directly to realising European policies for the knowledge society as agreed at the Lisbon (2000), Stockholm (2001) and Seville Council (2002), and as reflected in the e-Europe Action Plan.<sup>39</sup> The strategic goal for Europe in the next decade is 'to become the most competitive and dynamic knowledge-based economy in the world capable of sustainable economic growth with more and better jobs and greater social cohesion'. This requires wider adoption, broader availability and an extension of IST applications and services in all economic and public sectors and in the society as a whole.<sup>40</sup>

Virtual Residence, more particularly, contributes to the e-Europe goal of creating a safer information society.<sup>41</sup> The objective of this European Commission Communication is to promote new services supported by ICT which will at least match the security and privacy requirements of the current-day European Society. New cybercrime activities and privacy invasive measures are for example emerging and are potentially threatening everyday life in Europe. According to the Communication, such threats should be contained at a residual level of risk. They should not produce greater risks.

According to the article 7, *Respect for private and family life*, of the European Union Charter of Fundamental Rights, 'Everyone has the right to respect for his or her private and family life, home and communications'. It means that our residence is regarded as a social and legal sanctuary. The concept of VR deliberately takes the citizen's current residence as the starting point for raising the need for a private space in the digital world that is also protected as a legal and social sanctuary. The

preservation of such a private digital space will not go automatically hand in hand with the increasing digitalisation of everyday life, hence the need for a virtual residence.

The objective of virtual residence is also, through its implementation, to contribute to trust and confidence. The VR will be involved in the continuous work of what sociologists such as Antony Giddens refer to as 'ontological security', i.e. a sense of basic trust in the world they live in. Without trust, people would feel lost and unsafe in a world that is increasingly mediated by technologies. The virtual residence might contribute to building trust, provided it becomes socially meaningful for peoples' identities, guided by a legal framework that respects their privacy and establishes an acceptable level of security.

Without trustworthy conditions which constitute the prime platform of a sustainable Society, the acceptance of ambient intelligent spaces will be compromised. In this sense, privacy and security requirements have to be at least preserved and eventually enhanced. The security level of complex systems like a society is usually defined by the security level of its weakest link. If a new element is added to the Society/system, in this case the emerging ambient intelligence spaces, their inherent security level will contribute to or decrease the overall Society security level. The level of security of ambient intelligence spaces, the way these digital environments will manage the privacy of the individuals and of course the quality of their services will therefore tune the future quality of life of the European citizen.

Anecdotic evidence suggests that the weakest link in security lies with the human. Security firms foresee that lax security practices of lay computer users will fuel a boom in online identity theft. A recent UK survey<sup>42</sup> found that maintaining online identities is becoming a burden for many people who, on average, use 20 sites that require them to register and then log on afterwards. To make these

<sup>39</sup> See for respective documents: [www.europa.eu.int](http://www.europa.eu.int)

<sup>40</sup> European Commission (EC) (2002) Information Society Technologies. A thematic priority for Research and Development under the Specific Programme 'Integrating and strengthening the European Research Area' in the Community sixth Framework Programme, IST Priority, WP 2003-2004, EC: Luxembourg. <http://www.cordis.lu/ist>

<sup>41</sup> COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', COM(2000) 890 final, Brussels, 26.1.2001

<sup>42</sup> BBC Online 'Passwords revealed by sweet deal', 20 April 2004, BBC Online News.



different online personas easy to manage, two-thirds use the same password for all the different sites. The security industry argues people need to be more aware of the risks and need to protect their online identity. Virtual Residence could contribute to such awareness but it would also argue for developing more user-oriented ways to secure their identities. Asking people to remember many different passwords is not very user-friendly.

Trust, confidence and reliability are, amongst others, powerful enablers of 'domestication', i.e. the process whereby technologies become accepted or rejected into people's everyday lives.<sup>43</sup> Provided that the VR is able to reflect multiple identities, to protect the privacy of these identities and to offer acceptable levels of security, it might indeed facilitate the acceptance of new technologies. It could provide citizens with a familiar concept for understanding new privacy and security challenges and thus enhance the trust and confidence necessary for people to feel at home in their future smart/intelligent homes and to be at ease with their online lives. Comparable to the domicile and residence concept in the physical world, a similar level of sophistication is needed in the future for the virtual residence.

One of the inevitable challenges VR needs to address is the trade-off between keeping certain personal information private and receiving convenient, efficient services will have to be made.<sup>44</sup> Ambient Intelligence depends for its successful functioning on the wide adoption by citizens of that trade-off.

Virtual residence may today be seen as closely related but very distinct from the physical residence, hence notions as cyberspace and infosphere. The cyberworld is traditionally regarded as

a separate and almost parallel environment to the physical world. But as the diffusion of new ICTs increases and as ICTs become integrated in everyday life, clear boundaries between the two worlds will disappear.

## Background information on VR and this report

The term virtual residence within the context of privacy and security was voiced by Bogdanowicz & Beslay<sup>45</sup> and further developed by Beslay and Punie.<sup>46</sup> A more extensive analysis was described in one of the chapters of the IPTS Report for the European Parliament LIBE Committee on security and privacy for the citizen in the post-September 11 digital age (2003).<sup>47</sup> In order to validate the concept of Virtual Residence, a selected group of experts was invited, firstly, to reply to an open-ended questionnaire (in two rounds) and secondly, to participate in an interactive workshop where the results of the two surveys are discussed. About 15 external experts with diverse backgrounds contribute, ranging from cyber law and law enforcement to trust, confidence and privacy as well as identity technologies, network security, Ambient Intelligence and ubiquitous computing technologies, and social studies of technology (See acknowledgments).

The first open-ended questionnaire, distributed in October 2003 had the objective to discuss the implications of Virtual Residence in five promising areas of the future Information Society, i.e. e-governance, e-health, e-entertainment, e-mobility and smart homes.<sup>48</sup> Short descriptions of possible applications of VR in each of these areas were given in a questionnaire. The experts were asked to:

<sup>43</sup> E.g. Silverstone, R. & Haddon, L. (1996) 'Design and domestication of information and communication technologies: Technical change and everyday life', pp. 44-74 in R. Mansell & R. Silverstone (eds.), *Communication by design. The politics of information and communication technologies*. Oxford: Oxford University Press.

<sup>44</sup> E.g. SRI (2003) Distributed Identities: Managing privacy in pervasive computing, SRI Consulting Business Intelligence, Explored Viewpoints, May 2003.

<sup>45</sup> Bogdanowicz, M. & Beslay, L. (2001), 'Cyber-security and the future of identity', *The IPTS Report*, Special Issue on Cyber-security, No. 57, September 2001, 23-27.

<sup>46</sup> Beslay, L. & Punie, Y. (2002), 'The virtual residence: Identity, privacy and security', *The IPTS Report*, Special Issue on Identity and Privacy, No. 67, September 2002, 17-23.

<sup>47</sup> Clements, B., Maghiros, I., Beslay, L., Centeno, C., Punie Y. & Rodriguez, C. (2003) Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), IPTS-JRC, July 2003.[EUR 2083 EN]

<sup>48</sup> These fields are, amongst others, also proposed by the Information Society Advisory Group (ISTAG) in its latest document on 'Ambient Intelligence: from vision to reality', October 2003. [www.cordis.lu/ist/istag-reports.htm](http://www.cordis.lu/ist/istag-reports.htm).

1. To complement the argument in favour of the application of VR with additional details or new elements raising the need for VR.
2. To provide arguments against the example, i.e. if you believe it to be one where VR is not pertinent.
3. To propose other illustrative examples in the selected area. You are also free to go beyond the selected areas.

Results of the first questionnaire led to more clear ideas on the possible application fields of VR in order to prove its relevance and usefulness. Objective of a second questionnaire (November 2003) was to deepen the concept itself by focussing on its three major dimensions or constituents: privacy, security and identity. In that questionnaire, also, the notion of territory, property and space were introduced by defining virtual residence through its boundaries. It has the objective to provide a tool that enables users to manage proximity and distance with others, both in a legal and a social sense, as they do also in the physical world.

The results of both questionnaires were used by IPTS to prepare background notes for discussion and validation at an interactive workshop, held in Sevilla, 19-20 January 2004. The objective of the workshop was threefold:

1. Get a clear account of what VR is and what it is not, based on previous research and on the responses from an open-ended questionnaire (in two rounds);
2. Highlight and detail the VR concept regarding the issues of Identity, Privacy and Security and their related social, economic, legal and technological challenges;
3. Identify and propose future research challenges and policy options regarding the development of VR.

This report does not only present the results of the workshop. Rather it should be seen as an integration and synthesis report of the work IPTS has been doing during the last years, although not continuously, on Virtual Residence. The workshop undoubtedly played a major role here, and we are

grateful for the comments of the workshop participants on earlier versions of the report.

Two more chapters follow:

- **Virtual Residence: Definition and basics** – In this chapter, the concept of Virtual Residence is defined and explained; also its three dimensions are identified, namely the smart home, mobility and life online, as well as the basic constituents of the VR concept.
- **Possible application fields for VR** – Following the presentation of the concept itself, in this chapter certain application areas and examples are presented. The application fields considered are e-entertainment/culture/leisure/education, e-government, e-health and smart home.

### 3. Virtual residence: definition and basics

#### Virtual residence as a legal and social sanctuary

The home represents a private territory, a sanctuary where there is intimacy, anonymity and a possibility of solitude. The protection of the *material/physical* home is one of the oldest human rights and it is still enshrined in international human rights law and in national constitutions. Although the notion of home as a sanctuary might hide the tensions, struggles and inequalities (e.g. gender) that occur in the lives of many families, its symbolic meaning as a private space cannot be underestimated. The home is more than a certain physical environment; it is also about feeling at ease and being comfortable. The idea of non-interference in order to 'manage' his/her relational, civil and political life as a free human being is regarded as crucial in a democratic constitutional state. Values protected by the inviolability of the home therefore might need to be extended to the virtual world, hence the notion of virtual residence. This argument urges that ethical and normative questions be raised and that societal choices be made that go beyond procedural data protection rules.<sup>49</sup>

<sup>49</sup> Clements, B., Maghiros, I., Beslay, L., Centeno, C., Punie Y. & Rodriguez, C. (2003) Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), IPTS-JRC, July 2003, EUR 2083 EN.

Private digital territory needs to be protected in a similar way to the way physical residences are protected today. On the one hand, it would allow one to have an inaccessible personal digital place where private digital assets could be stored and manipulated, and on the other, it could represent a virtual personal sanctuary, i.e. the virtual residence. As mentioned above, having a physical place where one can be left alone as a free human being is a crucial component in democratic societies and a similar zone of non-interference in the digital world would thereby be legitimate as everyday life becomes increasingly digitized. 'Anonymity spaces' where no monitoring and surveillance is possible could be considered, or 'anonymity moments' during the course of the day.

Just as the notion of physical 'residence' has evolved –in some countries<sup>50</sup>– to encompass other (mobile) spaces such as the car, VR should not be seen as restricted to the physical residence. Moreover, similar to the way people move through time and space, VR should be seen as a mobile and dynamic concept travelling through different Aml environments.

The boundaries between traditionally distinct environments (e.g. work, home, school) are disappearing as the private sphere is brought into the public sphere and vice versa. Although the distinction between private and public spaces 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. Socio-cultural norms, habits and legal rules provide the guidelines for people's assessment of what is a private or a public space.

But it is clearer today that digital world is more a new part of the Society which offers the individuals a greater polyphonic every day life space and probably more complex, instead of an alternative environment. The individual has now to deal with numerous areas where his /her basics fundamental rights but also his/her duties are more and more difficult to maintain at an equal level independently of the nature of the space: digital or not.

## The three dimensions of virtual residence

### Smart home

The increasingly connected future home and its domestic infrastructures as one of the 'nodes' in the networked society.

The smart home of the future would contain a huge number of sensors embedded in the home environment and in home objects. These tiny sensors will be connected in sensor networks which can monitor everyday activities in ways that are completely invisible<sup>51</sup> to the people being monitored. The potential risks of privacy invasive monitoring and surveillance are high. For every sensor, a different debate could be held –as argued by researchers involved in the US based Georgia Tech Aware Home<sup>52</sup>– on where (and where not) to install a sensor in the smart home, and for what purpose the sensor information can or cannot be used. Sensors may be used to detect physical activity (e.g. a person entering a room, a temperature change, an object being moved) and therefore do not necessarily collect personal information. Sensors can also safeguard privacy through anonymity but coupled with other data, especially identification data (e.g. video camera) they may become privacy invasive (e.g. identifying and storing who moved the object).

Natural borders could easily be crossed in the smart home where rooms are equipped with sensors. Other people are able to know – remotely, if they wish– who is in the home, in which room, with whom (other inhabitants and/or visitors), at what time, and also, maybe, what one is doing. It is easy to argue that people can opt out by not installing, activating or using these features, but the situation is more complicated since services are expected to provide added value. For example, monitoring the most private spaces of the home such as the bathroom might even be worthwhile, for medical purposes such as preventive medical care.

There are many different possibilities and technologies to be considered, but it should be

<sup>50</sup> E.g. France : Conseil Constitutionnel 12 janvier 1977, decision 76-75 DC, 'fouille des véhicules' et protection de la liberté individuelle.

<sup>51</sup> A fundamental characteristic of Aml is indeed that computing capabilities move to the background and become invisible, hence R&D programs such as 'the disappearing computer', an EU funded activity in Future and Emerging Technologies (FET) of the IST research program. <http://www.disappearing-computer.net>

<sup>52</sup> Gooley, C. & Saponas, T. (n.d.) Privacy issues of the Aware Home. Paper on the Georgia Tech Aware Home project. <http://www.thegooley.com>; See also <http://www.awarehome.gatech.edu>.

clear that privacy invasion is a real concern in the future home embedded with sensors and computing capabilities. If there are no privacy enhancing strategies available, people might not be willing to live in this smart home. As long as sensitive data remain in the home, and thus within the legally and socially protected environment of the home, it could be argued that privacy concerns are less imminent. But since the smart Aml home is a connected home and thus accessible, manageable and visible from the outside, new privacy invasive threats are becoming possible from the outside world. But even within the home, certain rooms are more private than other rooms, and household individuals could spy on each other, raising again privacy issues.

The smart home also faces security challenges. In such an intelligent environment, the risk of external attacks could be much greater than they are today with computers connected to the Internet. This is due, for instance, to the proliferation of access networks which increase the number of entry points and also due to the intense interconnection of these networks. Moreover, threats will come not only from outside but also from inside the home. Home network security needs to take into account different life styles and household compositions. Security requirements are different – in terms of authorization and confidentiality, for instance – for single-person homes, single-parent homes, couples with small children and couples with teenagers. Friends (teenagers and adults) and visitors also need to be taken into account in the home security policy. The notion of binary network security (access or not) will have to be replaced by more complex security mechanisms whereby differential access is granted to different actors. Home network security will become in the future not only more important but also more complex.<sup>53</sup> A crucial and new concern is also that home network security will become ‘critical’ in the future Aml, hence the notion of ‘Critical Domestic Infrastructures’ (CDIs) (See further).

### Mobility

Just as the notion of physical residence has evolved to encompass other (mobile) spaces such

as the car, and just as people move through time and space, so virtual residence should be seen as a mobile and dynamic concept travelling through different Aml environments (home, work, school, leisure, neighbourhood, city). The Aml space indicates a seamless connectivity and interoperability between these different environments. This would mean that people can access their virtual residence as a protected private space from any other public and private space. This follows the sociological trend, enabled by ICTs (e.g. mobile phones), of the blurring of traditionally distinct spheres of living (e.g. home and work).

Mobility in Aml Space not only implies the movement of people but also the movement of personal data in cyberspace via things such as caches, cookies, liquid software<sup>54</sup> and downloadable applications. Therefore, it seems to be necessary to envisage online extensions of the virtual private space that encompass intelligent agents. These agents move through time and cyberspace by ‘encapsulating’ personal data to carry out requests for their real life counterparts. Some intelligent agents, for example those used in online travel shopping, compare the discounted fares offered by major airlines and are able to book them online, having received the users’ consent. In order to find the best flight ticket corresponding to the user’s specific criteria, the intelligent agent has to ‘go’ through numerous web sites comparing the user’s personal data with the travelling information offered. This example illustrates how online personal information belonging to someone’s private space can spread around in online public spaces, without the owner knowing about it. It indicates also the blurring of boundaries between online public and private spaces in the future Aml space.

### Life online

Internet activities that relate to living in a physical residence, i.e. the online lives of people, families and households.

In an intelligent environment, more and more personal information will be gathered, stored and possibly accessed by or disclosed to third party

<sup>53</sup> Elisson, C. (2002) Home network Security, *Intel Technology Journal*, Vol. 6, Issue 4, November 2002, 37-48.

<sup>54</sup> Liquid software is software that easily ‘flows’ from machine to machine. It is proposed as a new way of constructing computerized networked systems.



sources, service-providers, institutions and/or other people. This information encompasses not only basic personal identification data such as age, sex and location but also information and content such as events information (past, current and future), working documents, family albums (pictures, video, chat) and even shopping, medical and financial records.

Standard Internet search facilities can today be used to gather information about where people live and work and what their interests are. This raises the question of whether personal information on the Internet is public, since the Internet is a public network.<sup>55</sup>

There are possibilities for individuals to control or restrict the flow of personal information but the market in personal information tends to place the burden and cost of this on the citizen. Since information about people is a resource for organizations, they might collect as much as they can unless internal or external costs become too high. Organizations are unlikely to act unilaterally to make their practices less privacy invasive. Unless choices are easy, obvious and cheap, people will probably go with the default position and that is, in cyberspace, more likely to be privacy invasive. As a result, the privacy level available online is less than that which is required by the norms of society and people's stated preferences.<sup>56</sup>

## The basics

With Ambient Intelligence, the monitoring and surveillance capabilities of new technologies can be seriously extended beyond the current possibilities of for instance credit-card and shopping records (e.g. consumer loyalty cards), Internet logs (e.g. e-mail, news postings, discussion forums) and detailed phone invoices. Some argue it might even mean the end of privacy<sup>57</sup> since it will be very difficult for people to find a place where they can be left on their own; a space where they will have 'the right to be left alone', the latter being one of the first definitions of privacy, developed by Samuel

Warren and Louis Brandeis in 1890.<sup>58</sup>

Virtual residence should exactly be that space, a legal sanctuary similar to the protection of the physical residence but than in a networked society. The following elements detail the main constituents of the concept of VR. The core issues of identity, privacy and security will be clarified for each of these basics.

## Territoriality, proximity and personal/residential space

The concepts of territoriality, proximity and personal space have been studied extensively in the past, from many different angles and in many different ways. It is our purpose here, to demonstrate that these concepts are crucial to understanding the privacy, security and identity implications of VR.

Social relations are managed, amongst others, via proximity and distance to others. The physical barriers of proximity that regulated access to persons and to personal information in traditional societies are disappearing in an Ambient Intelligence environment. This is related to territoriality. According to Altman (1975: 125), territoriality in particular human territory – which is different from animal territory – is defined as a 'self/other boundary regulation mechanism involving personalisation or marking of a geographical area and the communication of 'ownership' by its users or occupants'. Territorial behaviour is then described as a series of mechanisms to regulate routine social interaction. Establishing territories and accepting others territories are ways of stabilising social interactions.

There are three main categories of territory, depending on their degree of importance and permanence of use of its occupants:

A primary territory over which the individual has complete control (e.g. body);

A secondary territory still controlled by the individual/group but not completely. It is a space

<sup>55</sup> Tavinim H.T. & Grodzinsky, F.S. (2002) Cyberstalking, personal privacy and moral responsibility, *Ethics and Information Technology*, 4, 123-132.

<sup>56</sup> Regan, Ibid: 397-400.

<sup>57</sup> E.g. Garfinkel, S. (2001) Database Nation. The death of privacy in the 21st Century. O'Reilly, 2001.

<sup>58</sup> Warren, S. & Brandies, L. (1890) The Right to Privacy, *Harvard Law Review*, Vol IV, No.5. [http://www.lawrence.edu/fac/boardmaw/Privacy\\_brand\\_warr2.html](http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html).

that is negotiated and agreed upon with others. (e.g. your house);

A public territory characterized by free access but with a temporary quality of, for instance, more individual control (e.g. public phone booth, public toilet).

The seriousness of territorial encroachment and its reactions to it vary according to when a primary, secondary or public territory is at stake. Virtual Residence is to be situated at the level of secondary territory since it is based on a claim of ownership of a personal/residential space. One can 'declare' a VR, so to speak, as a result of (implicit or explicit) negotiation with others. One has control over the VR but it is not an absolute control.

The VR thus is a personal/residential territory but than for the digital environment. As a result, since territorial behaviour deals with regulating social interaction, digital social interactions need to be managed via the VR. Territorial behaviour can be exercised through the management of the frontiers or boundaries. According to Hall,<sup>59</sup> personal space is usually translated into physical distance from others. VR is thus also about the management of proximity and distance with others in this future Ambient Intelligence space that is characterised by a collection of technologies, infrastructures, applications and services across different Aml environments (car, home, the neighbourhood, the city, etc.). Depending on distances, the nature of these territory changes and its owner has less and less control. Boundary regulation is an important element in the protection of property. Boundary regulation needs to be dynamic since their permeability changes with the circumstances.

With a defined digital territory in this Aml space, the individual will not permanently need to negotiate who belongs where or who has rights to what. Using the VR for that would be a solution to providing stability for social interactions in the digital world, similar to the one in the physical world where people do not have to negotiate territories and personal space all the time.

Privacy can thus be considered as a dynamic boundary regulation process.<sup>60</sup> Personal territory and the boundaries around it can also be seen as 'soap bubble', according to Sommer.<sup>61</sup>

The management of digital territories via its boundaries is elaborated more in detail in the next section. Another important element is the marking of VR as a territory, as will be dealt with in the section on indicators.

### Boundaries and border crossings

A residence is by definition a limited territory designed by boundaries. These limitations permit to express and enforce specific rules which are implemented exclusively in this dedicated space. In the physical world, the borders of everyday life spaces are characterised by great diversity but they are the result of socio-cultural, legal and/or economic rules and motivations. Fences are commonly used to establish the borders of a residence for instance, but depending on the social context, it might be less tolerated or more dangerous to cross the open grass of a US residence than crossing the gate of a European one. In both cases however, indicators or markers are available to inform others where public space ends and private property starts.

Residence boundaries are not only set and operated by the owner of the residence. The well-known quote 'one person's freedom ends where another's begins' underlines that boundaries regulation is both an individual and collective concern. One of the roles of public authorities is exactly to guarantee a certain balance between both. The boundaries of the Virtual Residence should also be seen as resulting from both the individual and the community.

Its digital borders have to be considered as an extension of the physical ones and should then both ensure responsibilities and protect rights. If the physical residence is seen as a legal sanctuary, therefore the virtual residence delimited by digital boundaries will gain the same nature: a digital legal sanctuary. Comparable to physical borders, the digital boundaries can take various forms (e.g.

<sup>59</sup> Hall, E. T. 1966. *The Hidden Dimension*. (1st ed.). Garden City, N.Y.: Doubleday.

<sup>60</sup> Altman, I. 1975 *The Environment and Social Behaviour*, Brooks / Cole Monterrey

<sup>61</sup> Sommer, Robert. 1969. *Personal Space: The Behavioral Basis of Design*. Englewood Cliffs, New Jersey: Prentice-Hall, Inc.



explicit - implicit, strong – weak). Contrary to the physical borders of the traditional residence however, the ones of the virtual residence are more dynamic and changeable. We could for instance imagine a temporary dedicated space within the virtual residence that is used for professional purposes, following the trend of blurring of the boundaries between work and home. Specific privacy and security frameworks for that temporarily work-space could than be established.

According to Gary Marx, people experience an invasion of privacy when borders are crossed. He identifies four borders and argues that new technologies create new opportunities for 'border crossings'.<sup>62</sup> These borders are:

**Natural borders:** Walls, doors, cloths, darkness, but also sealed letters and telephone calls protect personal information and activities; and indicate private spaces. What you 'normally' or 'naturally' can sense (see, hear, smell) or comprehend when your presence is not hidden, is regarded as public. It means that you are entitled to perceive it, although not necessarily to share it. Sensors attached to the body measuring temperature and hart beat in order to assess if someone is nervous during a conversation (e.g. job interview) would be a future Aml example of natural border crossing.

**Social borders:** Social norms and rules indicating expectations about confidentiality and its varying degrees according to the position of people in social networks (e.g. family members, doctors, or judges, colleagues at work). Reading a fax or photocopy that you happen to see but that belongs to others can be regarded as privacy invasive. In the future Aml space, an example of social border crossing would be to identify people via biometrics when entering a shop in order to check their credit history that is stored in other databases.

**Spatial and/or temporal borders:** People may prefer not to convey their complete lives to everyone, but only different parts of it to different target groups. There may be a need for them to remain separated, both in time (e.g. employer knowing about the sins of your youth) and space (employer knowing about your current leisure activities). These borders involve assumptions about the compartmentalisation of ones' personal biography. Crossing these borders may be perceived as privacy invasive, for instance when face recognition software allows people to check if someone is present at a publicly broadcasted event (e.g. via webcam).

**Ephemeral or transitory borders:** Interactions, communications and remnants such as garbage are fleeting, like a river, and are expected not to be captured or preserved (e.g. a slip of the tongue or an everyday life bloomer should not follow people eternally). Things (e.g. information) may get lost and have the right to get lost. The memory amplifier or Life Recorder example mentioned below indicates how these borders can be crossed in the future Aml space.

Central to border crossings are ideas about what is public and what is private, about where the private person stops and the public person begins. The problem is not only that the borders between both are fluid, relative, multi-dimensional and dependant on context, situation, culture and personal preferences<sup>63</sup> and therefore difficult to generalise, but also that with new Aml technologies, the crossing of these borders becomes easier and possibly more likely. In the name of personal, private or public/national safety and security, monitoring and surveillance could be done by individuals (e.g. spying on your neighbours<sup>64</sup> or on other people<sup>65</sup>), companies (e.g. tracking products<sup>66</sup> and making consumer profiles) and states. Without effective privacy and data protection measures, this

<sup>62</sup> Marx, G.T. (2001) Murky conceptual waters: the Public and the Private, *Ethics and Information Technology*, Vol. 3, No. 3, pp. 157-169.

<sup>63</sup> Marx proposed to differentiate between the individual, the intimates, selected others, formal relationships and the rest for determining whether information is private or public, rather than looking at a private or public space as such.

<sup>64</sup> Privacy invasive threats are usually defined as coming from governments and/or private companies but with Aml technologies becoming available for everyone, people could start to watch each other. Already today, with wirelessly connected CCTV (Closed Circuit TV) it is possible to watch your neighbors with security cameras installed to protect the home. The former obviously raises privacy concerns. See for instance: 'Wireless cameras raise privacy fears', *Newscientist*, 17 May 2003. <http://www.newscientist.com>

<sup>65</sup> Just recently, the president of the YMCAs of Australia proposed to ban all mobile phones with a camera from swimming pools across Australia as a 'proactive response to a potential problem' (illicit photographs). BBC Online, 'Australia bans mobiles from pools', 12/06/2003. <http://news.bbc.co.uk/1/hi/technology/2984780.stm>

<sup>66</sup> Cf, infra examples of Benetton or Gillettes.

brave new world of smart environments and interconnected objects could become an Orwellian nightmare.<sup>67</sup>

Also new opportunities for border crossings could emerge with personal information and/or activities that were once thought to be meaningless or harmless. Consider, for instance, an application that is developed allowing people to record, store and search for all conversations they had in the past. Some call it a 'memory amplifier',<sup>68</sup> others a 'Life Recorder'.<sup>69</sup> It has the advantage that people would never forget anything and any statement made, not only of the person himself but also of the interlocutor, is recorded and stored for possible use afterwards (and even many years later).<sup>70</sup> This clearly indicates the crossing of ephemeral and transitory borders. A private conversation is no longer private since extracts or even the complete conversation could be disclosed to others at any time and place in the future.

### Indicators

One of the problems today is that there are very little indicators for what is public and private in the digital realm. Not only are there privacy concerns about accessing private spaces that have no clear indicators or that give no prior indication that they are private, but there are also concerns about the digital footprints people will leave behind in the future Aml Space. Internet users, especially newcomers, typically assume that their activities in cyberspace are private since no one in physical space is observing them as they use their computers. However, 'click stream data' or 'mouse droppings' leave 'electronic footprints' that become a detailed digital record. Unless they have been explicitly made aware of this fact, they may not realize this is occurring.

The automatic capture of personal information via IP numbers or cookies for instance is not clearly signalled and users are not always well in-

formed about it. As Regan<sup>71</sup> notes, 'the rules of the cyber-road are not clearly posted... Because of the non-obvious nature of cyber-tracking, some visual cues about when and how tracking occurs may be necessary in order to make cyberspace somewhat more comparable to what people have become accustomed to in physical space'.

It could be argued that today Internet users do have knowledge of the collection and possible use of personal information because 'privacy notices' or 'information practice statements' on websites, but these are typically small font notices that users have to look for. Visual labels could be more effective. People may also be unaware that personal information about them is available via search engines.

The need for labelling has recently also been stressed by Simon Garfinkel, a columnist for the MIT Journal Technology Review, related to spyware. He proposed mandatory labelling of the features of software programs. Spyware programs either record the actions (e.g. keystrokes) of computer users for later retrieval or automatically report on computer actions over the Internet, without the users knowing about it. The problem is often that it happens with the user's explicit consent, by clicking on the 'I agree' button when installing a program. Hardly anybody reads these license agreements however. There are technical means to deal with spyware programs but another way to fight it would be to impose uniform labelling of software. Such legislation would be similar to the US Pure Food and Drug Act of 1906, i.e. the legislation that is responsible for today's labels on food and drugs. Such legislation could be called the Pure Software Act of 2006 and would force makers of spyware to reveal their program's hidden features.<sup>72</sup>

### Storage

The issue of storage is at the core of the Virtual Residence concept. The increased digitisa-

<sup>67</sup> Mattern, F. (2003) Ubiquitous Computing: Scenarios for an informatized world, ETH Zurich, Paper to be published. <http://www.inf.ethz.ch/vs/publ/index.html>; Bohn, J., Coroamă V., Langheinrich, M., Mattern F. & Rohs M. (2003) Disappearing Computers Everywhere. Living in a World of Smart Everyday Objects, Paper for the EMTEL Conference, London 23-26 April 2003. <http://www.emtelconference.org>

<sup>68</sup> Bohn, J. et al., Ibid.

<sup>69</sup> See for instance [www.motorola.com](http://www.motorola.com); [www.mit.edu.com](http://www.mit.edu.com); [www.nokia.com](http://www.nokia.com). (Lifeblog project); [www.research.microsoft.com](http://www.research.microsoft.com) (SenseCam project)

<sup>70</sup> It is assumed that technologies for archiving, searching and indexing will have further matured.

<sup>71</sup> Regan, P.M. (2002) Privacy as a common good in the digital world, *Information, Communication & Society*, 5:3, 382-405.

<sup>72</sup> Simson Garfinkel, The Pure Software Act of 2006, The Net Effect Column Series, April 7, 2004, Technology Review.

tion of our everyday lives means that more and more data on our activities will become available in digital format. All that data does not per definition has to be stored but much of the value added services that Aml can provide is based on available and thus stored data. Think of the beta-initiative of Google launched in March 2004, providing one gigabyte of free Web-based mail storage in exchange for context-sensitive advertising. Apart from the controversy it caused on possible privacy breaches since e-mail content is scanned – although only by automated software – it shows that storage is not only becoming ubiquitous but also relevant for providing context-sensitive services. Google even argued against throwing away mails since you never know how useful a mail can be in the future.<sup>73</sup>

Virtual Residence can make sure that stored data are secured and private but VR storage does not necessarily mean storage within the home. In principle, VR content can be stored anywhere, i.e. in the house or with third party providers (e.g. Gmail).<sup>74</sup> It can also be stored on portable barriers such as smart cards, memory sticks and e-clothes, and even on chips implanted in the body. Storage can be distributed (automatically) as well amongst all these different spaces.

Privacy and security mechanisms may be different with own storage versus third-party storage but with Ambient Intelligence, the physical location of storage becomes less and less relevant. The level of privacy and security will be more defined by the location from where the data are required or accessed, than the place where they are really (physically) stored. The interactivity and connectivity of the nearby environment of the user will become more important for privacy and security. Identity management systems (IMS) can regulate access.

Mainly three kinds of data which will be stored by different players can be described:

- The users store some data in their virtual residence space.

- The nearby environment of the users which is considered as an Ambient Intelligence space collect data and store them in the VR space.
- Outside users store data in the VR space. They can be friends or other members of the family, or third parties from the company who manage some facilities delivered to the smart home, to public or e-government services.

The implementation of the concept of Virtual Residence is expected to have an impact on the two main dimensions of storage: from where the data have been requested and/or collected, and the nature of the data itself.

## Interfaces

The concept of virtual residence can be seen as a virtual representation of the smart home. It could be used as a mental map to manage security and privacy, both remotely and from within the home. Today, 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 users judge 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 this new Aml space. Virtual residence could be used to represent the online private space of people, families or households in Ambient Intelligence and it could enable the creation of new ways of living in cyberspace. It could be a mental model and virtual space on its own for dealing with the definition of public and private in the online world and thus for managing personal identities,<sup>75</sup> privacy and security.

The concept of virtual residence could contribute to clarifying the difference between public and private by way of providing a visual and mental model for representing the online private space of people, families or households in Ambient Intelligence. It could be used as a mental map and

<sup>73</sup> See for article on Gmail: <http://www.google.com/press/press.html>

<sup>74</sup> See also section on e-entertainment and the example of a collective family entertainment server.

<sup>75</sup> Hansen, M. & Berlich, P. (2003) Identity Management Systems: Gateway and Guardian for Virtual Residences, Paper for the New Media, Technology and Everyday Life in Europe (EMTEL) Conference, London, 23-26 April 2003. <http://www.emtelconference.org>

virtual space on its own for dealing with public and private in the online world, in the same way as the digital city metaphor is used for online public life in a city.<sup>76</sup>

The virtual residence would then become a user interface for people's online lives based on a representation of the characteristics of a physical residence, with rooms, doors, bells, etc, and their corresponding subtleties of leaving a door for instance half open. It would not only provide a 'look and feel' of where perceived levels of privacy are important, but it would also take the context of specific activities into account. For example, a visitor could be taken into a specific virtual room implying certain social and privacy related rules and norms; a colleague would join you in the study room, automatically establishing the working context by opening the right files, putting other data into the background. Not all boundaries of the virtual residence have to be known from the start, but can evolve and change over time in the same way as social norms and values are elaborated in the physical world. Users may benefit from the virtual residence metaphor as an interface for Identity Management Systems whereby the user remains in control of his/her privacy and private space.<sup>77</sup>

### Access control

An identification system is a prerequisite to the implementation of an access control policy for the VR. Indeed it seems desirable to define several level of access among the users connected to the smart home. Even among the members of the residence, a hierarchy of access is necessary regarding the relationship between the members of the group. In the case of a family, the parents will probably appreciate to restrict the access of their children's to some specific data of connected facilities. Simultaneously the privacy of each members (the children as well) of the family has to be taken into account.

Therefore, the way the users are identified by their VR, in this case the smart home, will have a direct impact on the easiness they manage their privacy.

In the case of RFID tags and even more with a contact less ID card, the user still have the easy possibility to be left alone by dropping his/her card in the basket. For the RFID tags this 'switch off' action will be challenging by the ubiquity of these tags in all of the personal items of the users (shoes, watch, pullover, underwear, etc...)

In the case of embedded chips, the so-called biochip or even biometrics systems, access to the smart home could be granted via biometric identification methods and as such, there would be no direct privacy threat involved so long as the system is just event driven. But when access data are stored and time stamped, the system is likely to become privacy invasive, since it can reveal the time a particular person entered or left the home. Another crucial question related to time is how long the data are stored: is data retained for a specific period of time or for ever? When time stamped data are stored, privacy invasion likelihood increases. There is a difference between a computer having a record of the movement of objects from one room to another (e.g. beer from the kitchen to the living room) and having exact data on who drinks what, at what time, in which room (e.g. controlling children's behavior).

### Location

High accurate location capability constitutes one of the main success factors of the future ambient intelligence spaces. Indeed, in order to provide suitable and personalised services, this intelligent environment needs to locate the potential beneficiary. The objective can be to 'follow' the individual with some specific data and keep them available independently of the place or because of the specificity of the location, to allow dedicated access to some particular data.

The implementation of VR is concerned by both of these situations and will simplify the usage and protection deployment for these data. If a user is located inside the residence, he/she might have access to a certain domain of the VR data which would have been inaccessible outside the boundaries of the residence independently of his/her identity. The dichotomy of the VR storage can be

<sup>76</sup> E.g. Lieshout, M. J. van (2001) Configuring the digital city of Amsterdam - Social learning in experimentation. In: *New Media & Society*, Vol 3 (1) pp. 27-52.

<sup>77</sup> Hansen & Berlich, Ibid.



also applied in the residence were some rooms can be link to specific ambient intelligence services or more basically specific data.

### **Presence: bridges between the physical and the virtual world**

As parts of our lives become increasingly digitized, our notion of presence will most likely change. Emerging in the context of virtual reality, research on presence focuses on the *experience of being there*. It is defined as a psychological state in which virtual objects are experienced as actual objects in either sensory or non-sensory ways. The question then is: 'How real is the virtual residence'? In order to see it as real, people's awareness of a medium that is presenting something as 'real' has to be minimised. Some traditions of research on presence focus on perceptual experience, which is central to theorising about advanced human-computer interface systems. Such an approach studies the workings of the brain, and seeks to learn how it be 'tricked' into perceiving virtual stimuli as if they were actual stimuli.<sup>78</sup>

Research into presence is today not limited to a particular academic tradition, nor is there a theory of presence (yet). Neuroscientists, psychologists and philosophers are approaching the matter according to their own perspectives (e.g. Artificial Intelligence, Virtual Reality, brain technologies) but also interdisciplinary enterprises are under-

taken with the objective to develop novel media that can better convey a sense of being there.<sup>79</sup>

But research on presence illuminates that the question 'How real is the virtual residence' may not be the crucial issue, but rather 'How do people think, act and feel in their virtual residence'? Important for understanding VR for that purpose is that its operationalisation needs to go broader than a traditional stimulus-response psychological framework. Virtual Residence requires an account of presence that includes the social and relational dimensions of on-line interaction. Users will not only perceive stimuli through their VR, they will also interact with virtual objects, with others and – in one way or another – with themselves.

Lee offers a broad typology of presence, which helps clarify its relevance for discussing VR. First, objects can be virtual in two ways: *para-authentic* or *artificial*. A para-authentic virtual object is one that represents an actual object: a virtual tour of the Alhambra in Granada is para-authentic, for it aims to reproduce the experience of actually being in the Alhambra (see <http://www.arsvirtual.com>). An artificial object, however, has no actual counterpart. Lara Croft's adventures in Tomb Raider, for example, are completely artificial (if deeply engrossing for some). These two characteristics of virtuality can be situated in three domains of virtual experience, i.e. physical, social and the self, as is illustrated in the following table:

<sup>78</sup> Lee, K.M. (2004). Presence, explicated. *Communication Theory*, 14(1), pp. 27-50.

<sup>79</sup> See for instance:

Anania, L. (2003). What do we need presence for? *Cognition, Technology and Work*.

Heeter, C. (1992). Being there: The subjective experience of presence. *Presence: Teleoperators and Virtual Environment*, 1(2), 262-271.

IJsselstein, W.A. (2002, invited paper). Understanding Presence. *Proceedings of the AIIA 2002 'Workshop sulla percezione della presenza in ambienti virtuali o remoti'*, Siena, Italy, 10-13 September 2002.

Table 1: A typology of social experience, Lee (2004).

Domains of virtual experience	Characteristics of virtuality	
	Para-authentic	Artificial
Physical	Experience of para-authentic physical objects; i.e. objects that have an actual real-life counterpart. E.g. virtual 3D tour of tourist attraction, television news.	Experience of artificial physical objects, created or simulated by technology. E.g. video games, science fiction films.
Social	Experience of para-authentic social actors; i.e. connecting with other humans through technology. E.g. email, photographs.	Experience of artificial social actors, which are not human but convey humanness. E.g. interacting with robots or software.
Self	Experience of para-authentic self, i.e. one's own, actual, self but mediated through technology. E.g. seeing oneself in a teleconference, hearing one's voice on a tape.	Experience of an artificial alter-self/selves, which is/are constructed inside a virtual environment. E.g. adopting an identity in a chat room, identifying with a film character.

This typology shows that there is more to presence than perceptual realism and that the study of presence in relation to VR requires a multidimensional approach which takes into account these different elements involved in providing a sense of *being there*. Future research on VR should build on this typology in order to better understand issues such as people's sense of security, privacy and identity in a VR environment.

Psychological research also has made clear that people tend to respond to media in similar ways as they respond to the social and physical environment. In this regard, media equals real life, according to Reeves and Nass.<sup>80</sup> They argue even the simplest of media are close enough to the real people, places and things they represent to spark genuine natural and social responses. This is true for *all* people, regardless of profession, age, gender, education, etc. Occasionally, people will not take the virtual as real, but the 'default' option is to equate media with real life. This yields the overall conclusion that people will – essentially – trust, feel safe, and interact with media (including the technologies that allow for VR) following the norms and expectations of social life. If media and real life are the same, or at least acted upon in the same manner – then knowledge of how people respond to others should reveal a lot about how people respond to media, and vice versa.

The 'phenomenology of virtual residence' is also a viable alternative for understanding how people think, act and feel in their virtual residence. From this point of view,<sup>81</sup> the concern is not the degree of 'reality' which a virtual environment can achieve – instead, this environment is taken *as if it were real*. Interactions with a virtual residence are real since *they appear to be real*. Further research is needed in this regard to know if people think, act and feel the same in their life on-line as in their life off-line. In particular, research should focus on differences in the perception of risk in both milieus. If a VR environment creates greater feelings of uncertainty, then higher levels of trust will be required for people to feel safe and protected from intrusion. Specific tools and systems (both technical and non-technical) might be required to ensure those levels of trust and guarantee greater acceptance.

By understanding computer-mediated interaction as another element in individuals' lifeworlds, and by acknowledging the empirical results which suggest that media equals real life, the 'virtual' will, at some point, be dropped. VR will simply be an extension of people's residence, subject – in principle – to the same beliefs, feelings and behaviour of residents as always. This is characteristic for the user-oriented way VR is defined from the start. The blurring and progressively eroding boundaries between the real and the virtual world should support the acceptance of Ambient Intelligence.

<sup>80</sup> Reeves, B. and Nass, C. (1996) *The Media Equation: How people treat computers, television and new media like real people and places*. Cambridge: CUP.

<sup>81</sup> Berger, P. and Luckmann, T. (1967). *The Social Construction of Reality*. London: Penguin.



## 4. Possible application fields for VR

### E-entertainment/culture/leisure/education: the example of a collective family server

The collective family server should not be restricted to traditional entertainment needs. It also contains digital assets related to hobbies, leisure, culture and education. Moreover, the family server is the place where not only bought or subscribed entertainment content will be stored but also where user-produced digital content will find its place. The CR should indeed not be seen as a distribution system for digital content but also as places where self-generated multimedia content is available for others.

Copyrights on music (CD) or movies (DVD) for instance, expect that these are used only for private listening and viewing. A person can watch his DVD wherever he/she likes (at home, in the car, at work, at the hotel) as long as he carries the (original) copy physically with him. But already today, it is not necessary anymore to have a physical copy. Millions of Internet users shared during the last years digital music files via peer-to-peer computing. More recently, licensed music-swapping services are offered by many different companies. Apple's iTunes is a current well-known example of an online store that features more than 700,000 songs. Recently also Sony launched an online music shop called Sony Connect.<sup>82</sup>

In the future, it is expected that digital storage of entertainment will increase considerably and that viewing or listening will therefore not be restricted to having a physical copy. It is easy to imagine the digital storage of family entertainment on a family server which is accessible not only in the home, but also outside and on the road. Virtual Residence could be the virtual space where all the family entertainment – defined broadly as mentioned above – is stored and that grants (legal and social) access to its use by the members of the family who may be at geographically distant locations.

A collective family entertainment server would have many advantages. Basically it would make VR content accessible anytime, anywhere

and to anyone (allowed). Also users would need less physical space in the home for storage of material while available content and choice would increase. More diversity of content will be possible through personalisation and customisation and increased flexibility through permanent and location-independent access to the content. Quality time management was also mentioned in the VR questionnaires to deal with dull moments in life (e.g. waiting time) and with unexpected free time. It would also be easier to categorise and classify content during these spare moments. Retrieval of content would in principle also be facilitated. Other would argue against this efficiency view because 'empty' moments in life are also important

An important issue related to the family entertainment/culture/leisure server is storage. Virtual Residence storage should not be equalled with storage within the home. In principle, VR content can be stored anywhere, i.e. in the house, with third party providers or at distributed locations. Rather the question is how to personalise or familiarise content that is owned by the family but only in digital format and, that is not necessarily stored at home? Physical copies give a certain authenticity to non-tangibles. People have intimate objects. Their looks and design play a role in the way people construct and maintain their identities. The VR needs to contribute to the feeling of owning the content; otherwise people will not accept it. Experts believe also that storage would be preferred above on-demand retrieval because own storage increases the feeling of being in control over the content. Security mechanism may be different with own storage versus third-party storage and online retrieval but in the end, not only storage but also (remote) access need to be considered.

The VR family server has the purpose of making clear that cultural preferences are to be protected by the notion of freedom of expression (first amendment). Initiatives such as censoring explicit lyrics and banning pornography are in contradiction with this right. Digital storage outside the physical house should not be an excuse for infringements that limit freedom of expression.

Digital content for entertainment, culture and leisure stored within the VR would also give rise to

<sup>82</sup> Sony's online music shop opens in iPod's shadow, FT.Com, May 6, 2004.

possible new business and/or revenue models (e.g. use-based pricing schemes). New types of content demand could arise based on tightly defined personal needs. Moreover, having a common space for digital content might contribute to new ways of sharing content amongst family members and peers. This could give rise to new and unexpected (grassroots) uses. Finding revenue models for the VR model will be needed to get industry support for such an initiative. A single administrative domain would also simplify digital rights management from a business perspective. It remains to be seen however if VR will lower or increase consumer spending to entertainment.

All this will require a re-assessment of digital copyrights. In the same way as for instance someone can step into your car and listen to 'your' music, one should be able to invite others to access and enjoy – perhaps temporarily – VR content. Instead of limiting users to a fixed numbers of digital copies, anybody with access to the VR should be allowed to listen to it, just like a song playing on the home stereo can be heard by all people in the home. VR could be a concept to clarify new copyright issues for the private digital sphere. In physical private space, it is well understood that one is allowed to play music and show copyrighted material without having to be afraid of being sued for copyright infringement. Virtual meeting places do not (yet) have the same private character. Moreover, in contrast with physical meetings, virtual encounters often require identification. But how to let others enjoy any copyrighted material decorating yourself or your Virtual Residence without the risk of breaching copyright laws. People should be able to transmit their digital media to selected recipients through public networks, in a secure and private way. This would be part of the VR.

A major challenge for the realisation of the VR family server will consist of the management of these digital assets, at different levels. Several approaches for security and privacy policies are possible. VR could be of value if it can integrate those policies within a 'domestic' framework that facilitates their understanding by the family members. VR would be a comprehensive and effective way

for managing and enforcing the security and privacy policies of the family. Some experts see it as the single container concept for all digital aspects related to the private sphere.

There is the issue of categorisation, classification and the maintenance of the systems of content retrieval. Also, there is the risk of a possible loss of face-to-face interactions since information and content can be exchanged digitally and thus without in-real-life physical interaction. This does not have to imply however that social interaction within the family would diminish. It can be argued that virtual communication facilities will increase since sharing a digital space requires social interaction, in contrast with individualised storage and management.

The Virtual Residence will need to find a way to respect however, privacy requirements within the residence. Having a common digital space does not imply everything will be shared within the virtual residence, nor that everything will be visible to everyone. The VR will need to find ways to deal with privacy implications of a wide range of different relationship amongst couples, parents, parents and children, children amongst each other, and, all of these with other people.

This is also a question about control. Users might feel too controlled by centralized systems. Anecdotic evidence from Philips' Ambient Intelligence Homelab – i.e. a fully equipped semi-real life home to test prototype Ami technologies and peoples' reactions to it – raised the issue of power relations in social interactions amongst family members.<sup>83</sup> Who controls these intelligent systems and how to deal with hierarchical positions within these relations? And who is to blame when something goes wrong?

Both opportunities and threats for this common digital space seem to come from ongoing and future demographical and socio-economical trends in Europe, such as an enlarged Europe, the aging society; increased mobility, the mosaic society; diversity and choice of personal life styles, affecting the structure of groups and communities and the way people live and work. Household structures (family size and composition) are chang-

<sup>83</sup> Aerts, E. (Ed.) (2002) Ambient Intelligence in HomeLab, Published by Philips Research for the occasion of the opening of the HomeLab on April 24, 2002, Philips Research, Eindhoven. <http://www.newscenter.philips.com>

ing as well, with a decline of traditional nuclear families and an increase of dual income households and single parent/single person households. How for instance, will deal a shared virtual residence with divorce and separation? Access to and perhaps ownership of for example digitally stored pictures and sound recordings will have to be agreed upon.

### **E-government: taxes and acquisition of citizen's rights**

A nation administrated by a government exists because it delivers to a group of individuals a citizenship based on rights and duties. This citizenship is built on mainly two constitutive elements: an identity set up with some identification tools and processes, and a location or residence. But the growing Information Society and its continuous process of digitisation are challenging now these two pillars of citizenship. The erosion of space and time dimensions and the disembodiment of electronic communication constitute major issues for the government and its relationships with its citizens.

In the future, e-government services are expected to become a natural and determinant part of the citizen every day life. These emerging applications figures as well as one of the most important policy objectives for a sustainable development of the European Information Society.<sup>84</sup> The efficiency and usefulness of e-government are critical dimensions for the citizen, not only because it has to provide the required public services but also because it is intended to create trustworthy environment and bridges between the citizens and the other private actors.

In numerous forecasted e-government services, proof of people's residence or location appears to be sufficient when identification for access to these services is required. Thus, the declaration or registration of residence empowers individuals who live in this residence with a bunch of rights and potential services delivered by the government. Today, free entrance to museums is offered in many cities for city inhabitants providing they can prove they live in the city. Provision of

this evidence thus requires some form of identification but not necessarily full user identification (e.g. name).

Virtual Residence could be the gateway through which new e-government services that require identification are delivered. It would protect privacy by only providing necessary rather than full identification by serving as a central point of requests or transaction issued from different administrations to the benefits of a group of people, usually the family who leaves in the residence. Being a member of this digital household represented by the virtual residence will then confer some rights attributed by the local and or national authorities.

On the side of the government, administrative registration of VR could also be useful in order to collect local taxes generated by e-commerce as the latter is location independent. Indeed, with reduced tax revenue,<sup>85</sup> it might become critical to provide and to maintain local services.

By promoting the implementation of VR, e-government can become a real driver force for a better acceptance of ambient intelligence space considering its institutional role of trusted third party, and go beyond the limited relationships between the citizen and its public authority. Indeed, the registration of VR which will primarily facilitate the development of e-government services can also reinforce the notion of virtual legal sanctuary and therefore offer simultaneously to the citizen a well publicly protected digital space for his/her life online. The personal data which are used for e-government services as well as the citizen's ubiquitous/distributed storages will receive the protection and the authentication of the government (law) for other social or economic transactions. The objective is not that the e-government will manage the storage data but it will have to assess and guarantee that the numerous private storage providers implement the state of the art of privacy and security measures and comply with the concept of VR: a digital legal sanctuary.

By recognising administratively the Virtual Residence, the government will then offer VR an institutional protection it already provides to the

<sup>84</sup> e-Europe 2005 goals.

<sup>85</sup> State and Local Sales Tax Revenue Losses from E-Commerce: Updated Estimates, Donald Bruce & William F. Fox, Center for Business and Economic Research, University of Tennessee, September 2001. <http://www.statestudies.org/ecomreport.pdf>

physical residence. This policy option will not only reinforce the evolution toward e-government, but it will also favour a greater acceptance of this new environment by raising trust.

The administrative recognition of a virtual residence can also play a role in favour of a reduction of social divide by offering the rights usually to a residence for people who might not have a permanent domicile. Of course, this VR potential impact supposes that in the same time free online access will be available.

### E-health: family medical dossier

Today, medical files are primarily managed by medical institutions and not by the patients themselves. In the future, medical information will not only be gathered via existing institutionalised forms of medical diagnosis (e.g. visit to the doctor, hospital check-up, etc.) but also via direct sensor-based monitoring, at different levels: in the body (implants), embedded in clothes (smart fabrics) and at dedicated places such as the smart home. All this information can be stored in medical files of individuals and families/households.

Also, given the current and future budgetary pressures on healthcare systems (e.g. as a result of the aging society) medical services will increasingly be delivered in the smart home. This is reinforced by the fact that the smart home will enable in-house monitoring of medical data. Health information monitored in the smart home also 'leaves' the home because of its connection/communication with external institutions (doctor, hospital, social security, etc.) and external resources (grid, distributed computing, remote software). Also, this information does not necessarily need to be stored in the home network but can be stored elsewhere, as long as the data are protected. Data will have to be accessible remotely however.

Placing sensitive medical information in the VR would protect the medical files as belonging to the private (digital) property, similar to the protection the physical residence has today as a private space. This would also make clear that the property of medical data is in the hands of the patient. Using the VR as interface would allow the man-

agement of access rights, i.e. making sure information is disclosed only to those who have access rights. The typical example here is employers, or future employers wanting to know as much medical information as possible before offering people a job. The VR would facilitate establishing a security model for health data access controlled by the users themselves.

The generic advantages of e-health are well-known: better and more efficient healthcare, helping people to live longer and increased autonomy and convenience for special populations (old, disabled, and sick). More specific advantages are: easy access to various medical experts and to second/third opinion diagnosis, early diagnosis about health problems, tracking health problems and better record keeping. There are also risks to e-health such as the loss of personal contacts and social interactions at the expense of virtual and remote encounters. But there are also new opportunities for sociability offered by Aml. Cabrera and Rodríguez describe for instance a scenario whereby Aml-based assistive technologies enable elderly people not only to live autonomously for longer but also to retire elsewhere while staying connected at the same time.<sup>86</sup>

More specifically related to the role of a VR for e-health, it is important to differentiate between different facets of e-health such as:

- Users/patients sending data to medical experts and vice versa;
- Remote diagnosis and possible treatment over (broadband) networks;
- Emergency medical treatment and access to medical data;
- Permanent, sensor based monitoring of persons medical status in the home;
- Intelligent agents for analysing medical data: e.g. early warning systems.

Especially storage, remote access and communication seem to be crucial issues given the risks for privacy breaches and thus the need for secure protection of data and communications. VR can play an important role here. The videolink

<sup>86</sup> Cabrera Giráldez, M. & Rodríguez Casal, C. (2005) The role of Ambient Intelligence in the Social Integration of the Elderly. Book chapter in 'Ambient Intelligence. The evolution of technology, communication and cognition towards the future of human-computer interaction' G. Riva, , F. Vatalaro, F. Davide, M. Alcañiz (Eds.), IOS Press, 2005, <http://www.ambientintelligence.org> '



used for remote consultation would than be regarded as private and thus protected.

Any remote access to medical information might be problematic however. Some experts believe a local storage solution (e.g. smart card) would be preferred by both consumers and health professionals. But it is also acknowledged that secured back-up records are needed.

Also ownership is an issue. It is not just about rights to one's own health information. There is a difference between data and interpretation. Doctors might be reluctant to give results of individual tests because they want to give an overall diagnose putting together all the evidence. How will this be dealt with? There may also arise some difficulties if it becomes possible for the patient/person to forge/destroy his/her medical records. This could affect social security schemes or insurance companies.

There is legal concern that the residence analogy might diminish the protection of medical data since in some cases, medical data are today better protected than the residence. But there might be a need to preserve some flexibility so that for instance, the collection of aggregate data for statistical purposes and for health governance would still be possible. Individual protection and societal benefits should go hand in hand.

### Smart home: critical domestic infrastructures

Today, the residence is already composed of sensitive infrastructures but they are not really interconnected and their level of dependency on information is relatively low.

In the future, the smart home will have complex and intertwined networks in order to increase the connectivity, the interaction, and the 'intelligence' of home devices and services. This environment will contain many smart devices able to sense activity in the home and able to communicate this information to other appliances, people and networks, both within the home and outside the home.

Security will become an increasing concern because of the scale of Aml (millions of connected

devices and people), the foreseen mobility needs (which introduces more vulnerability than in a static world), its heterogeneity (in contrast with closed, co-designed systems), its complexity of hardware and software (introducing the dependability challenge) and its distribution of knowledge and resources (co-operation and interconnection).<sup>87</sup> Indeed, the notion of binary network security (access or not) will have to be replaced by more complex security mechanisms whereby differential access is granted to different actors. The security networks will also be challenged by the evolution of the way users will have access to these networks: from an access point linked to a specific location, to a sphere or area of access including under a same domain various environments.<sup>88</sup> As a result, the parameters for this new paradigm are change, dynamism, de-centralization (distributed), flexibility, mobility, heterogeneity, temporality and context-dependency, in contrast with present day security parameters that are relatively stable, well defined and consistent.

In such an intelligent environment, the risk of external attacks could be much greater than they are today with computers connected to the Internet. This is due, for instance, to the proliferation of access networks which increase the number of entry points and also due to the intense interconnection and interdependency of these networks. Moreover, threats will come not only from outside but also from inside the home. Home network security needs to take into account different life styles and household compositions. Smart Home network security will become in the future not only more important but also more complex.<sup>89</sup>

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 and their criticality. Residential network administration will probably be outsourced, and as a result, domestic networks will extend beyond the physical boundaries of the residence. Analyses of the consequence of particular failure mode and its frequency of occurrence will have to be established in order to assess the risks inherent to this new environment and to offer the consumer/citizen the opportunity to refuse it or accept it.

<sup>87</sup> ISTAG, 2002b: 12.

<sup>88</sup> William J. Mitchell, *Me++: The cyborg self and the networked city*, the MIT press, 2003.

<sup>89</sup> Elisson, C. (2002) Home Network Security, Intel Technology Journal, Vol. 6, Issue 4, November 2002, 37-48.

The multiplication of actors involved in the management of the smart home systems tend to be in favour of increasing the frequency of potential failures. But it could be argued that most of these systems will be based on fault-tolerance concept in order to minimize the number of disruptions.

Considering the gravity of these disruptions, 'domestic infrastructures' will become critical since disruptions and attacks on the everyday life of the citizen could be much more serious than they are with current day Internet connected computers. For instance, health applications at home that break down as a result of domestic infrastructure problems could pose medical threats to patients. The higher level of seriousness will represent a stronger challenge for the acceptance of such systems. Domestic infrastructures will become 'nodal points' in the networked society and the management of risks and of the security of this domestic infrastructure will then be seen as critical for the citizen.

Therefore, a crucial and new concern is that home network security will become 'critical' in the future Aml, hence the notion of '**Critical Domestic Infrastructures**' (CDIs). To highlight this, first, it should be noted that today all kinds of infrastructures provided by industry and government already exist that are essential for society to function.<sup>90</sup> The major ones are: communications and information, electric power, oil and gas, banking and financial services, public administration, transportation, emergency services and water supply. Infrastructures

offer services but at the same time, they put assets at risk. 'Criticality' therefore draws our attention to the fact that the possible disruption of an infrastructure could affect the functioning of large portions of society and even of a whole country in a pervasive and serious way.<sup>91</sup> Moreover, the vulnerability of these infrastructures increases as they become more and more interconnected via ICTs.

CDIs could become the backbone for all kind of services managed by information and communication in the home. As is the case with public critical infrastructures, the vulnerability of CDIs is expected to be increased as a result of their interconnection and interdependence and their software based management. It is specifically this that is critical. 'Criticality', as regards domestic infrastructures, should also be seen from the citizen's standpoint in order to safeguard his assets, values and preferences, in contrast with global societal concerns for public infrastructures. Indeed, the influence of personalisation in the definition process of the list of critical assets will be more important in the case of CDI than for country infrastructures.

Illustrated in Figure 1, a special role is foreseen for the gateway operator. This could be the citizen who would be assisted by intelligent agents in order to oversee applications, control the resources, define and control access rights, choose between several provider, etc. Part of these operator functions could also be outsourced to third party service providers.

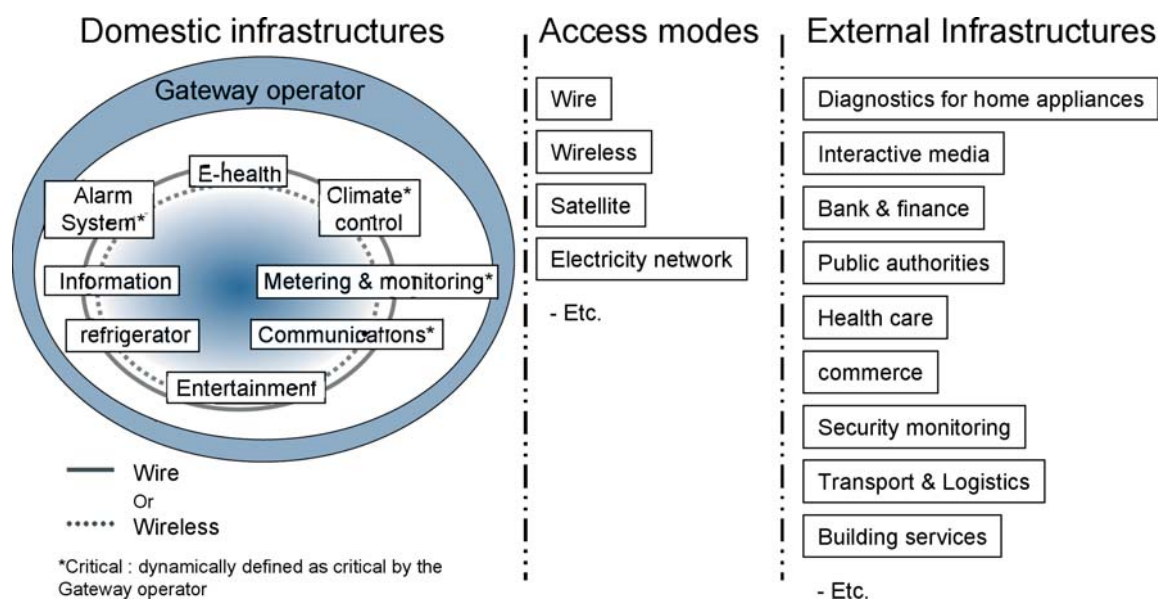
<sup>90</sup> Protecting America's Critical Infrastructures: Presidential Decision Directive 63, W. Clinton, USA, 1998, <http://www.fas.org/irp/offdocs/pdd-63.htm>

Vulnerability and Security in a New Era, The Swedish Commission on Vulnerability and Security, OU 2001:41, Stockholm, 2001 [http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001\\_41eng.pdf](http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41eng.pdf)

<sup>91</sup> The future of Canada's Security and Defence Policy: Critical Infrastructure protection and DND Policy and Strategy, Charters, D. <http://www.ccs21.org/ccspapers/papers/charters-CSDP.htm> Protection of the Canadian Critical Infrastructures, Canadian Security Intelligence Service, July 2001.



Figure 1: The connected home: internal and external infrastructures



The notion of 'gateway operator' is related to a concept that has already existed for many years, i.e. the residential gateway (RG). It was initially conceived by the Residential Gateway Group (RG Group) in 1995 as a centralized physical device, placed between an in-home network and wide area network (WAN). Nowadays different perspectives exist on how RGs should be designed and implemented because of the proliferation of wired, wireless, mobile and satellite networks. An Open Services Gateway Initiative (OSGI) alliance has, for instance, been constructed to define a multi-service RG that is open, platform independent, and allows for the dynamic delivery of managed services to consumers.<sup>92</sup> In the future home, different RGs might be conceived as entry points to the domestic critical infrastructures but there is also the possibility that they could be bypassed by others. However, security is an important issue with all of them as they are points of entrance to the home network. This is especially true for those parts of Aml that are outsourced.

The growing ambient intelligence spaces will also require the development of methods integrating in the same action the assessment of unwanted hazards, vulnerabilities as well as threats and crimes, their durations, and potential conse-

quences and liabilities. By being connected, the citizen and his domestic sphere are exposed to potential threats:

Cyber-intrusions can penetrate through the electronic communication links and cause damage to information assets or to other domestic infrastructures.

A cyber-intruder may also use the domestic infrastructure, for example computer and communication resources, for attacking a third party.

The citizen will have to be reassured and protected against threats and crimes that might cause unacceptable failures. The attitude to risk will need to be based on risk assessment criteria and thus on risk management.

Specific privacy considerations need to be solved according to the domain, permissions, time of the connection, and negotiated by both sides: the service provider and the citizen.

In the same time, it is also important to make provisions for when CDIs fail. The severity of the failure and its duration will depend on the extent to which there are methods for rapid recovery and what alternative methods are in place.

<sup>92</sup> Infocomm (2002a) The connected home. 4th Infocomm Technology Roadmap Report 2002-2007, Infocomm Development Authority of Singapore, November 2002. <http://www.ida.gov.sg>

As with other more traditional infrastructures, service quality for users and security levels should be part of the services offered. These user requirements will be satisfied by solutions deployed by different actors all over the supply chain. The ecology of social, technical and market interaction needs to be addressed in analysing the means for securing CDIs. This implies socio-policy measures beyond the technical ones.

Hazardous infrastructures have been highly regulated, because there is a clear awareness of the perils involved. It is difficult to imagine the establishment of rules for assuring CDIs, but it is possible to think of the request for minimum security measures (e.g. anti-virus, firewalls). The issue of liability remains open.

The implementation of the Virtual Residence concept to the future smart home could complement and facilitate the prospected sensitive management of CDI security. Indeed, analysis of

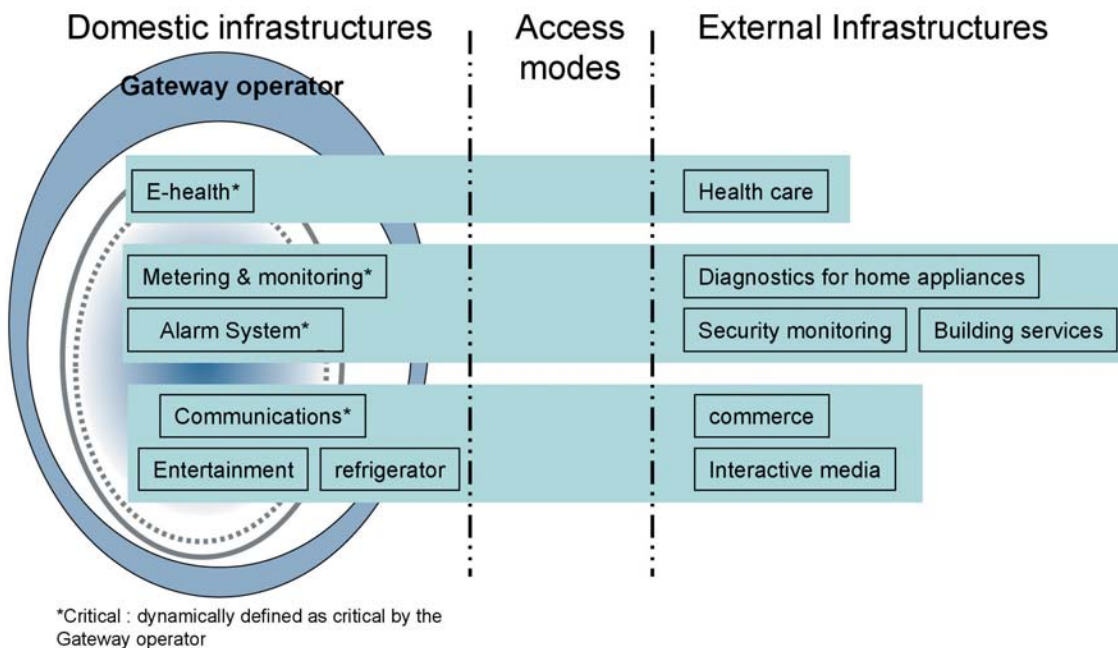
security concerns in Aml space could be based on two main dimensions:

The future home of the citizen: according to the security expert Carl M. Ellison,<sup>93</sup> 'when the home network is connected to the Internet, the domain under consideration is no longer the home'.

The growing mobility of citizens in the European Information Society: personalisation of Aml space which promotes mobility underlines a series of critical security issues where the bridge established between physical parameters, the location of the citizen, and virtual ones like database and user preferences, might constitute the ultimate security threat.

These two dimensions highlight clearly the key issue of new boundaries management and protection in this future integrated environment. Therefore, the concept of virtual residence as regards security aspects would constitute, by definition:

■ Figure 2: The virtual residence applied to internal and external infrastructures



<sup>93</sup> Ellison, C. (2002) Home network Security, Intel Technology Journal, Vol. 6, Issue 4, November 2002, 37-48.

**A passive protection** against potentially intrusive measures conducted by public and private organisations as well as other citizens. The private territory is a legal (and social) sanctuary. Laws and social norms protect the home or domicile as a private space. The fourth amendment to the US constitution has traditionally been considered to protect homes and the area immediately surrounding them from unreasonable government intrusion. Definition of the characteristics of this new virtual and legal sanctuary gives the citizen a clear (legal) basis for suing people who may break into his/her virtual residence. It can also facilitate the establishment of insurance contract linking together heterogeneous environment under a single coverage.

**An active protection** against potential cyber-crimes. By establishing a clearly demarcated private digital territory, the user would be given the opportunity (the rights) to prosecute any violation

of this private sphere on the basis of digital evidence (intrusion detection software, etc.) and to use authorised active preventive measures to protect it (passwords, firewalls, etc.). These tools will contribute to the required opacity of this private digital space. As an extreme example, parallels could be drawn with the right to use firearms in the US in order to protect the residence.

Virtual Residence concept can therefore provide a comprehensive and more coherent platform for the management of the CDI security which will constitute a determinant element for the acceptance of the future Ambient Intelligence spaces. Independently of physical borders among distributed storages and software, Virtual Residence offers a single umbrella under which the CDI's risks are identified, assessed and reduced to a residual accepted level.



## ■ ANNEX II: Study on Digital Territories

### 1. Executive summary

According to ISTAG, Ambient Intelligence is a vision that places human beings at the centre of future development of the knowledge-based society and ICTs. Aml space consists of a set of technologies, infrastructures, applications and services operating seamlessly across physical environments (e.g. neighbourhood, home, car); thus spanning all the different spheres of everyday life. Physical space becomes augmented with digital content, thus transcending the limits of nature and of direct human perception. A new term is needed for this new kind of space, which captures its dual nature. The term “digital territory” (DT) has been coined in an attempt to port a real world metaphor into the forthcoming synthetic world.

In order to validate the vision of DT and its associated concepts and assess their impact to society and technology, a study has been carried out under the supervision and funding of JRC/IPTS. The results of this study are collected and presented in this report.

The aim of this study was to analyse the concepts, technologies, legal and human factors that underlie Digital Territories. More specifically, the objectives of the study were to:

- elaborate the concept of Digital Territory (DT),
- detail the source of problems addressed within this concept, related to the balance between security and privacy in the everyday life of the citizen and the definition of meaningful digital public/private territory boundaries,
- analyse the underlying technological, economic, social and legal challenges,
- validate the concept and its foreseen ramifications and
- raise awareness as to what research and policy option avenues exist.

The study was carried out by a Core Expert Group (CEG) with the assistance of outside experts. The CEG employed different tools for ad-

ressing, depicting and validating the issues and concepts of the study. These included tools to generate input (study of literature, two phase focused survey with the use of questionnaires, interviews), tools to discuss and produce output (web-based forum, tele-conferencing sessions, group discussions, brainstorming) and tools to engineer concepts (scenario-based analysis). Outside experts participated in a questionnaire-based survey and also discussed their views during interviews. The results of these have been summarised in the background report, which was validated during a validation workshop held in Athens in June 2005, with the participation of IPTS, CEG and outside experts.

The main issues that were elaborated within this study are the following:

- The concept and vision of DT, its relevance and need according to different aspects (legal, social, economic, technical) and different social levels (individual, family/group, public) and settings (domestic, urban, mobile, ubiquitous, shared, etc).
- Key and emerging technologies, challenges and problems for realising the concept of DT in the future Information Society, as well as related policies on infrastructure, applications and services for DT.
- The specification of meaningful DT boundaries and the notion of distance in future society, as well as methods and tools for people to manage distance and proximity in Aml spaces in ethical, legal and social terms.
- The Digital Bubble as both a concept and a tool for managing contextual data (i.e. representation, selection, filtering) and interactions and information flows. Particular illustrations will be presented, in terms of examples and situation analysis.
- The private and public virtual spaces, their forms and perceptions in future Aml environments, the balance between security and privacy in everyday life and the related potential roles of public and private bodies in the implementation of DT.



- The bridging between the physical and digital worlds with the use of DT and Aml technologies.
- The investigation of issues, related to privacy, security and trust that can delineate suitable legal and social frameworks for Aml environments and the successful implementation of DT in the future society.
- Security, privacy and identity concerns, tackled for the various DT categories and peoples' online activities in terms of their protection and law reinforcement.
- Suitable DT measures to deal with known or emerging risks related to the security and privacy in the everyday life of 'mobile' citizens.

The study adopts the main concepts that underlie the Ambient Intelligence vision and its ramifications as they have been described mainly by ISTAG, but also in the various IST reports and project deliverables. We have also examined the results of several R&D projects, ongoing or finished, in both sides of the Atlantic. These are summarized in various literature sources (see references at the end of section). Of these, we have considered the following as more relevant:

- The FP5/FP6 IST/FET Disappearing Computer I and II initiatives ([www.disappearing-computer.net](http://www.disappearing-computer.net)). The mission of the initiative was to see how information technology can be diffused into everyday objects and settings, and to see how this can lead to new ways of supporting and enhancing people's lives that go above and beyond what is possible with the computer today. Specifically, the initiative focused on three-interlinked objectives:
  - Create information artefacts based on new software and hardware architectures that are integrated into everyday objects.
  - Look at how collections of artefacts can act together, so as to produce new behaviour and new functionality.
  - Investigate the new approaches for designing for collections of artefacts in everyday settings, and how to ensure that people's experience in these new environments is coherent and engaging.
- Project e-Gadgets ([www.extrovert-gadgets.net](http://www.extrovert-gadgets.net)), which was part of DC I initiative and described

GAS (Gadgetware Architectural Style), a set of user requirements, specifications, rules and guidelines for the development of Aml artefacts, a set of prototype artefacts, a software platform that enabled composition of services offered by the artefacts, demo applications using the artefacts and a suite of end-user tools that could be used to compose and manage these applications. This project proved that the vision of Aml is realizable on top of wireless network infrastructure using conventional development tools. It also contributed to discovering the technological and human factors that affect the adoption of Aml applications. In this study, we have used the body of knowledge generated during e-Gadgets as a starting point in our attempt at exploring the Aml landscape. We have also used some of the scenarios developed during the project as test-beds for the DT scenarios

- Project SWAMI (<http://swami.jrc.es/pages/index.htm>), which aims to identify and analyze social, legal, organizational and ethical implications related to issues such as privacy, anonymity, manipulation and control, and identity in the context of Aml. The SWAMI project consortium has reviewed existing Aml projects, studies, scenarios and roadmaps, and they have produced four "dark" scenarios on Aml that highlight and detail the key socio-economic, legal, technological and ethical risks related to identity, privacy and security. As a result, they define and study various research and policy options, which could serve as safeguards and privacy-enhancing mechanisms that address the risks and vulnerabilities associated with the introduction of Aml. This study adapts the findings of SWAMI to DT and related concepts, and complements it by focusing on the "bright" side of Aml
- The Convivio human network ([www.convivionet.net](http://www.convivionet.net)), which promoted the design of human centered interactive applications. Convivio members are concerned with how we could design Aml applications that would truly serve the interests and activities of people, without disturbing their lives, thus improving their well-being and quality of life. Convivio members are prominent human factors, HCI, design or software engineering re-

searchers who constitute a balanced mix of academia and industry. The network organizes workshops, produces studies and publishes regularly a web-zine. We have used Convivio as a source of human related issues and as a dissemination medium

- The notion of Virtual Residence (VR) has been proposed as a means of tackling new concerns about identity, privacy and security within an Aml space that encompasses both physical, online and virtual lives, and the embedding of computing in everyday devices. It consists 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, and households and their virtual representation and mobility and interoperability between different Aml environments. VR has served as a starting point for DT (in fact, DT is a generalization of VR), while it still is the most easily comprehensible example of a DT. VR has been evaluated in a previous workshop organized by IPTS; this study partly utilizes the results of this workshop

Territories, that is, areas under a clearly established jurisdiction (their contour necessarily delineated by a boundary) initially referred only to land. A territory is usually a continuum in space; the real and digital elements of DT however, may co-exist in disparate locations: the substitute for continuity in DT is proximity. A territory has a measurable quantity of elements which are contained within its borders. However, the elements of a DT are active, as opposed to the usually passive objects found in real world territories. In Aml space, even traditionally passive objects may become active elements when enhanced with sensors, processing and communication abilities. Transient elements, like activities or procedures, can now become elements of DT. Another interesting property of digital objects is “persistence”. Digital objects tend to leave traces in every territory they have been to: data not properly erased, state information, registry entries, timestamps on servers etc. With the proliferation of ICT, the notion of territory can be expanded to cover other domains, and with it the definition of a boundary has to change. Boundaries can be natural, social, spatial and temporal, and ephemeral or transitory. Whether the environ-

ment is real or digital, one needs to deal with territories by studying their boundaries. While boundaries are often recognised both socially and legally in the physical world, the digital environment clearly lacks such a definition of borders. As a result, any abuse or violation of these borders would not even be noticed.

The above constitute the basic assumptions that underlie this study. In order to elaborate on these and because of the novelty of its subject (i.e. the notion of DT) we decided to adopt a breadth-first search strategy. Our aims were first to clarify (to ourselves and to the outside experts) the notions of DT and agree on a basic “ontology of terms” before we proceed with analysis. Thus, the study does not analyse in particular any aspect or notion that relates to DT; instead, it records these, searches for the historical sources of each and attempts to project them on the Aml environments of the near future.

In the light of these, the study has met its aims and objectives successfully, as it provides answers to all the above and can serve as a starting point for future, more focused studies. In the Introduction, we describe briefly the findings per particular objective. Here, we summarize some of the key findings:

- Towards the realisation of DT, key technologies need to progress and technological challenges and bottlenecks need to be addressed.
- The bubble metaphor captures most of DT properties in an intuitive way.
- In DT, proximity is the substitute for territorial continuity. However, a case-based new definition of proximity is required.
- DT should always have a recognized owner and a purpose. Identity is the core property of DTs and is marked or discerned much in the same way as this happens in physical territories. It generally reflects the identity of the owners or inhabitants. The owner of a DT can be a single person, a group, or an agent. The responsibility share should be defined by a set of “laws” on which there is consent from all parties.
- While boundaries are often recognised both socially and legally in the physical world, the digital environment clearly lacks such a definition of borders. As a result, any abuse or vi-

olation of these borders would not even be noticed.

- Digital objects tend to leave traces in every territory they have been to: data not properly erased, state information, registry entries, timestamps on servers etc. Thus, in Aml applications an important consideration should be the consideration of security right from the beginning of the design and during the entire life cycle of the engineering process.
- DTs and their components including the whole infrastructure they rely on are exhibited to security, privacy, identity and copyright related threats. These threats range from unauthorized information manipulation and disclosure (violations of personal or corporate confidentiality), to forgery, denial of service, profiling, and piracy or cloning. In order to address this issue, suitable measures have to be taken which include organizational, procedural and technical measures, such as entity and data authentication, data and traffic data confidentiality, authorization and access control, digital signatures, privacy and copyright protection.
- Study of the legal framework with concern to DTs and bubbles shall necessarily follow the clarification of all open definitional issues. The problem with Aml is that notions that are apparent and self-evident in the real world need to be re-defined, indeed in a way that shall bring general consensus. A regulatory framework is needed. Consequently research should concentrate on two topics: first, definition of the fundamental notions in the digital environment, and, then, elaboration on certain legal issues pertaining to them.

The members of the Core Experts Group have synthesized this final report based on their own background, their view of DT and related concepts, the available literature, the background report and the results of the validation workshop. It is the will of the CEG to pursue research in DT and raise awareness in the concept by organising workshops, publishing papers and submitting the results of the study to consultation meetings.

## 2. Introduction

*This is a report prepared as a result of the Call for Tender J02/38/04 "Study on Digital Territories" and the contract No 22603-2004-12 F1ED SEV GR awarded to ATLANTIS Research Organisation by the Institute of Prospective Technological Studies (IPTS) of the DG Joint Research centre of European Commission.*

This work presents an analysis of the Ambient Intelligence as a vision that places human beings at the centre of future development of the knowledge-based society and ICTs. As Aml space consists of a set of technologies, infrastructures, applications and services operating seamlessly across physical environments (e.g. neighbourhood, home, car, etc.) it spans through all the different spheres of everyday life. Physical space becomes augmented with digital content, thus transcending the limits of nature and of direct human perception. A new term is needed for this new kind of space, which captures its dual nature.

The term "**digital territory**" (DT) has been coined in an attempt to port a real world metaphor into the forthcoming synthetic world. This new term carries certain assumptions and gives rise to sub-concepts; it requires a certain level of technology and will be realised at a pace affected by specific factors; once adopted, it shall cause an imbalance to existing personal and social structures.

Living in Aml space requires a proper balance between a complex diversity of interests and values related to freedom of speech, access to information, protection of the individual sphere, trust, security, protection against discrimination, protection of identity, and protection against intrusions by public and private actors.

In such an environment which is extremely personalised, the protection of personal data, which is networked and therefore remotely accessible, is very important. The natural way to achieve this is by establishing boundaries – digital boundaries, which people tend to accept intuitively.

A **digital territory** is an ephemeral Aml space: it is created for a specific purpose and integrates the will of the owner (an individual or group operator) with the means to achieve it (including infrastructure, properties, services and objects) within

an Aml space. A DT can be composed of sub-spaces, which are determined with respect to their services, usage, etc. A territory is usually a continuum in space; the real and digital elements of DT however, may co-exist in disparate locations (in the end, any digital element is recorded on a hard-disk or other medium which has a specific physical substance and location – although the latter may change with time, i.e. if the device is mobile). The substitute for continuity in DT is proximity; however, a case-based new definition of proximity is required.

A territory has a measurable quantity of elements which are contained within its borders. **Borders** are no more defined as “lines” to traverse or not. Borders are conceived as spaces “in-between”, *spaces of negotiation*. **Markers** are a way of defining / denoting the boundaries, the borders and the points of negotiation and crossing.

The elements of a DT are active, as opposed to the usually passive objects found in real world territories. Transient elements, like activities or procedures, can now become elements of DT. Another interesting property of digital objects is “persistence”. Digital objects tend to leave traces in every territory they have been to: data not properly erased, state information, registry entries, timestamps on servers etc.

**Privacy**, usually synonymous to personal space, is translated into physical distance from others. There is private territory; for example related to one’s physical body – personal and total control exercised. However, there is also public territory which is characterised by free access and a duration quality; related to one’s use of public amenities.

**Ownership** depends entirely on the purpose the DT serves. The owner claims territoriality in order to regulate the DT environment. **Identity** is a property that emerges for the DT owner based on the purpose that DT serves, on the data it stores and on the activities it supports; identity emerges from will. The owner of a DT can be a single person, a group, or an agent.

A (digital) **bubble** is a temporarily defined Aml space that can be used to limit the information coming in or leaving it. A bubble is a metaphor for visualizing DT. As a direct consequence to its relationship with DT, the bubble concept clusters to-

gether all the interfaces, formats, rights and agreements etc. needed for the management of personal, group and public data and informational interactions. Such contextual activity can be based on privacy, personalisation, priority, location, membership, ambience, social circumstances, and time. Hence, the bubble concept (being the visualisation of a DT) can be used to make filtering and selection of data possible.

**Bridges** between physical and digital are actually elements/components of Aml spaces linking the physical and the digital. Sensors, actuators and RFIDs are examples of bridges between the physical and the digital. Building a bridge is a process. It shows intention, expected functionality, changes the nearby area of the two banks it links and probably, in the future, invites for changes or evolution of its structure according to new needs. Building a bridge is also a design decision.

As a consequence, **mobility/adaptation/change** can both be recognized (sensed) and realized. Mobility can be sensed in relation to nearby points of reference but can also be achieved as a DT moves in space. Adaptation, as goal-directed change, can be sensed by nearby DTs who sense another DT’s desire for change, but can also be realized by an internal change of states (generated, in turn, by some external event) in a DT. Finally, change can be sensed as a state transition of a DT (e.g. movement in space or internal state transition), but can also be induced on nearby DTs by another DT (e.g. by generating a certain set of rules).

One illustrative example of DTs is the home, which is conceived as a private place and created to protect the family. Historians locate the appearance of the “house” as we know it today, with its divisions to common areas and to bedrooms between the 17<sup>th</sup> and the 18<sup>th</sup> century. At the same time, working was disconnected from the house and being at home was conceived as a retreat from the world. Not surprisingly, the most familiar example of a bubble is residence, which is also protected under EU law. Home is a protected sphere delimited by the walls of house; but the notion of privacy follows the home owner outside the house (i.e. car). Accordingly, the bubble of protection follows a person’s movements as long as these are related to the Virtual Residence (the home in the digital era).

Bringing the public into the isolated territory of the house was the result of the “media” tech-



nologies, starting with the radio. In its future evolution, the “Home” DT is complex (regarding its structure), is owned by an individual, group, or family (regarding its ownership), can support different degrees of privacy (regarding membership), its use is role based, it can be fixed or transforming, temporary or enduring, based on ownership (regarding its occupation in space and time) and can also become interactive.

Security and privacy concerns are associated with all categories of DTs, such as location based systems and services, virtual residencies and mobile phone networks. Elements of DTs and their components, including the whole infrastructure they rely on, can be identified in security, privacy, identity and copyright related threats. These threats range from unauthorized information manipulation and disclosure (violations of personal or corporate confidentiality), to forgery, denial of service, profiling, and piracy or cloning. To address these issues, suitable measures have to be taken which include organizational, procedural and technical measures, such as entity and data authentication, data and traffic data confidentiality, authorization and access control, digital signatures, privacy and copyright protection. In a digital environment, boundaries need to be well-defined and easily perceivable by all individuals active in the digital context. In order for them to operate properly, boundaries in the digital environment must become as clear as boundaries in the real world.

Study of the legal framework with concern to DTs and bubbles shall necessarily follow the clarification of all open definitional issues; once it becomes clear what is meant by DTs and “bubbles” and what their relationship to an individual exactly is, only then may legal research apply its methodology in the digital context. The problem with Aml is that notions that are apparent and self-evident in the real world need to be re-defined, indeed in a way that shall bring general consensus. A new “social-contract” is needed, that will make visible or generally perceivable any interaction in which a bridge is involved. A *regulatory framework* is needed. The multiplication of bridges and their growing pervasiveness imposes to adopt a more global approach driven by regulatory framework and proper standards.

Consequently research should concentrate on two topics: first, definition of the fundamental no-

tions in the digital environment, and, then, elaboration on certain legal issues pertaining to them. While doing this, however, we must use the principles that underlie our contemporary legal system; principles that have been formed over human history and that will not easily be abandoned in view of a new reality (the digital environment), unless there is a very good reason for it (and until today none has appeared). Therefore, what should indeed be done today is to find the “parallels” between the real world and the digital environment and to try and accommodate legal notions from the former to the latter, in order to secure a possibly trouble less transition.

This report is developed in order to elaborate the concept of Digital Territory and the elements of which is composed. As far as the structure is concerned, it aims at serving the purpose of ‘slowly’ introducing the reader in the context of DT and then present various aspects that have to do with key and emerging technologies, definition of various concepts and issues related to DT and Aml. The report is based on the results and findings of the study (through the overall bibliographical review, the questionnaire survey and the workshop). There is an overall introduction to the study concept, the tools and methods utilised for the implementation and then a detailed introduction of the concept of Digital Territory. Key and emerging technologies as well as new *concepts* such as bubbles, private and public spaces, bridges between the real and digital world are presented. Then a list of issues covering legal and social framework, security and privacy concerns and mobility of citizens are examined in the framework of the DTs. Finally there is a list of suggestions for raising awareness on the study results and developing synergies with other projects and studies, as well as a list of conclusions that came up throughout the study.

### 3. Tools and approach for the study

The Core Team for this study consists of a high level expert group, comprised of experts of international reputation in the fields of expertise required by the present study. These high-level advisors had the overall scientific responsibility, ensuring high quality of the study deliverables. The members of the core team have complementary



backgrounds and fields of expertise and more importantly, an already established excellent collaboration and joint previous experience in the field of Aml where they have worked together.

Another important factor that enhanced the study processes and progress (in terms of time and financial resources), is that the majority of the members of the core team work in the same country (Greece), thus, meetings and face-to-face interaction was held without additional cost (i.e. travelling) for the study.

Beyond the continuous interactions and collaboration between the experts responsible for carrying out the study, a wider pool of researchers and field experts was formed in order to provide insights and input under specific requests by the study team. Already established networks and communities in the fields of Ambient Intelligence and ICT to which the study participants are affiliated played a significant role and contributed valuable information and views, promoting the study's quality.

This group was selected from networks and associations, in which the team of experts participates. Two such networks are the DCnet and Convivio – access to the members of these networks was facilitated because two members of the team of experts serve in their Steering Groups. DCnet involves researchers who participated in the projects of the Disappearing Computer IST/FET proactive initiative ([www.disappearing-computer.net](http://www.disappearing-computer.net)). FET DC projects yielded results that greatly advanced progress towards realization and acceptance of Aml environments that consist of everyday objects enhanced with ICT modules. The Convivio network ([www.convivionet.net](http://www.convivionet.net)) promotes the design of human-centered interactive applications and hosts a multi-disciplinary community of researchers and practitioners that pays careful attention to the nuances of everyday life: technology is not seen as separate from the lived reality – and quality – of people's lives, but as deeply related.

The team of experts employed different tools for addressing, depicting and validating the issues and concepts of the study. These included tools to generate input (studies, survey, workshop), tools to discuss and produce output (tele-conferencing sessions, group discussions) and tools to engineer concepts (scenario). More specifically:

- Studies of available literature, including scientific publications, popular science articles, social studies, documents and reports, from business plans and roadmaps through EC directives and regulation proposals.
- Focused surveys, with use of questionnaires and interviews, to groups and individuals from different domains (i.e. technology, public authorities, commercial, research/academic, design, law, sociology, etc). The team performed a two-cycle survey, each cycle containing about 20 questions, which was disseminated to more than 100 people; although we expected to receive at least 30 contributions, the response rate was much smaller (less than 15).
- A proposal was made by the core team for the organisation of a workshop funded by the Convivio network on the subject of „Digital Territories“. The workshop was approved and provided the team with the opportunity to discuss before an audience the main issues that underlie the concepts of DT and VR, to present and debate opinions and to approach the subjects from different perspectives, which eventually led into an open discussion. The output of the workshop was an additional input produced by the literature studies and the questionnaires.
- Meetings between the core team were held almost on a monthly basis in order to discuss emerging issues or brainstorm. Furthermore there were online discussions using teleconferencing facilities (the IBM Centra software will be used). In between these sessions, e-mail and telephone were used to exchange ideas and comments on draft versions and intermediate findings of the study.
- A simple web-site, mainly serving as an electronic repository for the core study team (i.e. with protected pages) and within it an electronic discussion forum was set up, where the team of experts and other interested parties “met” for discussing issues that relate to DT and VR concepts. The forum provided the opportunity to conduct focussed discussions, while keeping track of the exchange of opinions.
- The core team developed various scenarios involving the application of DT and VR concepts in a future everyday Aml environment.

The scenarios were produced during two brainstorming sessions conducted during the second month of the study and were used as tools to engineer different concepts, aspects, issues, etc of the DT and VR concepts

In the following section, it is presented the methodology that was followed during the study for investigating each one of the issues addressed in the call.

## 4. Study methodology and work plan followed

The study was carried out within **four major strands** of activities, each aiming in producing the aspired results and required deliverables.

### Strand 1: initialization and planning

The first strand was about the study initialization, planning and support activities and took place the first 11 Weeks of the study. The primal aim was to establish a common understanding of the study's objectives by all actors involved.

The kick-off meeting for the study was organised on the 2<sup>nd</sup> of February 2005 in Brussels. The following people participated from IPTS: Ioannis Maghiros, Yves Punie and Laurent Beslay, while from the contractor's side two people participated: Effie Amanatidou and Achilles Kameas. In this meeting there was a discussion concerning objectives and scope of the study, the approach and methodology to be implemented, the timetable and deliverables, the validation workshop, the overall study content and the project management. The issues undertaken in the framework of the study were further analysed according to different aspects (technical, legal, social, economic) and levels (individual, group, public).

As a result of the discussions the timetable and the list of deliverables were revised and the core team met shortly after in order to 'kick off' the actual work for the study. That meeting took place in Patras.

The following activities were decided and delivered accordingly:

### Setting up the study's groups

A pool of more than 100 individuals selected from different domains were defined as a basis for the designed surveys. The plan was to divide 5 domain groups (with collectively around 30 people) following the first survey cycle, according to contributors' active interests and field of expertise.

### Tools design

**Questionnaires**, an **electronic discussion forum** and **a set of scenarios** to be used as tools to investigate and engineer different concepts, aspects and issues on DT were produced by Month 3 of the study.

In drafting the questionnaires for the Focused Surveys, ATLANTIS' experience due to the participation in studies such as the current 5 Year Assessment questionnaire survey of the 5th Framework Programme, as well as in the 5 Year Assessment questionnaire surveys of the 3rd and 4th Framework Programmes (1994-1999) was proven valuable.

A specific proposal for the questionnaire was prepared by the contractors after thorough study and assessment of past and currently used questionnaires for similar types of studies taking into account the experiences gained as well as the specificities of this survey and the final design format was decided in close collaboration with IPTS.

Combined with the above, considerations of aesthetics, epistemology, practicality and cost – effectiveness, were also taken into consideration in order to guide the designing of the questionnaire, the target being for it to be short, simple, and capable of producing statements of use to programme administrators and policy makers.

### Strand 2: carrying out the study

#### Literature studies

Studies of available literature, covering from scientific publications to business plans, roadmaps and EC directives, were carried out by the core team throughout the study.

#### Focused surveys and interviews

There was a two-cycle survey with the use of questionnaires and interviews:

- The first cycle commenced early during the study and addressed more than 100 selected people from different domains. The questionnaire was carefully designed and included about 20 questions. A couple of the questions had to do with (indirectly or directly) presumable contribution to the validation. Aspects of the devised scenarios were also incorporated in questionnaire bits.
- Although we expected to receive at least 30 contributions, we only received 13 responses in the first cycle. The initial plan was to “position” the contributors in 5 domain groups, but due to the limited response rate we decided not to proceed with this method. Following the first analysis of results, the first cycle of interviews was then organised, with selected individuals.
- Accommodating the interviews and first cycle survey outcomes, the second questionnaire for the 2nd survey cycle was designed. As there was no division of the experts, there was no need to follow the initial methodology of designing a set of 5 questionnaires, each addressed uniquely to a domain group.
- Using a revised questionnaire (unique) the 2nd survey cycle started. Along with the analysis of incoming contributions, interviews were organised and conducted.

### Analysis and integration of survey outcomes

After the completion of both cycles of the Focus Surveys, there was an analysis of the incoming contributions and results mainly focusing on qualitative aspects of the responses in order to identify stakeholders from many different domains (members of scientific, social or industrial networks, societies and associations and user groups).

The outcomes of the analysis along with the recommendations of the survey participants were synthesised and presented in a report which was integral part of the background report for the workshop. Analysis results were also a valuable input for the interim and final reports.

### Producing the background report

A **background report** covering all topics addressed in the call was developed, serving as the background document for the workshop. This was

produced in two versions: The first (draft) version was delivered for reviewing and commenting to IPTS before the workshop; comments were received and integrated in the final background report that was distributed to the workshop participants two weeks before the workshop date.

### Raising awareness

Raising awareness on the concept of DT was one of the major objectives of this study. To this account, interaction with individuals, communities, networks, and domain experts was established via the study's tools (i.e. interviews, forum, etc). The validation workshop was also organised with a view to raise awareness being its -parallel to validation- fundamental goal. Discussion in mailing lists and other web forums by the core team experts was also a means to serve this purpose. Moreover, a workshop on DT was proposed and organised with funding from the CONVIVIO Network (not by the study/IPTS).

The core experts' team considers raising awareness as an activity which they intent to keep ongoing even after the completion of the study. More specifically: Follow-up will be pursued by organizing special workshops and sessions in conferences and events. Promotion and raising awareness on DT and study outcomes will also be done via the CONVIVIO web-zine (<http://convivio.idii.it/>), where one of the core team members, Dr. Achilles Kameas, serves as Editor-in-chief.

## Strand 3: validation

### Organizing the validation workshop

Planning of the validation workshop started essentially from the very beginning of the study in order to ensure that all organisational aspects would be taken into consideration.

As stated in the tender specifications, the validation workshop was organised on project month 5 and had 2 days duration in order to ensure that there was enough time to cover all issues that will arise.

Although most of the experts invited in the workshop were from Central and Northern European countries, we decided to organise the workshop in Athens due to the fact that the team

members proposed for the elaboration of the study are located in Greece; we thought that it might be more appropriate to have the experts travelling to Athens than having a group of 10 people from Greece travelling to a more central location such as Brussels. Furthermore, Athens is easily accessible from all European cities.

In addition, the adequate participation of the experts proposed was ensured due to the already existing good working relations with the members of the team and the given personal and scientific interest in the issues examined by the study.

The venue for the workshop was selected based on the parameters listed below:

- High quality and aesthetics of the venue
- High quality of the facilities provided
- Cost effectiveness in terms of offered services
- High quality of the technical and support staff that will be provided for the duration of the workshop
- Easy access

### Analysis of results and Interim report

Workshop workings during brainstorming and interaction sessions were analysed further by the core study team. Emerging outcomes were cross-validated after the completion of the workshop through interviews. An interim report including the minutes of the workshop was delivered to IPTS for comments.

## Strand 4: integration and final results

### Integration of work and final report

The latest strand regards the integration of all study findings and results in the present **final report**. This report consists of the following: (a) synthesis of the results in combination with the comments and suggestions provided of the Draft background report as well as the Interim report and workshop minutes (b) an executive summary; (c) a proposal on how to further raise awareness on the results of the study; and (d) conclusions (including research and policy) for the whole study.

## 5. Detailed introduction of the concept of digital territories

### Digital territories

A DT is an ephemeral Aml space: it is created for a specific purpose and integrates the will of the owner (an individual or group operator) with the means to achieve it (including infrastructure, properties, services and objects) within an Aml space. A DT can be composed of sub-spaces, which are determined with respect to their services, usage, etc. For example, a DT could be distinguished in compartments, as in real life: private compartments (no interaction) and public compartments (where interaction with other DTs is possible). DTs form larger communities that can be thought of as DTs themselves since they have the defining characteristics given above. Thus, a DT may contain other DTs or be at the same level (i.e. independent). There's also a need to define "mechanisms" to connect existing sub-DTs, e.g. like city districts having detached family housing areas, which have roads connecting separate family houses and their driveways to each other. Other interesting factors would be the critical mass and drift attributes, which concern sizes of groups and how uniform they grow or break apart into new individual DTs because of growth or hierarchical changes. However, as it is difficult to suggest that any DT is only of a digital nature, it would be actually problematic to try to separate digital and physical instantiations.

One illustrative example of DTs is the home, which is conceived as a private place and created to protect the family. Services have to do with practical issues (like food and cleanliness) and with relationships to the world (for example entertaining and entertainment). Size really depends on the identity of the individual and their current situation.

A DT is defined not by physical space or borders alone but by the following non-physical characteristics as well: (i) information processing and/or information exchange with the external to the DT world, (ii) reaction to events taking place externally to the DT, (iii) its owner/governor, who uniquely characterizes this DT. However, since information is not a physical entity that can be enclosed within a clearly defined physical space (e.g.



disk surface) but it can move and change forms and shapes (carrying the same information content semantically and entropically) it can be thought of as a ubiquitous entity possible shared by many DTs. Thus, an important characteristic of DTs is the ability to share, transform and route information (both about themselves and about other DTs).

The relationship between DT life span and identity persistence is based on three main elements: 1. Unity: all the different sub parts of the DT always represent the same entity, 2. Permanence: independently of the dynamic property of DT and the evolution of its shape, the identity of the entity remains the same over time, 3. Uniqueness: as the digital world tends to offer the possibility to provide multiple identities to the same subject, a DT could also belong to several subjects and therefore contribute to the building process of several identities.

Since a DT is an ephemeral entity, an issue arises as to how the DT dissolves and what happens to its constituent entities and acquired resources after it has dissolved. Since the primary reason of existence of a DT is information storage and processing (with possible interaction with other DTs and the physical environment), dissolution of a DT is akin to having the information processing come to an end. Equivalently, since information cannot simply disappear (information erasure costs as entropy increases for each erased bit), the results of the processing or the state of the DT when it stopped processing information can be stored by other DTs for further processing of history keeping. Resources borrowed from other DTs or the environment are marked as free (by the owner DT just before it dissolves) so as to be utilized subsequently by other existing or newly formed DTs. Concrete DT behavior rules should clearly indicate when the resources can be allocated to other DTs and according to which criteria.

## Ownership and identity

Ownership depends entirely on the purpose the DT serves. The owner claims territoriality in order to regulate the DT environment. Identity is a property that emerges for the DT owner based on the purpose that DT serves, on the data it stores and on the activities it supports; identity emerges from will.

Identity is the core property of DTs. It is the aggregated, or rather directed data pertaining to the task-at-hand, while ownership could refer to all such data, as well as the transactions that these are involved in. There could never be a DT without identity, if one defines identity as an entity with an aim.

Identity can also be understood as an ever-mutating entity. In this sense identity is itself also indivisible and has multiple variations. Utilising the concept of “bridging” it is possible for DT to become increasingly “large” and still retain its defining characteristics. Should it lose those, it will transform to another DT, but one that will be somewhat defined by its originating entity.

DT should always have a recognized owner and a purpose. Ownership for a DT has to be claimed by an individual even though the use of a DT can be shared with a defined group of people. One of the possibilities behind an individual in digital domain can be a common alias used by a group of people. The ways to check the identity have to be developed.

Identity of a DT is marked or discerned much in the same way as this happens in physical territories. It generally reflects the identity of the owners or inhabitants. The concept of ownership of a DT is mainly defined as the uncontested right/authorization to regulate the function and formulate the identity of the DT. It can also vary in terms of clarity of definition. It may be temporary, collective, it may also be subject of disputes and “wars” as it happens to any territory. Ownership, above all, is *practiced*.

The owner of a DT can be a single person, a group, or an agent. The responsibility share should be defined by a set of “laws” on which there is consent from all parties. In the case of the agent, responsibilities and decision power are partly transferred to the agent from the single person, a delegation of rights.

A single person owns his/her own DT, but when certain civil rights are withdrawn or mental capabilities are lost (e.g. dementia) some personal DTs might be managed by a trusted other. Agents cannot be owners, but the owner person or group can delegate responsibilities to agents. Groups can have consensus or majority (in several levels), just like the groups decide on.



If a company is the owner, then it must be a legal entity; that entity is the owner and thus responsible. If there is no legal entity the user takes a risk.

Some DTs might be shared by a family, or by a group of co-workers. Responsibility is shared just as with physical territory. The existence or lack of audit trails might make this more or less possible to enforce.

## Functions

A DT is a place wherein information processing and storage happens. In essence, it is an information processing entity: it receives input, applies internal processes and produces output; it perceives and affects its environment; it enables communication and migration of data and processing within its borders.

It is an *entry point* to personal information, manifested by some physical token or physical area (e.g., a meeting room, or a person's living room). The physical parameters of a DTs manifestation help the owner/user to visualize the *virtual* properties of the corresponding digital space.

Being an information processing entity, a DT has an internal state. DT changes over time; it moves between states based on internal or external events. Its global state is based on the multiple local states, but at one instance in time there is one state (out of many possible). One global state is possible but unlikely given the constant flux of the networked society. DTs are like media, they do not stand still; they are always in flux. Change is the constant. Thus, the only global state that can be ascribed to a DT is that of change, its ability to adapt, transform and communicate.

Which is the way to create DT? Launch and learn – rapid prototyping: we can't afford anymore to follow "waterfall-like" development cycles. So we launch and adapt after learning. Centralized data management of a DT will be difficult if the DT gets large. It's better to distribute control when needed.

The DT life span can be eternal and then DT is expected to evolve. But the membership is of a shorter time-span, related to the user. Identity is persistent while DT is transient. Generally, the life span of a DT goes along the life-span of its

owner(s). A DT that no-one owns is a "no man's land", it may only bear the traces of previous life but this considered "dead" until a new ownership appropriates those traces for its own purposes.

When a DT is dissolved, its owner(s) own(s) the resulting components. The Aml environment gets informed and enlarged by its transactions with DTs, but it is the DTs that "own" their core data. Still, there exists a space between the two that must be acknowledged and whose artefacts are part of "public domain". As members might be able to store their copy of the DT data, it might end up deteriorating into multiple "bite size" ownerships. Before its dissolution, the owner of the DT might have the possibility to transfer some rights he has acquired to someone else or to another DT. DT owners, can give, sell or destroy components or ignore them, which might cause them to decay if they are not picked up by others. If the DT is "abandoned" (not dissolved) then anyone may claim it and its elements.

## Classification of DTs

Attempting a classification of DTs, we should first define suitable elements which can characterize different DT categories. Such core elements should directly relate to DT definition and functions. Among characteristics, properties, factors of a DT, the following are suggested to serve as the main DT classification parameters:

- Structure
- Ownership
- Membership
- Use, services
- Presence in space and time
- Interactivity (external and internal) and information processing

### DT classification based on structure

There are two views regarding the internal structure of a DT: the first is that there is no internal structure, and the DT is merely a representation of its owner's purpose. The other is that a DT is composed of sub-spaces, related to specific usage and services.

Considering that a DT *does* have an internal structure, classification can be based on a) the complexity of this structure and b) the level of hierarchy for DTs contained in or containing other DTs. Therefore, a classification based on structure can be:

- According to complexity, inclusiveness:
  - Complex DT: contains at least one different DT
  - Unary DT: self-contained, contains no other DT(s)
- Based on relationship/association with other DTs
  - Same level DTs: two or more DTs being are at the same level of hierarchy when contained in a 'larger' DT
  - Contained DT: a DT that consists a sub-space of another DT
  - Generated, evolved: A DT generated or evolved by another

### DT classification based on ownership

According to the number of owners, an approach for classifying DTs could be the following:

- 1 owner: the DT is directly associated with a person or entity
  - Individual
  - Personal
- More than 1 owners: jointly owned
  - Group
  - Common
  - Family
- 0 owners (DT stopped/abandoned or completed serving a purpose)
  - Abandoned or dissolved

### DT classification based on membership

Based on members, their inter-relationship and control they have over processes and data

- Individual (absolute control over data)
- Private (restricted membership)
- Public (public availability)
- Kinship (partial control over data, granted based on relationship)

### DT classification based on use

DTs could also be classified according to the type of usage and services, for example, whether they are privately or commonly owned, put to private or public use, whether they represent a specific role of the individual, whether they are of personal use to serve personal, customized purposes, route or process personal information, etc. Considering such a classification we could speak of:

- Private use DTs (privately owned to serve personal purposes)
- Public use DTs (can be privately or commonly owned)
- Personal use DT (customised)
- Role based DT (e.g. serving the citizen, employee, parent,...)

### DT classification based on occupation in space & time

We could say that a DT is a subset of space existing for a certain amount of time. Attempting to classify DTs according to their existence and persistence in space and time, we could classy them:

- According to size and form
  - Varying size (e.g. extending, shrinking,...)
  - Fixed (e.g. predefined, limited size)
  - Transforming (maybe same size, changing appearance/form)
  - Mutating (changing size and/or form and/or properties)
- According to time
  - Transient, momentary, temporary, short-term
  - Long-term, continuing, enduring

### DT classification based on interactivity

DT interactivity can be of two levels: 1) internally, within the DT and 2) externally, between the DT and the environment. External interactivity could mean that the DT acts on the environment (e.g. stimulating, causing changes) and/or the external environment acts on the DT

- DT Active "outwards" (DT -> environment)
  - Information providing (sending)

- Reactive (responding to environmental stimuli)
- Lending resources
- DT Active “inwards” (environment -> DT)
  - Receiving information
  - Sensing external stimuli (passive, internal reaction)
  - Borrowing resources
- Interactive DT (environment <-> DT)
  - Sharing info
  - Exchanging info, resources
  - Sensing the environment and acting (e.g. changing its properties)
  - Network component
- Dark spot
  - Does not allow/support interaction

### An example on classification: the home

Considering the aforementioned categories, the “Home” DT is:

- Complex (regarding its structure)
- Individual, Group, Family (regarding its ownership)
- Private, Kinship (regarding membership)
- Private use, role based (regarding its use, services)
- Fixed or Transforming, Temporary or Enduring, based on ownership (regarding its occupation in space and time)
- Interactive (regarding its interactivity)

## 6. Key technologies for DT and emerging technologies involved

### Location-based Services

The vast majority of wireless network users today are highly mobile due to the demands placed on them by their professional activities. Regardless of whether users move in their countries or a foreign country, there are a number of services offered by their service providers that depend on the place where they are. For instance, such a service may be a notification that a user may ap-

proach some accident scene or a list with hotels with available rooms. Such services are called Location Based Services (LBSs) and today tend to constitute a great percentage of the services provided in wireless communities.

The driving force behind LBS is *positioning* which means the ability to track the location of mobile users while they are on the move. The most widely used technology is the *Global Positioning System* (GPS). There are, also, some other technologies besides GPS which rely on signals emitted from base stations of a mobile network and not signals coming from satellites. This, however, requires that the user is a subscriber of a mobile telephony provider.

In addition to GPS, *Geographic Information Systems* (GIS) are also a key technology to LBS. These systems provide data related to a specific geographic location where a user moves. Such data include the morphology of the natural terrain (e.g. mountains, rivers, canyons etc.) as well as man-made structures (e.g. buildings, bridges, highways etc.).

The third component of the technology behind LBS, along with GPS and GIS, is the Location Management Function (LMF). This comprises the interface between GPS and GIS and the wireless network LBSs.

Some types of location-based services appear below along with examples explaining their functionality:

**Location-based information.** As a typical example, consider a mobile user arriving in a city and wishing to find accommodation. This LBS system (i.e. location based information) would interact with GPS and GIS, through LMF, and send to the mobile equipment of the user a list with hotels having availability of rooms along with the price per night.

**Location-based billing for phone calls or data transfer.** With this service the user can have different charges per minute for the phone calls or data transfers she/he makes depending on whether she/he is near a home zone, with small charges, or away from such a zone, where the charges may be higher.

**Emergency services.** Dialling an emergency number from her/his mobile phone, the user is

connected to the appropriate authorities of the place where the user happens to roam when the emergency arose. Due to the importance of this location based service and the requirement for immediate response from the nearest authority, the FCC has forced all wireless carriers in the US to provide a minimum level of accuracy for all users who dial an emergency number from their mobile devices.

**Tracking.** This type of LBS includes services as diverse as *fleet tracking* and *e-commerce*, for instance. Fleet tracking is used by companies wishing to know the location of their vehicles (e.g. trucks delivering sensitive materials). E-commerce belongs to this type of services since a user may want to know (by enabling this service), for instance, about sales offered by local stores or to be notified if she/he is close to a store that sells things of interest to her/him.

### Mobile devices

The term “mobile device” is used to denote, simply, mobile phones carried by a mobile telephony subscriber or, at most, some PDA (Personal Digital Assistant) carried by a user during his everyday movement activities. Nowadays, however, embedded systems technology, aided by VLSI advancements at the microelectronics level, has made possible the design and construction of devices much smaller than mobile phones or PDAs but with similar computing and communicating power (see, also, Sections 0 and 0 for other types of mobile devices). Such systems are collectively called *sensor devices* (see also Section 0 for currently available sensing capabilities for electronic devices) since, apart from their computation and communications capabilities these devices are able to sense different qualities of their environment and control, accordingly, their actions both in an atomic and a collective mode where many such devices participating in decision making as a function of their local sensory data (a mode commonly called *swarm intelligence*).

To bring things into a future perspective, we would like to mention that nanotechnology has made possible the creation of miniature mechanical (e.g. rotor machines) and electronic devices at the molecular level thus providing a much broader definition of a mobile device.

### 4G and WiFi

4G, which actually stands for *Fourth Generation Wireless Network Communications Technology* is a new standard promising to seamlessly integrate all existing wireless communications standards and devices providing broadband services and very fast data transmission rates. 4G was originally conceived by DARPA, the inventor of the Internet, which chose an architecture for 4G similar to the architecture of the Internet. This is reflected on the adoption of the end-to-end Internet Protocol (IP) and peer-to-peer networking. 4G is expected to be publicly available somewhere between 2006 and 2010, providing 4G users access to a variety of applications ranging from the traditional phone calls to digital television program viewing.

One of the major differences between 4G and 3G is that 4G will be based exclusively on packet switching for the entire range of services it will offer to users. The networks will be digital and will be able to support data transfer rates around 100Mbps compared to the maximum 2Mbps offered by 3G today (for non-moving users). The software/hardware infrastructure that will implement 4G will be able to embrace and harmonize all wireless standards such as 3G, WiFi, WiMax, and Bluetooth along with the necessary “glue” logic for making the harmonization possible.

The 10 to 50 times speedup offered by 4G in comparison with 3G is due to the use of the technique known as *Orthogonal Frequency Division Multiplexing* (OFDM), a data multiplexing and transmission technique invented and patented by Bell Labs about 35 years ago in 1970. OFDM not only manages data transfer at speeds even larger than 100Mbps but it can eliminate interference effects that arise when high-speed, high-frequency signals collide with buildings.

WiFi, which stands for *Wireless Fidelity*, and is, technically, implemented by the IEEE standard 802.11x, where “x” may be empty, equal to “a”, “b”, “e”, “f”, “g” and “h” at present. The main difference between the different versions of these WiFi versions is the data transfer speed, the transmission range as well as employed modulation technique. The data transfer speed and coverage are small (being, respectively, 54Kbps and about 50-100 meters), compared to 3G/4G and WiMax

(see below) since the main purpose of WiFi is to provide the means of connections to nearby wireless stations or “hot spots” as they are commonly known. Thus, WiFi implements the concept of a WLAN, which is Wireless Local Area Network.

WiMax is an attempt to increase the coverage, broadband services and speed of WiFi networks, implementing what is commonly known as a WMAN, that is a Wireless Metropolitan Area Network. WiMax is based on the IEEE 802.16 standard and can offer broadband access with a bandwidth of 40Mbps per channel and a range of several tens of kilometers. WiMax is supported by a number of companies that include Intel, Cisco, Fujitsu, Lucent, Nortel, Siemens, Alcatel, Samsung and Ericsson (Nokia, a founding member of the WiMax standards, left the consortium in May 2004 for lack of short-term business success of the standard leaving itself in business in the 3G/4G terrain).

### Aml sensors

Aml communities consist of both animate and inanimate agents who sense their environment and control their actions as well as communication activities with other agents depending on what they sensed.

Although sensing capabilities similar to the human senses seems far beyond reach for current sensor as well as computational intelligence technology it is, nevertheless, possible to equip inanimate agents with the capability to sense a variety of environmental conditions and direct, analogously, their actions. Thus, it is currently possible to construct a great variety of accurate mechanical/electronic sensors, some types of which appear below (their names explain their functionality and range of potential applications):

- Radiation sensors
- Gas sensors
- Thermal sensors
- Mechanical strain/force sensors
- Position sensors

- Proximity sensors
- Collision sensors
- Sound sensors
- Magnetic field sensors
- Humidity sensors
- pH sensors
- Tachometers
- Acceleration sensors
- Odor sensors (for a limited type of odors)

Current technology makes it also possible to integrate a number of the sensors mentioned above into miniature PCBs, comprising autonomous sensor nodes capable of detecting, sampling and transmitting a large variety of external stimuli.

### RFID tags

RFID (Radio Frequency IDentification) devices are wireless devices attached on tags used to identify the item on which the tag is attached. RFIDs can be carried by people or animals or be attached on objects. They can even be small enough to be implanted under the skin.

The main advantage of RFIDs compared to other identification schemes, where the identification takes place through “swiping” a magnetic card through the slot of a special reader, is that they are *contactless* and *non-line-of-sight*. This means that reading the contents of an RFID take place without the RFID making physical contact with the reader and without the RFID needing to be specially aligned. This makes the identification process especially fast and burdenless.

There are two types of RFIDs, *passive* and *active*. They both use radio frequencies in order to transmit data. Their main difference lies in the way the oscillations, which produce the electromagnetic wave that carries the information, are powered. The following table summarizes their main characteristics.



	Passive RFIDs	Active RFIDs
Power source	From reader (through the induction effect on coils under the influence of a nearby magnetic field)	From battery or transformation of other forms of energy such as sun light
Availability of power	Only when the reader is within the range of the reader	Uninterrupted, as long the battery lasts
Required signal strength from the reader	High, since it must transfer energy to the reader (through the induction effect)	Low since the RFID is powered by its own source
Strength of signal sent to reader	Low, since not enough power exists to transmit a more powerful signal to the reader	High since the RFID is equipped with transmitter with active components which power continuously the oscillator tank during its operation
Data capacity	Between 32 and 128 bits	Up to 1Mbyte
Cost	Low since it consists of a single coil	High since it contains active (semiconductor) components

More specifically, passive RFIDs operate by absorbing and temporarily storing in a coil energy drawn from the electromagnetic wave emitted by the reader, using it, instantaneously, to transmit the data they contain. This is why a strong signal is needed by the reader. The opposite is, of course, true for active RFIDs which require only a low power stimulus in order to activate their active transmitter and send a powerful signal containing the identification data. Of course, passive RFIDs also have increased processing capabilities and are able to have sensors attached to them and perform data logging.

### Wearable Computing Devices

One decade ago “wearable computing devices” were simply conventional computers in the form of a pair of glasses able to display characters and graphics, as well as a light; walkman-like device able to perform computations and send the results to the glasses. Input was given using a small keyboard or voice commands. This device plus some means of wireless communications constituted the single paradigm of a “wearable computing device”.

Nowadays things have changed. One can wear more types of computing devices than the “traditional” wearable computer described above. See Section 20 on RFIDs, which can easily be woven into clothing material, Section 10 for computing devices “worn” inside a living tissue and Section 10 for an example of a pet-wearable computing device. The way these devices collect, process and communicate information is funda-

mentally different from the analogous functions of the common PC we have on our desktop. This is why, of course, we talk about the “disappearing computer” as we used to know it. We, also, believe that the classical wearable computer (the glasses-with-a-screen one) is simply a miniature version of an IBM PC and cannot, actually, be called “wearable”. This is because the classical wearable computer still computes like and has parts similar with the classical, heavy and voluminous PC of the 80’s. Modern wearable computing devices collect information in a variety of ways, not simply with a mouse or keyboard but using special sensors and wireless connections. These devices can also act collectively and form communities from which “swarm intelligence” phenomena arise.

### Bio-implants

Bio-implants refer to devices that are inserted into the tissue or organs of living organisms of all kinds with a goal of monitoring and regulating certain vital functions of the organism. Currently, there are electronic devices in the form of a bio-implant that can replace certain nerve tissues, substitute the retina of people with impaired sight, or regulate the heartbeats of people with heart beat irregularities. RFIDs (passive) also exist (see Section 0) which are small enough to be implanted under the skin of living organisms. The fact that the RFID is implanted into the skin, thus making it inseparable from the bearer, makes it impossible to be lost. This may also have applications in the identification of people suffering from dementia, in order to quickly identify them and contact their relatives in case they are lost.

One of the major problems of bio-implants is the power supply. The fact that they are implanted in a living organism makes it impossible to use exhaustible power supply sources such as batteries, no matter how small they may be since replacing batteries would, possibly, mean subjecting the organism to an operation and to all the implications that this may have, let alone the less important costs involved and the fuss. However, this does not seem to present any difficulty since current technology has made possible the creation of devices that obtain their energy supply not from batteries but by transforming forms of energy abounding in their environment into electricity. Thus, there are bio-plant candidates that can draw power using the piezoelectric phenomenon, movements of the organism and ambient light.

### Integrating the technology elements into the DT framework

The technology has certainly exceeded expectations at the dawn of the 21<sup>st</sup> century. Nearly every idea that seemed infeasible or crazy a few decades ago is now realizable. The increase in computing speed and memory capacity of electronic components, along with their miniaturization, has made possible the creation of autonomous devices able to accomplish a variety of very demanding tasks which give the impression of intelligence.

The main obstacles for bringing together technology and the DT concepts are *regulatory* and *social* in nature and not technological at all. Imagine for example how people will react if they learn that a tracking system exists that can, also, utilize GPS signals and become so small (which it can) so as to be, essentially, a bio-implant powered by a rotor machine propelled by the blood flow in an artery or, simply, by the movement of the bearer. Well, who could prevent their implantation into human beings just after their birth, materializing to much more frightening dimensions, an Orwell's nightmare?

From a more optimistic point of view, there are already primitive DT examples which can show the way of implementing the more sophisticated DT concepts. There are already ad-hoc, sensor networks performing useful collective computations, based on the signals they sense

from their environment. These networks contain units which can also be mobile and move autonomously. On the other hand, there are also many people carrying wireless devices with them all the time. Smart homes containing wireless networks connected to the Internet are being built. A great variety of broadband services are now available over wireless networks. Network access points ("hot spots") are being created by other people or even moving vehicles. What is missing though from fully taking advantage of the available technological wealth, is people's awareness and political will to regulate the DT concept and its implementation using the technology. This, of course, is added to the fact that DT, which is still at its initiation, has a lot of definition, philosophical, and conceptual issues to care about before a more decisive step is finally taken towards the technological developments.

## 7. Boundaries and the management of distance and proximity

### Borders and markers

"Traditionally in architecture it has been taken for granted that we are engaged in inventing and constructing borders and limits". The question of blurring boundaries between architecture and its environment rose in the '90s. Architecture and landscape unite in a whole, in a continuum; thus, architecture became landscape and geography. The territory concept has become more valid than space itself. Digital technologies bring up new questions on architectural borders (and markers). Ensuring continuity without being contiguous and linking distant spaces have become crucial space design problems.

Nowadays, the need for defining boundaries has is not too pressing. Up to now, the definition of space definition used to be dependent on the definition of its boundaries. The work of concurrent architects goes beyond boundaries: "Space is produced through dispersion and discontinuity, with work with intermittencies and openings, with expansion and frayings, with syncopation and facings, with cuts and trimmings, with folds and unfoldings, rather than with the geometric purity and continuity of old profiled geometries of the Euclidean".

Physical borders delimit the local action of an activity, its local presence, while we are used to the fact that *the overall deployment of an activity transcends locality*. Distant local spaces may be the support of a synchronous activity, physical proximity is not always necessary. At the same time *a local space could participate to different bundles of activities*, be a node of distinct activities networks. A complex overlapping of physical and digital territories occurs. We must examine if the definition of physical borders and the definition of digital ones are two distinct operations closely related.

One could argue that digital territories, in certain crucial cases, deny the importance of physical borders. Electronic monitoring and control “transgresses the physical boundaries of the building by screening interior and exterior side by side, rendering them apparently equal and interchangeable” (Kolatan). *Panopticon*, as one of the more powerful schemes of the 19<sup>th</sup> century architecture and the modern society is at least to be reconsidered.

Borders are no more defined as “lines” to traverse or not. Borders are conceived as spaces “in-between”, *spaces of negotiation*. More than that, a border is always produced by a field of forces that define its ephemeral stability. At the same time it is the index / symptom of the existence of this field. A fence in an archeological site in the city center shows the tension between the economic and the city’s memory dimension. An archeological strategy may be defined that permits the development of new buildings, while offering a virtual representation of an ancient site under them. In that case physical and digital territories collaborate, the digital extending the borders of the physical.

In both physical and digital space, a border is *related to “action”*:

- Defending to cross it.
- Permitting to cross it if certain conditions are fulfilled.
- Crossing it after negotiation, leaving something behind.
- Crossing it but not having the permission to freely circulate in all territory.
- A meeting place for the two sides that do not want to cross it.

We could establish *ephemeral* borders. A closed space could be delimited in a public domain to host a private or “private” - public activity, controlled by an ephemeral “owner” that dissolves after the end of the activity the borders settled. Ad hoc gatherings in a public space for a specific purpose delimit a semi closed space that could enter to conflict with the occupational intentions of a second group. Territories must be rapidly defined and be ready to rapidly dissolve after the end of the activity’s scope. An ephemeral Digital Territory could be established before the gatherings’, physical manifestation in space, in order to invite the participants for a specific purpose. More than that, this digital territory could live after the end of the event as a link between persons, as a communication tool, leading to a future ad hoc gathering.

Borders must never be fixed once and for all. Flexibility in their construction is needed. A possibility of their constant redefinition must be present. Borders must be transformable and their markers ephemeral or changeable.

**Markers** are a way of defining / denoting the boundaries, the borders and the points of negotiation and crossing. Thus a marker can be defined as a set of landmarks with associated constraints, both of which are denoted by symbols. Markers are the technical means of realizing the borders as intuitive interfaces. They can be expanded to include interfaces, authorization, access control, information visualization, affordances, semantics, functionality, etc.

The fundamental problem in technology-based interaction is mediation: technology interposes itself in such a way that people interact with a proxy of other people. One important threat is the lack of clear indicators or demarcations, which therefore facilitates the crossing of one or more of these borders. We need semantically rich indicators of interaction affordances and dialog states.

Legally speaking, a boundary shall be a zone where an interaction in the sphere of the individual (where the digital territory pertains to a single individual) occurs. Such interaction shall relate to any lawful relationship, be it a conflict, a voluntary interaction, a transaction, or even some sort of crime. The border shall be a perceivable point, whose existence can be confirmed and proven (lawfully - in court) if necessary. It shall illustrate

the conceptual point where an action is performed in the digital world. A marker could be a digital implementation of the individual's will.

Experts consider markers as real-world visualizations of borders, which can be elements of the environment or tokens representing information sinks for holding and distributing information. The properties of markers are more important than their locations, since their *behaviour* can describe their effects even better than their locations. Therefore, locations should be regarded redundant. The legibility of markers may be affected by numerous factors. According to related replies given by experts, such factors are:

- Cultural factors;
- A shared perception of the markers. Adopting existing (gestural, cultural, etc) demarcations where possible and adapting them to a new environment might help in an "intuitive" acceptance of these markers. Still, intuitive does not mean disappearing – a marker to be effective must be "clear" and distinct. The challenge is to translate them into technology standards;
- The marker's properties, the marker or interface-node on the thresholds and proximity values;
- Definiteness / Certainty, Levels of markers, Visibility, Clearness of definition, Multiformity, Physical manifestation, Position, Language or signage.

## Ethical and social perspective

From an ethical perspective, regarding information and communications systems, also coupled with bio-implants and genetic issues, the following aspects/needs are identified:

- To improve privacy protection (data protection), respecting the individuals' right to maintain boundaries, but also to preserve privacy, autonomy, and solitude.
- To empower individuals against the introduction of systems likely to reduce their freedom and autonomy (video surveillance, behaviour control, and personal profiling) or likely to increase individuals' dependency on selection and decision mechanisms which are not transparent or understandable.

- To address individuals' right for information security, at the same time, ensuring appropriate respect for their rights, especially regarding the confidentiality of their personal data.
- To conduct continuous risk assessments, especially in order to assess the impact of new technologies (precautionary principle).
- Also, other social considerations arise, such as:
  - How far should bio-implants remain invisible to external observers, and how we relate to persons with such devices?
  - How far do we transform our social and cultural environment through DTs and their building elements?
  - How far can these technologies be used to track human beings and in which cases should this be legally allowed?
  - To what extent do these technologies allow manipulation by and for advertising?
  - To what extent might these technologies be misused by military?

Distance management and control can be achieved if appropriate security and privacy protection measures are implemented, empowering users to activate or deactivate such mechanisms according to their context- or environment-based wishes and preferences. Privacy impact analyses should be conducted in connection with the introduction of DTs and their components, and privacy and security policies set up, compliant to existing ethical norms, legal provisions, and social considerations. With respect to an individual, participating in DTs, a number of possibilities should be offered, in order for them to accept and enjoy developments towards DTs and their services:

- User Information capability, i.e. information of users about functionalities, services, security and privacy policies, and threats associated with using DTs.
- Negotiation support and informed consent, i.e. user-friendly interfaces enabling effective negotiation between individuals and DTs about the security and privacy related terms regarding usage of services offered by DTs, existing practices, remaining threats etc.
- Dependably Controlled disclosure, i.e. an individual controls his/her information, includ-



ing his/her identity information, without however creating space for repudiation attacks.

- Distance levels, i.e. defining different authorization levels, along with appropriate access control mechanism.

From a technological point of view, besides user-friendly interfaces, (context oriented) description languages, or interaction supporting protocols, components of DTs and DTs themselves should be characterized by a number of capabilities, in order to realise the above mentioned possibilities:

- Activation/deactivation capability of bridges between physical and digital, controlled by informed participating individuals.
- Privacy-oriented detectors or sensors, used to detect/sense the existence of bridges or other devices/components of DTs able to collect, process and communicate whatever kind of personal information.
- Electronic signs (etiquettes or markers), attached to bridges or other components of DTs to inform approaching participants of their existence. For example, RFIDs could be used to provide this functionality.
- Privacy-oriented actuators, used by individuals, participating within DTs, to impose specific actions, such as bridge deactivation.

Also, reasonable security measures, both technical and organizational, should be applied to control unauthorized access, destruction, use, modification or disclosure of data. Technical measures include authentication, access control mechanisms and accountability, integrity, cryptographic support, anonymity, pseudonymity, unlinkability and unobservability. Organizational measures include security and privacy protection planning and strategy, security and privacy policy creation and maintenance and disaster recovery and business continuity planning.

## Legal perspective

From a legal perspective, boundaries in relation to a Digital Territory shall essentially relate to an individual's will to act or to remain inert (omit), and to the way such action or omission is per-

ceived by others in the real world or in Aml spaces. While within its own DT an individual is, practically, "left alone", once it chooses to interact or, for the same purposes, is chosen for interaction by another individual, then the notion of "boundaries" becomes necessary. In this context, a boundary, from a legal point of view, shall constitute the outer limits of an individual's DT (or "bubble"), where interactions are permitted or where infringements actually occur.

Boundaries in the DT context shall therefore coincide with the outer limits of an individual's "personal sphere", a notion already used in legal practice, in the digital environment. In the same context, the DT (or "bubble") shall essentially be such individual's "personal sphere" in Aml spaces.

Given that a DT is the individual's extension from the real world to the digital environment, the boundary of the same DT shall essentially denote the wish of an individual to interact or not. The boundary shall be the point in the DT where negotiations with other DTs take place and interactions (actions, contracting) occur. Boundaries are needed in this context, in order to demonstrate the event and the result of an interaction between DTs. While the remaining of the DT pertains to the individual alone in the digital world, the boundary is the DT's "point of interaction" (although it is not a point, a line or any other similar construct).

The real world counterpart of a DT boundary would be the exact point in space where an individual's will positively affects other things or people. This point however is not directly perceivable in the real world, but is usually the outcome of negotiation or social rules. In a similar manner, boundaries in the digital context should not depend on space and time but rather relate to the individual's wish to undertake (or omit) an action or to cause an externally conceivable event in Aml spaces.

Therefore, the boundary is the pre-defined space in the DT of each individual, where interactions with other DTs may take place. The boundary shall carry in itself digital information as to the individual's (holder of the DT) will. For instance, it shall hold information on whether the individual wishes to interact or not. It shall also include information on the terms and conditions under which the individual wishes to interact through its digital self. The boundary should, nevertheless, be dy-



namic: any change in the goals or behaviour of the individual will affect its DT's presumption to interact or not, within the term of the same DT. Therefore, "programmable" mechanisms should be put in place in order for the boundary in a DT to adequately reflect the complex functions of a human brain as to its wish to interact or not.

The notion of a boundary for each and every DT is also required in order to determine violations of such DT. Violations of an individual's DT in the Aml context are considered in a similar manner as in the real world. An individual who has preset its DT at "no interaction" with other DT's or at "interaction under certain conditions" may witness its rules being violated in the digital environment in the same way as in the real world. Other individuals, through their own DTs, may, intentionally or not, intrude on and violate an individual's DT. The notion of a boundary is therefore essential, in order to be able to demonstrate the event and context of the intrusion.

The boundary, therefore, in a DT is also the pre-defined space in the DT of each individual where violations of the same DT actually occur. It is the point, in the digital environment, where the "personal sphere" of an individual (or its DT) is affected in any way by another DT.

From this point of view, boundaries need to be well-defined points in the digital environment. If we are to witness points of intrusion (and to assign liabilities for the same purposes), we need to be certain that a boundary did exist at a given and well-known point, and that this boundary has been violated involuntarily by another DT. Boundaries should therefore be easily perceivable by all individuals active in the digital context. In order for them to operate properly, boundaries in the digital environment must become as clear as boundaries in the real world.<sup>94</sup>

Efforts therefore should focus both on the definition of boundaries in the digital environment and on the provision of adequate boundary-management tools to the individual. The clear definition of boundaries in Aml spaces shall provide the necessary basis for interactions – consequently, for an active, rather than a passive,

digital space. Only if individuals are given the opportunity to interact with other individuals in the digital environment in a safe and persuasive way, shall the notion of Aml spaces be used in the same way as in the real world. It should therefore become evident to everybody that each DT has a boundary, further to which no other DT may proceed lawfully without the consent of the owner of the first DT. The same boundary shall constitute the mean of expression of the DT's owner in the digital environment; it shall reflect its will and its wishes in the digital space. Given the lack of physical contact in the digital environment, the employment of adequate boundary-management tools is necessary in order to reflect the individual's dispositions even in the digital space. Such boundary-management tools shall be programmable only by the individual-owner of the DT and shall provide it with the efficiency to differentiate and interact exactly as in the real world. DTs shall become the extension of the individual from the real world to the digital environment only when issues evident in the real world (such as interaction, contracting etc.) are accommodated in the digital space in an adequate and convincing, to its user, way.

## 8. Bubble, a contextual data filter

### The notion of bubble

A (digital) bubble is a temporarily defined Aml space that can be used to limit the information coming in or leaving it. **A bubble is a metaphor for visualizing DT.** It has an owner (at the centre), radius (that defines its extend) and duration (it is ephemeral). Its enclosing membrane can be set to different degrees of opacity. As a direct consequence to its relationship with DT, the bubble concept clusters together all the interfaces, formats, rights and agreements etc. needed for the management of personal, group and public data and informational interactions. Such contextual activity can be based on privacy, personalisation, priority, location, membership, ambience, social circumstances, and time. Hence, the bubble concept (being the visualisation of a DT) can be used to

<sup>94</sup> This, however, does not necessarily refer to an extremely high levels of clarity, as even today we fight over what exactly constitutes each individual's "personal sphere" in the real world and when such notion is compromised (for instance, in family relationships, public administration relationships, penal law relationships etc.).

make filtering and selection of data possible. The bubble may be illustrated as a semi-transparent membrane that can be tuned to function differently depending on the will of its owner and 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 towards the bubble is tuned based on information needs and requests.

In Aml environments, the human becomes ubiquitous. The ubiquitous human (digital self) is formed as a collection of bubbles, and extends over several DTs (or bubbles, for visualisation purposes), while exercising different degrees of ownership (if any) on each. The bubble constitutes the extension of the individual in the digital world; it is its on-line self in the digital environment. A bubble can do what its individual wants it to do: it can react, be passive, contract, act etc. The bubble is connected to an individual's will and is, consequently, its on-line self.

In principle, a bubble pertains to an individual; it forms its protective "interface" however there are instances where a group can, in its conjugation develop its own bubble. This second bubble does not dissolve the single ones. Thus, a bubble can be a shared space created over many DTs. A DT may become too personal, so bubbles are a sharing mechanism.

So there can be no a 1-1 correspondence between DT and bubble, as in some cases these two notions describe the same entity, while in others they don't.

Counterarguments are:

- A DT is a concept we invent in order to extend the concept of privacy in the digital world. The bubble is a metaphor we use to describe the information exchange between DTs at a given time.
- A DT is a space; space has no borders. A bubble denotes a protected sphere, hence it must have boundaries.
- The DT is a model (snapshot) of the real world augmented with ICT, while the bubble is the personalization of a DT. A bubble is personal to someone; it is more private than a DT.

- DT is a space of interaction and bubble is a formation that exists only for some time in order to protect privacy matters and interaction between members of DTs or between other DTs. The notion of ownership of space is important because it is linked to privacy and security. A bubble is something spontaneous, which comes and goes.

The presence of a bubble in a DT defines the interaction possibilities. As soon as one enters a DT, one potentially has access to services, but one receives only those services allowed by his/her bubble; hence the bubble acts as a contextual filter of incoming and outgoing data. The activities of a bubble are influenced by what is happening in the environment.

The most familiar example of a bubble is residence, which is also protected under EU law. Home is a protected sphere delimited by the walls of house, but the notion of privacy follows the home owner outside the house (i.e. car). Accordingly, the bubble of protection follows a person's movements as long as these are related to the Virtual Residence (the home in the digital era). The system should be mutable and adaptable. The interface should be "plastic", i.e. nurtured and evolve as it is being used.

Bubbles can be either static or dynamic. If a bubble is conceived "static" for each individual (each individual has one bubble) then compartmentalization of this information should probably occur. If a bubble is "dynamic" for each individual (changing according to the Digital Territory intended) then each bubble shall contain the identity the individual wishes it to contain.

To create a bubble is a decision that derives from the **necessity to interact with others**, especially if the DT realises introductions from the outside, therefore is subject to changes. This makes it a dynamics decision.

A bubble is visible and recognizable from the outside. However, a bubble does not have visible borders from the inside, allowing the perception of its immediate environment. Thus it maintains its own structure without excluding external contributions.

Full control over individuals' bubbles is highlighted as an important factor. Issues such as filter-

ing, selecting which data becomes available etc. all suppose full and complete control of each individual over its corresponding bubble(s).

A (successful) bubble adapts (and protects its member(s)) to all forms and directions. Like a highly evolved species it protects its owner and can mutate to various forms as long as it maintains its basic integrity. Types of adaptation include: adaptation of complexity of internal structure; adaptation of “permeability”; adaptation of interpretation of data; adaptation of reflection; adaptation of absorption; adaptation of elasticity

### DT examples

In this section, we shall describe DT examples that have been proposed by the experts who participated in the survey. These examples describe different DT types and show how inspiring the DT concept has been, but also how differently it was perceived.

### Virtual residence

The notion of Virtual Residence was originally conceived to describe the Smart Home, i.e. the evolution of home from being a shelter from nature to becoming a shelter from digital environment (and its threats). It has been proposed as a means of tackling new concerns about identity, privacy and security within an Aml space that encompasses both physical, online and virtual lives, and the embedding of computing in everyday devices. It consists 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, and households and their virtual representation and mobility and interoperability between different Aml environments.

Virtual Residence is more than a space: it includes the activities that take place in it and the people (or agents) involved in or affected by them. Each individual or activity usually creates its own bubble. Thus, its size varies depending on the sub-DTs it includes at every given moment. Its use varies also, depending on the individual and the time: the same DT may be private or public at different times; some DTs are strictly private, some may be necessarily public.

Virtual Residence also presents a suitable case to examine issues that relate to content management and to identity. Content management refers managing access to the personal data and digital content stored in or associated with the Virtual Residence and in finding ways to negotiate the use of this data, either among DT owners, or external entities (owners of other DTs). To this end, appropriate markers have to be devised, which will mark the borders of the Virtual Residence and imply the protocols that have to be used in order to be accepted in the DT.

### The University

The primary purpose of the University DT is to facilitate teaching and learning activities. These include lectures, tutorials, workshops, access to library, support for Internet connections etc.

The University is a public DT, although it presupposes the existence of private sub-DTs. Its size depends on the number of members (students, staff) and is physically related to campus infrastructure. The infrastructure required to realise the University DT includes:

- Campus servers
- Communication (always plugged-on)
- Teaching software, presentation software, collaboration tools etc
- Teaching content deployment (teaching content per se may belong to library DT)
- Protection of intellectual rights
- Privacy as a right or a utility
- Aml components
- Identification services
- Location-based services

The teaching services offered by the DT can be digital (on-line learning), physical (campus), as well as of mixed form (open universities). These include knowledge sharing and exchange, research facilitation and promotion, facilitation and support of learning communities and knowledge certification

Thus, this DT involves diversiform human communities (e.g. varied ages, backgrounds, nationalities, etc). This DT is authorised to certify knowledge (type, degree, etc), which constantly

changes, adapts (new knowledge, challenges, findings, social needs, etc).

One could discern the following bubbles within the University DT:

#### **Student bubbles**

- a) Student communities bubbles
- b) Teacher bubbles
- c) Lecture bubbles, which can be described by the following properties:

**Owner:** professor on behalf of the University

**Purpose:** teaching schedule, teaching objectives, teaching strategy, target audience

**Confidentiality:** could be defined regarding content usage

**Privacy:** could be defined with respect to the necessary modes of communication (i.e. among teacher and student)

**Markers** (each of them defines borders not allowed to be crossed):

- 1. Lecture admission policy: screen message
- 2. Intention to participate
- 3. Authorization to participate: defines rights to use DT services and Aml components
- 4. Availability to communicate
- 5. IPR markers on digital content

#### **Bridges:**

- 1. Location model: where should Aml components be placed?
- 2. Create a continuum between classroom, home, library etc.

### **UTDT, a café in downtown New York**

A café is mostly perceived as a public space. Yet many private or restricted activities take place within a café. Consider for example two lovers who meet in a corner: they are willing to exploit the DT café in order to create a common transitory bubble, which will encompass the moments they share; however, there are data that will never enter this common bubble, but will remain in the individual DTs of each. Other customers may prefer isolation in order to read a book: they have to

clearly set the markers of their bubble so that they cannot be easily penetrated by the services offered by the café DT. Some other customers may prefer to watch a game together: they engage in a common bubble that includes activities that take place in the field where the actual game is happening, although they only watch it on the TV (which belongs to the DT café infrastructure). Other services offered by the café DT include wireless network connectivity, mobile phone network, games etc.

The bubbles within DT café reach an equilibrium state, so that bubble owners are satisfied. Sometimes, external or random events may shake this equilibrium: a new customer enters or someone leaves; an accident happens in the road outside; random messages are sent to those inside the café who use its wireless network (a policy touted by the café management to bring people closer); IP addresses are dropped at random, etc.

The effect that the dropping of the IP address has is an interesting one. It kicks the person out of the subgroup of internet services, yet he is still physically in the café. Physical and digital groups go hand in hand (i.e. the person sits in the café on table A using his laptop like everyone else here and he is browsing the internet in the same space, seeing everyone's network persona in parallel).

### **A neighbourhood**

A neighbourhood is a mixture of open and closed spaces, with private or public uses. It has a complex internal structure containing other DTs which may be tied to a physical space, such as residences, shops, streets, cafes, or encompassing activities, such as shopping, playing games etc. It is a surrounding where an individual forms meaningful and multi-layered types of exchange and relationships. These range from commercial, to civic and "interpersonal". They also are constantly changing.

The activities that happen in a neighbourhood can be transitory (i.e. a street fight) or more permanent (i.e. new neighbours moving in). The DT size is variable, as it depends on its constituent DTs. A neighbourhood can even be mobile (i.e. my residence neighbourhood, my work neighbourhood, my parent's neighbourhood etc.).



### The car

The car is sometimes considered as an extension to the home; thus the car DT could be part of the Virtual Residence DT. Even in this case, there is value in examining the car DT as an independent DT. It is most of the times a private DT (or confined to a group of people). It is mobile: it moves through other DTs. As it moves, it exploits the infrastructure offered by these other DTs in order to ensure continuity of bubbles contained in the car: the mobile phone conversation continues; the same goes for radio station reception or internet access. Because of this, however, it is vulnerable to attack by agents in its environment: sniffer programs may operate at a certain DT outside the car, which may sense and copy data in the car DT without the car DT owner(s) becoming aware. Although the car as an object leaves no traces on the roads it travels on, the car DT will certainly leave digital traces in the systems it connects to, as the car passes by.

### The suburban train

The suburban train is an interesting DT example, as it can be described using other, more elementary or familiar DTs. For example, most of the car DT features are “inherited” to the train DT, especially those that have to do with mobility. On the other hand, the train is mostly a public space that is used either for private or public activities; in this sense, it inherits several features from the café DT.

Further analysis reveals that in a train one could use the different types of proximity to define temporary bubbles. For example, an announcement may concern only those who disembark at Nerantziotissa station; it should not intrude on the privacy of the other passengers. Another example is passengers sitting in the same compartment: they may be engaged in a group activity (i.e. playing a game of cards, or watching a movie in one’s laptop that he has downloaded from his Virtual Residence), or they may be withdrawn within their individual bubbles. Even in the second case, some activities may intrude on the privacy of others, i.e. speaking loudly on one’s mobile phone.

## 9. Private and public spaces

Private and public are not two different opposed notions, but rather two different aspects along a spectrum that is defined by a gradual change in access rights. Individual, family or group can thus be considered as different instantiations of private space; they involve a private space where a group of selected few have access privileges.

Public on the other hand can be defined as a space with no access limitation whatsoever, nor selection; a space that is accessible to everybody.

The type of classification, in the private-to-public spectrum, depends on the application context. Classification is based on personal identity. The specifics of the classification can be about the individual life, family and relatives, or work oriented.

### Perception, control and social aspects

The management of privacy is directly proportional to the management of distance. Distance and access protocols are different in different cultures (i.e. Asian, North European, African, etc). Proximity is perceived differently by different populations, so we can say that proximity has a cultural background. Public, Social and Personal are different aspects of proximity.

Controlling distance and proximity is in fact a way to control security. The level of security can range: the closer the proximity, the lower the level of security that is needed. The closer the proximity in a DT, the more intimate one is and the more information one has access to. These proximate DT spaces can be described as a ‘private’ zone, a zone where only selected few have access to the DT of the individual.

Nevertheless, the more distance between DTs the less trust one may have over the information released, and therefore more secure management of the information is required. Public DTs need to be trusted, and trust takes time to build.

Intimacy is what defines the access rights in the private space in the physical (non DT) world. What people may expect from proximity (being in one’s private DT sphere) can be more openness, and more access to certain types of data to one’s



relatives. Therefore it may not be the distance (which in digital space does not exist), but the level of intimacy that is the measure of proximity in DT. Certain parameters can be defined to describe the level of intimacy, depending also on context, taking into consideration history (evolution of a relationship through time) as a factor.

Private spaces are spaces that only trusted parties are allowed in. Privacy can be realized by managing access rights, and therefore proximity.

## Historical aspects

In the history of architecture the division between private and public is a modern one, started to be established from the 18<sup>th</sup> century. Privacy was defined as “the state or quality of being apart from company or observation” and was very rapidly linked to the concept of domesticity.

The privacy as separation from the public realm and from other houses was related to the conception of the private as discontinuous and the public as continuous.

Needless to mention that historians locate the appearance of the “house” as we know it today, with its divisions to common areas and to bedrooms between the 17<sup>th</sup> and the 18<sup>th</sup> century, linked to the bourgeois society.

At the same time, working was disconnected from the house and being at home was conceived as a retreat from the world.

Bringing the public into the isolated territory of the house was the result of the “media” technologies, starting with the radio. In “The Thing”, Martin Heidegger criticizes the media *in* the house as diminishing the distance from the world.

The Radical Architecture of the sixties in one of its many theoretical trends denies the *house* in favor of the *home* proposing the *bubble* concept. Rayner Banham in his famous article “A Home is not a House” suggests the bubble as an active environment, very near the body. Takis Zenetos, a visionary Greek architect proposes the bubble in its parametric dimension. The bubble / capsule filters the environment, keeps unwanted information out, while accelerating the influx of information desired.

We could advance the hypothesis that the bubble concept in space design was developed under the influence of behavioral theories such as Sommer’s and Altman’s, where four zones from public to personal territory were defined. The bubble is positioned to the personal space very near to the person’s body, having three extensions (from center to the periphery) to the acoustical, optical and mental space. In the same theoretical framework, the bubble has an owner and is delimited by boundaries, which are denoted by territorial markers.

In the Radicals’ theory and design, the bubble was never dissociated from the supporting structure. It is the capsule / gantry concept that permits also the bubbles / capsules to be combined in different ways to form communities, which are always clipped on to the supporting structure.

The bubble defined the absolute private space, a strict personal area a filter between man and nature. In our conception of digital territories, the bubble is no longer physical but digital, the supporting structure following this movement of being digital. We could then argue that private (digital) spaces can possibly occur in public (physical ones), or public (digital) space in private (physical ones).

## The role of technology in manipulating the characteristics of a DT

One of the most important characteristics of a DT is its adjustable permeability. By this we mean that the easiness by which a DT (as a complex kind of space) can be “trespassed” by an external entity (another DT, for instance) can be adjusted taking into account a variety of parameters and issues related to both the DT and its surroundings. The key word here is “easiness”. The two extreme situations for a DT are either to restrict any kind of access to it from its environment or to allow full, unconditional access. Both extremes may lead the DT to “death” or severe damage due to either lack of vital external resources (e.g. information) or due to malicious attack attempts or stealing of information by other DTs moving in the nearby surrounding space.

Thus, it is critical that the DT is able to interact with its environment in order to avoid “starvation” (mainly information-wise) while, at the same time,

protecting itself and the information it exchanges with its environment. Such “selective permeability” and protection can be established by means of techniques adapted from modern cryptography and IT security combined with technological advances in networks security (either wired or wireless networks). In this section we will only outline the fundamental ideas behind this approach.

Perfect secrecy of information is a concept first formalized by Claude Shannon. In a few words, perfect secrecy is possible if perfect randomness is possible (one-time pad systems) which should be available in abundance (i.e. as the size of the information stream increases, the random bit stream should increase so as to be at least as large as the information stream). Thus, perfect secrecy comes at a twofold cost: (i) need for perfect randomness, and (ii) abundance of randomness.

Modern cryptography has disposed of both costs by introducing information secrecy schemes which are strong even if perfect randomness is not possible or, if possible, costly to produce in abundance. These schemes avoid these costs by introducing a cost which can be tolerated given current technological progress of cryptanalysis: “perfect secrecy” is replaced by “hard to breach secrecy”. In other words, no practical modern cryptosystem is perfectly secure but it is “almost” perfectly secure for years to come, unless some unlikely technological advancement is made (e.g. quantum computers are built which are easily available and at a reasonable cost – this prospect seems to be decades away though).

Thus, today’s technological advancements (stemming mostly from the field of cryptography) allow the definition of boundaries in DTs which can be strengthened and weakened at will in order to block or allow other DTs. Moreover, this strengthening and weakening can be graded so as to have different access right levels for various classes of interacting DTs.

## 10. Bridges between real and digital worlds

Digital Territories, which have been formed by the interconnection of physical objects that embed digital components, postulate the integration of the two worlds, searching for operative def-

initions of new evolving-in-time functionalities. There is a shift of emphasis from the personal computer as a discrete object in the physical space, to the physical objects *per se*, spaces, buildings, cities, all of them embedding computing devices at different levels.

Bridges between physical and digital are actually **elements/components of Aml** spaces linking the physical and the digital. Thus, they may be combinations of physical and digital media, often so interwoven with everyday life that they are no longer noticed as special, novel or distinct. For instance, when passing to someone a USB flash memory disc to exchange files, or when asking the colleague in the same office to send a file via an FTP server or a peer-to-peer program, the bridges between electronic and face to face interaction are themselves ‘disappearing’.

A DT could be characterized by its ability to create new bridges, by the ease with which its bridges are formed or broken. A DT must be able to accept a new bridge and integrate it to its overall functionality. A DT must be able to continue functioning if one of its bridges is broken. Thus, although not alone adequate for DT creation, bridges are necessary elements of a DT.

The need to create bridges arises from the generation of new, additional or transformed data, the need to transfer information, as well as the need to pass to a different level of hierarchy, either within a DT or between different DTs in Aml spaces.

Bridges are of interest when they enhance DTs by supporting modification of contained relationships, newly-emerging requests of DT members and enable the creation of (new) complex DTs. When created for generating complex DTs (i.e. by DT inter-connection), they allow consideration of new links that were not possible before.

## Aspects of real and digital worlds

### Bridges’ ontology

Bridges are discrete elements disposing of certain autonomy in their conception and internal structure. Sensors, actuators and RFIDs are examples of bridges between the physical and the digital world. When one builds a bridge between the physical and the digital space, it is in fact a bridge

between activities that take place in remote physical spaces in the same time.

Building a bridge is a process. It shows intention, expected functionality, changes the nearby areas of the two sides that it bridges and probably, in the future, introduces changes or evolves its structure according to new needs. Building a bridge is also a design decision. You must always decide which part you link with what, for how long and what type of actors you allow to pass. Bridging means that you create the conditions that allow communication and exchange of data to happen. It implies answering the following questions:

- Where bridges are located and how (locational model);
- What type of context information is processed (context model);
- What functional model links them (network model);
- Who is the owner and how his activities necessarily produce the above three models.

Bridges consist of Aml components *distributed* and *integrated* to physical space, offering functionalities that serve interrelated activities - schemes evolving in time. Building a bridge between the physical and the digital space, implies the conception of a *locational model* to decide Aml components allocation.

Aml components are *distributed* in the physical space. A location model represents the physical context as a relationship between an activity (group or individual), the space it occupies and the Aml components embedded in the space. A location model integrates a time parameter. We have different location models for documentation and management of physical space, for evolution-transformation of the physical space or for the digital extension of activities.

Aml components are *integrated* into physical space: they could be fixed to one place or mobile, integrated to the fabric or clipped on. They bridge the physical and the digital space in various ways as described by the locational model.

Building a bridge between the physical and the digital also implies the conception of a *context model* describing what do we expect to perceive

as *context information* from the physical world and what is needed in a DT. A *context model* is available to software applications; it captures the state of the physical world using sensors. A bridge can be a mechanism that provides input to a context model, because it makes the information captured by sensors available.

Bridges could be *temporal* or *ephemeral*. A DT could be characterized by its ability to create new bridges, by the ease with which bridges are formed or broken. A DT must be able to accept a new bridge and integrate it to its overall functionality. A DT must be able to continue functioning if one of its bridges is broken.

Bridges can be *mobile*, they can be *one-way* or *two way*, *personal* or *private* (e.g. a PC used for access to e-commerce, e-banking, etc) and they may become commonly available for sharing information (e.g. phone's loud speaker).

Bridges as physical elements are DT's manifestation in the real world and thus are integral parts of their identity.

Bridging creates the possibility for interaction, represents a possibility, yet actually having data flow across makes a recorded event become a fact in the virtual world. The existence of a bridge creates the potential and conditions that allow communication and exchange of data to happen.

## Bridges and privacy

The building process of DTs and the multiplication of invisible and uncontrolled bridges between the real and the digital environments may generate threats with respect to privacy and security.

Identity theft, loss of control, sense of powerlessness, compromised civil liberties, sense of disconnectedness, alienation, data capture from an actor that does not belong to the DT, circulation of unwanted personal data across organizations, persons, revelation of intimate details, control by persons not belonging to the DT, consumer tracking, unsolicited communications are some examples.

There is a general feeling that the more integrated Aml components will be, the more difficult the elimination of these threats will be. Bridges should have *properties*, in order for these threats to be minimized.

All actors of a DT must be aware of the existence of invisible bridges. These bridges are intrinsically linked with the notion of *markers*. In the case of an impact on the user's privacy, he/she should be at least informed in order to accept or not this new link. However the multiplication of these bridges and their growing pervasiveness makes necessary the adoption of a more global approach driven by regulatory framework and proper standards.

A new "*social-contract*" is needed, that will make visible or generally perceivable any interaction in which a bridge is involved. A *regulatory framework* is needed. The multiplication of bridges and their growing pervasiveness imposes to adopt a more global approach driven by regulatory framework and proper standards. The Aml components production industry must follow those standards in order to diminish these threats. One could install quality control organizations, like consumer unions, as a continuation of existing organizations with existing reputations.

It is usually stated that technologies are neutral regarding privacy issues. However, some technologies may be *privacy-friendlier* than others. Technologies must be evaluated and classified according to these criteria as low, moderate and high privacy-friendly technologies.

'*Trusted bridges*' could be a solution towards secure and privacy protecting DTs. Obviously, built-in security functionality is highly required. It seems that functional and non-functional requirements should be placed on bridges.

### Bridge enabling technologies

The creation of bridges arises from the generation of new, additional or transformed data, the need to transfer information, as well as the need to pass to a different level of hierarchy, either within a DT or between different DTs in Aml spaces.

Examples of current technology and artefacts that can be used as bridges are: Sensors / Actuators, RFIDs, Screens, Controls of any kind, User interfaces, Locative media, Smart materials, Nano – mechanisms, Location-based services, CCTVs, etc. When one builds a bridge between the physical and the digital space, it is in fact a bridge between activities that take place in remote physical spaces in the same time.

In the following, short descriptions of location based services, RFIDs, bio-implants, biometrics, user interfaces, and CCTV's are presented.

### Location-based services

The geographical location of an individual is the basis of these services. Mobile tracking devices can be implemented facilitated by the widespread use of mobile phones and GPS systems. LBS can be divided into location-aware and location tracking services, where in the former the individuals themselves are the receivers of the services while in the latter user's information is provided to third entities.

Their acceptance is influenced by technology user control features, application or service attributes (if appropriate for a given situation, for instance in an emergency, an individual will perceive privacy intrusion regarding his/her location data significantly lower than tracking data processed in his/her work) and personality traits (conscientiousness, extroversion, agreeableness, neuroticism, and openness to experience).

In conclusion, location based services are needed to realize ambient intelligent spaces, but they can also be exploited as monitoring or privacy limiting means or tools. In order to reduce privacy related risks and to increase acceptance of Aml technologies, privacy friendly or privacy enhancing LBS should be sought. Research should aim at developing LBS models privacy and security related requirements. The greater the degree of control of actions and data allocated to the individual, the more likely the individual is to accept and endorse these technologies.

### RFIDs

Radio Frequency Identification (RFID) technologies are expected to be one of the main components of the future Aml spaces and DTs. As mentioned in chapter 2, RFIDs consist of tags, i.e. tiny integrated circuits equipped with radio antennas (small chips with several thousand transistors and a small antenna) and readers. Tags may be active or passive, and their operating frequencies vary from 0 to 24,125 GHz, in the radio spectrum's unlicensed portion and where regulations govern power output for readers. According to the read/write capability of their memory, RFIDs may



be classified in low-end (very small, i.e. few bytes, read-only memory), middle (up to hundreds bytes, possibly writeable memory, and high- end (contact less smart cards with a microprocessor and operating system).

RFID technologies are already used in a wide variety of applications, from inventory management to transportation, aviation, healthcare, security and access control, animal tracking, and payment systems. Several other developments will imply a dramatic increase in RFID's deployment. For instance, consumer goods distribution will be facilitated by embedded tags, 'i-chips' developed by Hitachi are designed to be embedded into photocopier paper to enable automatic document tracking, RFID tags will be embedded in automobile tires, and RFIDs can be embedded into product labels by special 'printers' developed by Zebra Technologies.

Privacy advocates (Article 29 Data Protection Working Group) are concerned about the possibility of some applications of RFID technology to violate human dignity as well as data protection rights. Also, according to a statement published by US American civil liberties organizations and several academics, improper use of RFID technology has the potential to jeopardize consumer privacy, reduce or eliminate purchasing anonymity and threaten civil liberties.

In any case, tags can be read by third entities, without their owners being aware of it, and they do not maintain any history of past readings. Furthermore, tags and readers can be covertly embedded in the environment, thus raising privacy and security related concerns. It should be noted, however, that ISO 18000-3 Mode 2 tags have space for one read password that authenticates the reader before permitting access to a tag's content. Also, research work shows towards more secure and privacy-friendly RFIDs technologies. RFIDSec claims to have a high security RFID solution with integrated intelligence, which allows the tag to remain active after leaving the point-of-sale without compromising privacy or security. RFIDSec has been nominated for IST Prize 2006.

## Bio-implants

Bio-implants were already researched and developed in 1960s (consider for instance the first heart pacemakers), followed by bladder stimulation devices in the 1980s. More recent examples are active implants used as stimulators to treat pain from patients with tumor and trembling caused by Parkinson's disease, or to improve the restore function of quadriplegics. Currently available devices include cardiovascular pacers, cochlear implants, auditory brainstem implants, implantable programmable drug delivery pumps, implantable neuro-stimulation, deep brain stimulation and artificial chip-controlled leg.

Because bio-implant devices embed microchips, they may be classified according to their functionality or capabilities, as follows:

- Read-only, the simplest form of bio-implant devices, with limited storage capacity, mainly serving identification purposes, as for instance the identity of Alzheimer' patients.
- Read-write, as opposed to the above, further information may be added to the information already stored and distant programming is possible. An application example could be an individual's medical history.
- Read-write and radio signal emitter, which enables radio signal tracking (see RFIDs). These devices need a kind of power source so that they can be constantly monitored, since readers are usually mobile.

Biosensors, i.e. sensors implanted inside human body are used for accurate monitoring of inaccessible parts of it. In a human body, they may form a network to collectively monitor its health condition and making decisions based on it, as for instance alerting doctors to a probable medical crisis. Various specific chip devices are researched, such as artificial hippocampus, cortical implant for the blind, artificial retina and brain-computer interfaces. Bio-implants may cooperate with wearable computing and communication elements to enable further surveillance and tracking applications.<sup>95</sup>

<sup>95</sup> Already in 2003, a successfully tested prototype of a subdermal GPS personal location device was claimed.



Also RFIDs of very small size with no chemicals and with or without power supply can be used as bio-implants. For instance, VeriChip™, a sub-dermal RFID in the size of a grain of rice, is implanted into the fatty tissue below the triceps. Other devices use the human body (skin) as radio signal transmitters.

There is a need for bio-implants to be implemented in a manner respectful to fundamental rights and private life. Human dignity, inviolability of the body and physical and psychological integrity, privacy and data protection, and especially data minimization, purpose specification, the proportionality principle and relevance must be followed. Furthermore, the precautionary principle [9], as a general risk management tool should be applied in order to weigh the benefits of a technology against its possible risks.

### Biometrics

Biometric techniques, such as fingerprint verification, iris or face recognition, retina analysis, hand geometry, voice and hand-written signature verification, are increasingly becoming basic elements of authentication and identification systems. They process data related to human physiological or behavioural traits which serve as biometric characteristics, provided they fulfil properties such as universality, distinctiveness, permanence, collectibility, performance, acceptability and robustness.

However, biometric-based authentication and identification systems can make two types of errors:

- false match or acceptance, in the cases where they erroneously conclude that measurements coming from two different individuals as coming from the same person, and
- false rejection or non-match when they erroneously attribute to two different persons measurements taken from the same individual.

Biometrics as components of positive personal recognition systems are gaining special attention, since they are convenient to use and alleviate users from remembering passwords or other secrets, offering thus convenience and preventing re-issuance costs faced with other mechanisms. They still exhibit problems with accuracy and speed, as well as lack of secrecy. More impor-

tantly, however, they raise privacy-related concerns [8]. From a privacy protection perspective, biometrics-based identification should not be used for processing purposes, which can be achieved by applying only biometrics-based authentication. Also, centralised storage of biometrics data should be avoided, in order to reduce relevant risks. Instead, if necessary, biometric data should be stored in devices such as smart cards held under the responsibility of the individuals they refer to. Technical solutions of biometric systems and related standards should be elaborated taking under consideration these conclusions in order to be privacy-friendly, minimise the social risks and prevent misuse of biometric data.

### Closed circuit TV systems (CCTV's)

Image and voice acquisition systems such as closed circuit systems or cameras and web-cams with microphones, and more sophisticated tools have been increasingly used in Europe in the last few years. Developments and trends towards digitalization, miniaturization, dynamic-preventive techniques, networking, linking with extensive data bases, and combined with facial recognition systems or further image processing techniques increase extremely the opportunities and capabilities offered by these systems.

Such systems may serve a number of purposes, such as human, public interest and property protection, prevention, detection and control of offences, collection of evidences, and other legitimate interests. Video surveillance systems may be found in stadiums and sport facilities, in publicly accessible buildings such as museums and archeological sites, in transports sector and for traffic management, in airports, on ships, within medical facilities, and many other places. They can also improve procedures of our democratic society, as for instance activity transparency of local authorities and parliamentary bodies, especially when combined with conferencing and voting systems.

However, distant monitoring of events, situations and occurrences enabled by these technologies may pose severe threats to security of DTs and to privacy of individuals participating in them. Proliferation of image and voice acquisition systems in public and private areas should not result in violation of human rights and fundamental liberties. For example, there is serious risk that individuals

may be subject to disproportionate monitoring and information collection procedures, which will render their identification easy in a number of public and private places.

A further extremely serious threat appears in scenarios where CCTVs, integrated with facial recognition and human behavior analysis systems, are used for dynamic-preventive surveillance, since such applications may result in an individual's discrimination.

### New user interfaces

It is predicted that in the next 15-20 years neural interfaces will be developed that will increase the dynamic range of senses. Voice recognition has already been researched for some years and is used in current user interfaces. Aml scenarios include video interfaces capable of recognizing 3-D images and of tracking a user's movements. These can be extended to include recognition of an individual's emotions by voice or image analysis. In addition, eye direction or human thoughts may be exploited by future user interfaces, as mentioned in the literature.

The above mentioned user interfaces pose severe privacy and security threats. For example, using the current and expected future technical possibilities to intercept voice or to monitor places from a distance, sensitive information, such as authentication credentials, may be disclosed to unauthorized individuals.

## 11. Legal and social framework

Study of the legal framework with concern to DTs and bubbles shall necessarily follow the clarification of all open definitional issues; once it becomes clear what is meant by DTs and "bubbles" and what their relationship to an individual exactly is, only then may legal research apply its methodology in the digital context. The problem with Aml is that notions that are apparent and self-evident in the real world need to be re-defined, indeed in a way that shall bring general consensus. Such fundamental notions as "individual", "action", "omis-

sion" are elusive in the digital world, and research should first focus on identifying them in a concise and clear way. Only when there is a clear picture as to what an individual is and does in Aml spaces, we may turn our focus on case-specific issues such as privacy or identity in the digital environment.

Consequently research should concentrate on two topics: first, definition of the fundamental notions in the digital environment, and, then, elaboration on certain legal issues pertaining to them. For the sake of analysis however, after the first research task is elaborated, some insights shall be provided on those aspects of life that shall, presumably, be most affected by the emergence of Aml spaces.

### Fundamental notions

In order to be able to talk in a legally meaningful way of "Digital Territories", "bubbles" and the "individual in the digital world" we first have to define accurately such notions and their relationships.<sup>96</sup> While doing this, however, we must use the principles that underlie our contemporary legal system; principles that have been formed over human history and that will not be easily abandoned in view of a new reality (the digital environment) unless there is a very good reason for it (and until today none has appeared). Therefore, what should indeed be done today is to find the "parallels" between the real world and the digital environment and to try and accommodate legal notions from the first to the other, in order to secure a possibly trouble-less transition.

The analysis of the legal principles that underlie our legal system and which should be transposed in the digital world, is not within the scope of this study. Instead, some basic notions will be presented as an indication of possible ways to deal with these issues.

The first notion essentially relates to the human being. Evidently, our legal system is established upon the notion that human beings act in the real world. The definition of a human being in the real world is not necessary; it is, and has always been self-evident. This is not self-evident in

<sup>96</sup> While in this analysis, however, it has been presumed that a Digital Territory equals to a Bubble and that it refers to only one individual, who owns it and uses it as an extension to its self from the real world to the digital environment.

the digital environment. We need a counterpart of the notion of individual in Aml spaces, in order to use it as the basis for the legal system in the digital world.

The second notion that requires further clarification is the digital environment itself. What exactly is a Digital Territory? How does it relate to space and to the individual. In the real world, our legal system takes for granted not only the individual, but also the world she lives in. The world is divided into material and immaterial goods, property upon them is recognised, rights are awarded upon parts of the real world to individuals. At another level, individuals interact with one another or act against the other and all such actions entail legal consequences. All these notions (goods, actions) are obvious in the real world and the legal science mostly had to regulate them. Nevertheless, this is not the case with Digital Territories: the “condition” of the individual in the digital context (that is, whether, it is inert or it acts and reacts) needs clarification.

In the same context, the relationship between a Digital Territory (or a bubble for the same purposes) and the individual is of paramount importance. Does the term Digital Territory refer to the digital world, as opposed to the real world? And, if this is the case, how is the individual, as known in the real world, placed in it? Is it through bubbles? Are we to perceive that a bubble is the individual in one instance of life (for instance, while contracting, acting, interacting, remaining inert)? It is obvious that in Aml spaces we need a unit of measurement, exactly as the individual is the unit of measurement in the real world. What is going to hold this role? Although, while preparing this analysis, the convention was made that a Digital Territory is a bubble and at its centre is a single individual (that is, that a Digital Territory is the projection of the individual in the digital environment) indeed no general consensus has been struck to this event.<sup>97</sup>

The need to “project” the individual in Aml spaces in a comprehensive but coherent way is

stressed by the third fundamental legal notion that needs to be accommodated in Aml spaces: the notion of accountability. The enactment of individuals in an environment other than the real world does not mean that their behaviour shall remain unregulated. On the contrary, the introduction of new spaces requires the installation of efficient regulatory schemes, in order for them to flourish. General adoption of Aml spaces presupposes public trust in them, and such trust can only be gained through public conviction that the rights enjoyed in the real world are not compromised in the digital environment. This is why the projection of the individual from the real world to Aml spaces, together with the drawing of “parallels” between the two systems and installation of known legal notions to the latter, is important. Transition to Aml spaces shall be achieved in a better and more efficient way, if individuals can easily see themselves in the new environment and believe they know the “rules of the game”. To this end, re-invention of every single legal notion known to us for the digital world would not only appear a waste of resources, but also a project bound to fail.

It is therefore suggested that the above fundamental legal notions are approximated closely in future research. Our current research demonstrated a lack of clarity (and, perhaps, understanding) as to the basics of law in Aml spaces. Although the notion of digital territories is allegedly already present (through applications such as e-commerce, e-banking, agents etc.) it is suggested that such instances are momentary and piecemeal: an individual’s logs in the system, indeed performs an action within a digital environment, but then is out of the system again (and the whole transaction is regulated by firm, real-world legislative provisions). If we are to envisage enactment of the individual in a digital world we cannot continue adopting legal notions that accommodate other needs (of the real world), but we equally cannot rediscover everything. What is actually needed is further study of the basic notions (Digital Territory, bubbles, individual) in the digital context, and the creation of a scheme that shall strike public consensus, so as to be utilised in Aml spaces.

<sup>97</sup> Nevertheless, the Questionnaire did point out that “most respondents appear to accept the relationship between bubbles and Digital Territories as “a DT is formed from an aggregation of bubbles and is a bubble on its own”, hence rejecting the one-to-one overlap that was initially suggested. It is also found that “using the bubble metaphor may put limitations to the concept of DTs”, an approach that seems to be shared by most respondents (especially in combination with their replies to other questions), thus clearly pointing a separation from a one-to-one relationship”.

## Approximation of certain DT aspects

Based on the convention that a Digital Territory has a single individual (owner) at its centre and that a bubble is a mean for achieving public understanding to this scheme, we could identify several sections of human life that are bound to be most affected by it, and are, therefore, in need of immediate analysis.

The sector of privacy is obviously the first among them. The right to privacy, although disputed even today internationally, is obviously based upon the basic distinction between public and private spaces. Such spaces are mostly obvious to the real world: the home is evidently a private space, whereas the workplace or the common (city) spaces are most of the times considered public; consequently, all actions conducted within one of the above spaces is treated as public or private, thus signalling a right to privacy wherever applicable. Nevertheless, this distinction is not apparent in Aml spaces: given the digitisation of information, the boundaries between public and private are blurred in the digital environment. Aml spaces do not necessarily include notions such as “home”, “market” or “workplace”, because all actions are conducted in an abstract, non-present manner: information is digitised and circulated among virtual spaces, in order to perform a task. In other words, the separations of the real world into houses, government building, streets and shops, all distinguished through physical means (bricks and walls) is not present in the digital environment.

We therefore either will have to construct our Aml spaces in the same way as our real world (thus artificially introducing technical barriers and boundaries in the same way as walls exist in the real world), or we shall accept their non-bound nature and try to adapt to it. The transposition of the real world in Aml spaces (where, for instance, a Digital Residence shall indeed exist) is a task that is obviously self-evident to us and presents certain merits, the most important being the construction of a “viable” environment for the human being. Indeed, everybody would applaud the idea of constructing Digital Residences, Banks, Governments, Streets etc., because they could then live easier in the new environment.

On the other hand, if we impose upon the digital world notions of the real world, in order to

essentially better understand it, we risk losing important advantages that it offers. The lack of physical boundaries, the all-potent space and the freedom it offers are not assets to discard easily.

From this point of view, the process resembles the colonisation of a new world: we have a choice either to accept it as it is, and try to profit from it, or to impose our known schemes and patterns. Both methods, one of which has been tested in the real world as well, have their merits and their disadvantages.

From a public/private distinction, the line between public and private may be drawn either outside our Digital Residence, if we choose to transpose one in Aml spaces, or it can remain blurred and be redefined each time an individual acts in the digital world, depending on the method of progress we choose. In any event, we need to clarify in advance and in both models what shall constitute private and public in the new environment. Then we must define privacy, or “the right to be left alone”. Shall “alone” mean in the solitude of our home (as destined when it was first written back in 1896) or is it to mean “alone” in an endless space where an individual is idle and does not want to be disturbed (but perhaps does not object to being observed)?

A second domain that shall obviously be affected is human transactions. This time, Aml spaces must accommodate the individual’s need to interact with others; such interaction may either have a commercial context or a social one. In the first case, we shall need to define how and when transactions are realised. The internet and its expanding e-commerce provide useful guidance to this end: legislators chose to regulate the new market in the same way as any (international) market, they introduced known legal schemes (long-distance sales) and now profit from wide use of the new medium. Therefore, notions such as when a purchase is performed, where it is performed and what rights each of the seller and buyer has in the digital environment are already answered (in a more or less sufficient way). Aml spaces could profit from such know-how; the paradigm of transactions in the digital environment that follow the rules of the real world is already being tested. On the other hand, it should be pointed out that issues such as taxation or jurisdiction are not always satisfactorily resolved – from this point of view they



do seem to constitute the boundaries of the transposition of real-world economic and legal notions in the digital world.

Digital Territories therefore need to approximate the notions of transaction and, most importantly, interaction within Aml spaces. We need to establish how an individual interacts in the digital world, where and when this occurs (boundaries, bubbles), how it is perceivable by other individuals and what ways of interaction exist. The focus until today has been placed upon commercial applications only; Aml spaces need to turn their attention to everyday life as well, and to better define the “digital life” of an individual in Aml spaces as a whole.

## 12. Security and privacy concerns

Security and privacy concerns are associated with all categories of DTs, such as location based systems and services, virtual residencies and mobile phone networks. DTs and their components including the whole infrastructure they rely on are exhibited to security, privacy, identity and copyright related threats. These threats range from unauthorized information manipulation and disclosure (violations of personal or corporate data confidentiality), to forgery, denial of service, profiling, and piracy or cloning. In order to address this issue, suitable measures have to be taken which include organizational, procedural and technical measures, such as entity and data authentication, data and traffic confidentiality, authorization and access control, digital signatures, privacy and copyright protection.

The following subsections present security threats and measures, privacy threats and counter-measures, and identity management related issues.

### Security issues

The creation, collection, processing and communication of information are decisive factors in preserving human life quality in DTs. On the other hand, these factors may threaten security and privacy of individuals. Changes in the digital environment, where possibly dangerous devices or ICT components are installed and used have to be appropriately considered and addressed. Human or other entity hostile actions such as attacks on infor-

mation and communication infrastructures and the introduction of viruses or spy-ware constitute severe threats of our times, which are expected to be posed on future DTs. Information, knowledge based and surveillance systems have been developed to support managing digital environments, studying changes and tracking potentially threatening sources. However, similar technologies may be used to violate security and privacy.

### Vulnerabilities and threats

Components of DTs such as wireless network devices, bridges, sensors, software programs and storage systems may be physically damaged or purloined, thus breaching their availability. Also, the execution of malicious software may cause operational failures or system malfunctions (logic bombs, Trojan horses and viruses), and render the system vulnerable to possible attacks. Other threats include unauthorized use and breach of confidentiality. These threats can exploit vulnerabilities that exist in software, operating systems or data network configuration.

Further components of DTs, such as the networks, access control procedures and the personnel involved in their development, operation and maintenance, may be possible targets of malicious or unintentional actions. In particular, the Internet, being an open and dynamic system with respect to the topology and the technologies used, is extremely vulnerable to security, privacy and copyright related attacks. The vulnerabilities of computer networks result from the use of insecure sub-networks or segments, the sharing of communication channels, and the difficulty of securely identifying remote users. Getting around the access control procedures may also result to increased cost for using the computation and communication services, and to software and data destruction. Finally, employees may constitute a severe source of violation as relevant statistics show.

The possible security and copyright related threats might be classified, according to their implications, as follows:

- Unauthorised disclosure of communications' content or other sensitive data. This could be also in the context of corporate espionage activities, through remotely gathering supply chain data or individuals' preferences.



- Unauthorized access, alteration and deletion of sensitive and/or personal data.
- User impersonation (masquerading), aiming at unauthorized access to information systems resources and data.
- Denial of service, or breaching of availability of information system resources.
- Repudiation of the sending or receipt of messages, as well as the creation or alteration of data.
- Piracy or copyright violations, including illegal copy and distribution of digital work (or multimedia content).
- Traffic data analysis.

### Security and copyright protection

Security and privacy protection measures primarily aim at achieving the following characteristics: confidentiality, integrity and availability. Copyright protection measures aim at preventing illegal reproduction and distribution of digital works. To cope with the above-mentioned threats and vulnerabilities, at least the following security and copyright protection measures should be taken: identification & authentication systems and procedures, copyright protection, authorization and access control systems and procedures, and use of encryption in communication (e.g. digital signatures). These measures are discussed in the following.

Prior to data communication, peer entities mutually authenticate themselves. This is necessary because entity identities are recorded for accounting or auditing purposes and most times taken into account in decisions about access control. During the authentication process, peer entities demonstrate to each other the possession of authentication tokens, which may be passwords in the case of simple mechanisms or secret keys in the case of stronger mechanisms. To prevent unauthorized data disclosure, data encryption is applied, when data confidentiality is required. Due to performance limitations, symmetric cryptographic systems are currently preferred for this purpose.

To enable the detection of copyright violations of digital works, such as images, watermarking or fingerprinting techniques are applied. These techniques are robust and tampering resistant, and

allow the secure insertion of copyright management information in multimedia content or digital works.

DTs have to include authorization processes associated with controlling access to servers and the various assets of the whole processing and communication infrastructure. The discretionary concepts are suitable for owner-based authorization and access control, i.e., the asset owners are responsible for assigning the user permissions (e.g., read, right, execute, delete, change permission and change ownership), according to a system-wide policy. Also mandatory or role-based concepts are well suited for DTs, since they allow the realization of a system-wide access control policy.

Secure DTs should support the protection of data integrity. This means that the data cannot be modified when communicated or stored by unauthorized entities without detection. Integrity protection may be combined with data encryption, if a cryptographic system is applied in an appropriate operation mode. Secure DTs should also provide functions that ensure that the identification of the origin of any particular communication or data creation or alteration cannot be masked.

In addition to the above-mentioned technical measures, organizational-administrational measures should also be applied. These refer to security, privacy and copyright protection management, risk analysis and management, development of security, privacy and copyright policy, and disaster recovery and contingency plans. They describe the actions that the involved persons, from management and system administrators to owners, service receivers and mere users, have to perform. Specifically, security, privacy and copyright policies include related requirements and needed actions to implement them. Disaster recovery and contingency plans include measures to be applied in an emergency. There exist appropriate secure software engineering models that software programs, either obtained or developed in-house should comply to. The information security concept encompasses the specification, design, coding and testing of systems, so that security measures are built-in and not developed as add-ons or software patches, so that systems can operate robustly in spite of intrusions.

The establishment of policies and plans has to take under consideration the related legislation

being in force. At European Union and national level, there are Directives and laws which rule the conditions to create and use personal data and to copy and distribute digital works.

### Technologies and standards

Cryptographic techniques, information hiding techniques, public key infrastructures, virtual private networks, privacy-enhancing technologies, firewalls, monitoring and security analysis tools and security intelligent agents belong to technologies that comprise the basis for realizing secure DTs.

The basic building elements of most of security and privacy protection measures are cryptographic techniques, including both symmetric and asymmetric cryptographic algorithms such as 3-DES, IDEA, AES, RSA and ECCs, digital signature schemes and one-way hash functions. Digital signature schemes, which are primarily asymmetric cryptographic techniques, can be used to provide entity and data origin authentication, data integrity and non-repudiation services. According to related standards, there are two types of digital signatures: one uses mechanisms with message recovery and the other mechanisms with appendix. Asymmetric cryptography requires a public key infrastructure to exist, so that the associated algorithms can be proven and accepted to be used in global information commerce environments. Participants in this structure, such as Certification Authorities, provide their services in a trustworthy (tamper-resistant) environment.

Regarding information hiding techniques, watermarks and fingerprints may be used, in some cases in combination with digital signatures, for the realization of copyright protection. A large variety of watermarking techniques has been proposed in the literature, which are appropriate to address several application requirements, including data authentication and ownership identification. Features that are commonly required by different applications include robustness, tampering resistance and low error probability. Application-dependent requirements include unperceivability, invertibility, non-(quasi-) invertibility, watermark entropy and extraction speed. Watermarking techniques may be classified, from the point of view of detection, into blind or non-blind, private or public and readable

or detectable. Blind watermarks, as opposed to non-blind watermarks, do not rely (for reading or detection) on the comparison of the original (non-marked) digital work (image or text or audio). Private watermarks allow only authorized users to detect them. In this case, the knowledge of some secret information is needed. In contrast, public watermarks allow anyone to read them. Especially, the public or private nature of the watermark significantly affects the way it can be applied in application domains with contradictory functional requirements. Readable watermarks are the public ones, which allow anyone to read the marks. On the other hand, detectable (private) watermarks permit only the authorized users to check if given marks are present or not.

Public key infrastructures consisting of certification authorities (or service providers) mainly issue certificates binding an individual's public key to their credentials, i.e. to provide public keys' authenticity. Certification authorities verify these credentials and sign (compute their signatures) the certificates. Public key infrastructures enable the wide development of e-commerce applications, based on asymmetric cryptographic systems and digital signature schemes. The certification authenticity is proved by means of authentication mechanisms (signature verification), based also on asymmetric cryptographic algorithms.

The primary function of virtual private networks (VPN) is to protect the data from disclosure during transmission over any network paths. This protection allows the use of public networks to secure information exchange. Though there are some differences between the available VPN product solutions, they should provide confidentiality, integrity and non-repudiation. Internet may be used as the public network infrastructure.

Monitoring, vulnerability analysis and intrusion detection tools enable the recording / monitoring of actions especially in critical systems, determining weaknesses and detecting unauthorized system activities. Firewalls control the incoming and outgoing network traffic, in accordance with the security policy. Further technologies such as intelligent agents, risk management tools, anti-virus software and physical security mechanisms may be required to effectively implement security, privacy and copyright protection measures.

Security standardization has been carried out by a number of different standardization organizations, including efforts to harmonize the results of this work. Of particular note are IEEE, ITU-T, ISO, IETF, ETSI and CEN, and also national bodies such as NIST, BSI and DIN. Security systems and privacy protection techniques have reached a mature phase and several standards have emerged.<sup>98</sup> This has not been achieved yet for watermarking systems.

## Privacy issues

When it comes to DTs, we want to protect the right to privacy. However, privacy is a social value and has different cultural interpretations. We need to enable each person to define his/her own preferences of what should be protected, because these may differ very much. Privacy should be considered as a sphere of activities not necessary dependent on a specific space. The permeability of the sphere may weaken as a result of regulations, activities, context etc.

Usually we manage our privacy by controlling distance with each other. We exchange more information with our immediate neighbors than with more distant entities. Enabling people to apply the same distance management processes in Aml spaces, as they do in the real world, is a research issue.

People tend to give away personal data (i.e. loud conversations, bonus revenue cards etc) for very little return. For most data or circumstance, people usually don't mind. However, their concern increases sharply after some point (which depends on context). It is difficult to locate this point and not overcome it. An example is reluctance to give biometric information, although they don't mind giving away other pieces of information. It is a question of finding the right balance.

## Privacy threats

Digital traces are left after performing activities within a DT. Thus, interaction produces traces, which are not under direct control or perception by the participants. Though enjoying benefiting

from access to content and receiving of personalized, efficient and convenient services, most individuals are aware and concerned about possible privacy violations, as the collection and diffusion of personal information, such as their preferences or beliefs and state of health and wealth. Privacy related violations may be classified as follows:

- The communications of citizens including traffic data may be disclosed without complying with the relevant procedures being in effect.
- Family life violation or home intrusions may be facilitated due to virtually extended homes and removal of home boundaries.
- Monitoring or surveillance may be enabled or facilitated by using bridges between physical and digital space. Also the location may be inferred by monitoring individuals as they act within DTs.
- Identity theft may result from disclosure of related information and associated authentication credentials and may aim at conducting fraudulent actions.
- Spam or unsolicited electronic communication may result from misusing contact information disclosed to illegally acting entities.
- Profiling is possible through recording and analyzing individual actions, transactions, choices, communications, publications, preferences, beliefs, etc.
- Loss of control in the distribution of an individual's personal information is also possible if disclosed to unethically or illegally acting entities, i.e. individuals lose control over which information or identity to use in specific environments or circumstances.
- Also when there is no association between disclosed and collected information to a concrete individual, an "informational shroud" is created around a person, whose identity may be revealed later on.
- Remaining pieces of information associated with actions conducted in the physical or digital world, which have been recorded by

<sup>98</sup> At <http://www.infosyssec.net/infosyssec/> there are links to information related to almost all security standards. General information on IEEE, IETF, ISO and ITU-T standards is available at <http://standards.ieee.org/>, **A Special Case – The Virtual Residence**

components of DTs and are retained without being controlled by the individual they refer to, may give rise to severe privacy violations.

For instance, regarding RFIDs, privacy threats arise from the fact that tags with unique identifiers can be associated with a person's identity. Related threats stated in the literature refer to actions (an individual's behavior may be inferred by monitoring the actions of tags as for instance their disappearance), locations (individuals carrying unique tags can be monitored and their location revealed if their association is known to the monitoring entity), preferences (tags on consumer goods usually identify the product manufacturer, the product type, and the item's unique identity), associations (not only product classes but also identities or serial numbers of specific items are associated with customers as opposed to current practices), shadow or constellation (also when there is no association with an individual's identity, tags may shadow or create a constellation around a person), transaction (when tagged objects move from one shadow or constellation to another, it is easy to infer a transaction between the corresponding persons), and breadcrumb (though consumers may have discarded acquired items, associated information may be retained in corporate information systems, which could be revealed in case of subsequent malicious or criminal acts).

### Privacy protection

There is an international consensus on the principles that must be taken into account in handling information and communications of individuals, which are reflected in codes of ethics or specific relevant legislation. These are as follows:

- A privacy policy should be developed and managed, addressing the proper handling of personal data, consistent with data protection principles and practices and the choices made by individuals they refer to.
- Reasonable security safeguards should be adopted by data controllers to adequately protect personal data in their custody against risks, such as loss or unauthorized access, destruction, use, modification or disclosure of data. Security involves both technical and organizational measures. Active technical measures include authentication, access control mechanisms and accountability, and passive measures include integrity, cryptographic support, anonymity, pseudonymity, unlinkability and unobservability. Organizational measures include security and privacy protection planning and strategy, security and privacy policy creation and maintenance and disaster recovery and business continuity planning.
- Personal communications and related traffic data are confidential, and only for very specific purposes and under strict procedures is their secrecy level lowered, so that they become accessible.
- The collection of personal data should be limited only to the necessary for the fulfillment of a specified purpose. Personal data should be collected by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject
- The purposes for the collection of personal data should be identified not later than the time of data collection. Subsequent use of the data should be limited to the fulfillment of those purposes and not be further processed in ways incompatible with those purposes.
- Personal data should be adequate, relevant and not excessive in relation to the purposes for which they are collected and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. To assure data integrity, data controllers must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form
- Personal data should not be used or disclosed for purposes other than those specified according to the purpose specification principle, except with the consent of the data subject or as required by law.
- Individuals must be informed about the collection of their personal data (i.e. regarding when the data is collected, where it is stored and for how long, where it is transmitted and why, etc).
- A legitimate ground for the processing of personal data is the unambiguously given consent of the data subject. Data controllers should provide data subjects with the oppor-



tunity to give or deny consent for the collection and processing of their personal data.

- An individual has the right to access personal data relating to him or her and receive, in an intelligible form within a reasonable time and manner, the relevant personal data, a description of the purpose or purposes of processing, the recipients or categories of recipients and the available information as to the source of the data. If a request of access is denied, an individual should be given reasons for the denial and be able to challenge it. Also the individual must be given the right to challenge the use of data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
- Information concerning development, practices and policies relating to the management of personal data should be made readily accessible to individuals.
- Processors of personal information should be accountable for complying with privacy principles and practices. They should provide means to address improper handling or misuse of personal data. Services and mechanisms should be implemented to ensure that processing of personal data is done according to relevant laws and the choices of individuals they refer to. Auditable controls should be in place to ensure compliance with legislation being in force.
- The use of a reliable mechanism to impose sanctions for noncompliance with privacy practices and principles. The principles of privacy protection can only be effective if there is a mechanism in place to enforce them. The data controller should provide data subject with a means to report alleged violations of privacy policy to judicial authorities and also to provide access to regulatory authorities to audit services.

The above mentioned privacy protection principles may be translated into requirements posed on DTs as stated in the following [ISO/IEC 20886]:

- Privacy policy refers to the set of rules related to the generation, collection, processing and usage/exploitation of personal data, taking under consideration relevant legislation on data protection.

- Certification refers to the management and validation of credentials of entities involved in processing personal information.
- Audit refers to recording and maintenance of events data necessary to ensure law or policy compliance.
- Access control refers to functions needed to ensure that data processing complies with policies, law and regulations being in force, also including necessary corrections or updates of personal data.
- Enforcement handles redress when a data collection entity is not in conformance with the terms and policies of an agreement and any applicable regulations.
- Interaction refers to the interface with an individual or their proxies, i.e. presents proposed agreements from an information collection entity to an individual, receives information, preferences and actions, confirms actions and manages data movement.
- Negotiation handles arbitration between a data collection entity and a data subject.
- Validation checks for accurate, complete and timely personal data (data quality).

Cryptography, passwords, and especially pseudonyms are considered as very promising measures against many of the above mentioned privacy threats. However, there are certain limitations. For instance, cost is the main obstacle to use cryptography in RFID technology, and for using passwords in some environments, the identities of the components are needed.

Though encryption may provide some protection against privacy violations in electronic communications, it cannot be adequate, since traffic data such as sender's and receiver's identities or source and destination addresses, time of the communication and the information volume exchanged are still exposed to interception. Privacy protection may be achieved with support by privacy service providers, such as MIX-Networks, and / or by means of techniques based on anonymity or pseudonyms.

Privacy enhancing technologies are so designed that possibly less personal data is used, under the control of data subjects and for the specified processing purposes. Anonymity tech-



niques are the most effective means to achieve privacy protection. Also, pseudonyms are often used.

## Identity management

As mentioned above, identity theft is a privacy related threat which may result in fraudulent actions against individuals. We may differentiate between real identities, i.e. information used for the real identification of an individual, and on-line (digital) identities, i.e. real identities or partial information or pseudonyms used by individual entities or their proxies in their interactions in different digital territories. Examples of partial identities are driver's license number, frequent flier number, home phone number, credit card number, health registration number, e-mail addresses, cookies etc.

On the other hand, we may differentiate between on-line and off-line identities. Then, examples of on-line identities are usernames, pseudonyms, e-mail addresses, cookies, etc., and of off-line identities, a driver's license number, frequent flier number, home phone number, credit card number and health registration number. However, off-line identities may also be used as on-line identities.

Identity management is of crucial importance in deploying and operating DTs since their acceptance and usefulness will depend on building and maintaining trust relationships between all involved entities.

There are at least the following three requirements stated in the literature, regarding identity management:

- Reliability and dependability. A digital identity must protect users against forgery and related attacks while guarantee to other entities that users can meet transaction related obligations.
- Controlled information disclosure. Users must have control over which identity to use in specific circumstances, as well as over its secondary use and the possible replication of any identity information revealed in a transaction.
- Mobility support. Mobile computing infrastructure and components of DTs must be able to apply multiple and dependable digital identities, i.e. to remove technical limits that

do not allow applying such identity management solutions.

Multiple and dependable digital identities could be based on public key infrastructure and trusted third parties. Current schemes such as Liberty Alliance, Microsoft .Net passport and Novell DigitalMe satisfy some of the above requirements but lack satisfying dependability requirements. There are a number of issues related to identity management, such as lifecycle management, representation formats, cross-domain communication, anonymity support, trust management, controlled dissemination, architectural patterns and administration.

## Conclusions related to research and policy

Location technologies introduce new challenges with respect to privacy policy and law. Regarding identity management, appropriate schemes or techniques are needed for identity administration, anonymity support and dependability, pseudonym linkage prevention, trust models and evaluation methodologies.

Fundamental research of alternative cryptographic algorithms (i.e. factoring asymmetric algorithms, quantum computing, etc) is needed to overcome the vulnerabilities of existing ones.

## The role and position of law enforcement

Law enforcement in the digital context has, until now, taken two forms: first the form of Data Protection Acts, aiming at the protection of privacy in the information technology environment, and, second, crime prosecution in the digital environment.

As far as data protection is concerned, the current scheme includes a registration system and an independent state Authority to monitor all personal information processing within a single country. This system dates back to the 1960s, when it was deemed possible to register and control all processing of personal data; because of low proliferation of desktop computing, this scheme was adequate at the time. Nevertheless, after forty years of continuous information technology progress, this scheme appears already outdated; registration requirements have been brought down to registering only large-scale processing, leaving thus rou-

tine processing outside the scope of the law. Additionally, national Data Protection Authorities find it increasingly difficult to fulfil their tasks in a networked environment. To this end, international co-operation among several data protection authorities is aimed, with the purpose of resolving newly arisen challenges in a more efficient way.

The emergence of Digital Territories may further blur the scope of Data Protection Acts. In their original perception they were aimed at assisting the individual in real-world automated processing of his/her personal data. Nowadays, they are faced with the increasing problems of the networks environment, but still their point of reference remains the real-world individual and the processing of personal information in the real-world. It is to this end that monitoring and regulative measures have been implemented and applied. Nevertheless, this scheme shall be further challenged by Digital Territories. In an environment where by definition personal information shall be digitised, there is simply no place for a mechanism of registration of all processing of personal information.

On the other hand, the principles of Data Protection may indeed continue to apply. The “fair and lawful” processing principle or the principle of finality indeed retain their value even in Aml spaces. Regardless of the digitisation of information, it remains clear that processing must be done in a “fair and lawful” way. Additionally, the digitisation must include information that remains updated, is valid, close to the scope of digitisation and is being digitised and used for given purposes and for a given period of time. From a different perspective, the individual must indeed continue to give his/her consent each time for his/her personal data to be processed. Individuals should continue to have the right to know when their personal data are being processed, to be thus able to object to the processing or to request an amendment or deletion of their data.

Consequently, both the principles and the fundamental rights awarded to individuals by data protection laws appear to remain valid even in Aml spaces. Digital Territories shall not affect the right of individuals to have their personal information processed in a fair and lawful way. Perhaps the controlling and monitoring mechanisms will have to change: Data Protection Authorities may

have to change the way they work in Aml spaces in the future.

On the other hand, crime prosecution in the digital environment is a totally different issue. As long as new fields of human activity are constantly being discovered, crime opportunities shall also arise and prosecution mechanisms will need to keep up. The internet has already added several crimes and prosecution policies to contemporary crime prevention strategies. Identity theft, fraud, child pornography and other crimes have appeared in the digital environment; new policing and prosecution strategies are already in place for the protection of our society against them.

Digital Territories shall unavoidably add opportunities for new forms of crime in the future, exactly as any new medium and form of human activity has done in the past. The enactment of individuals in Aml spaces shall create new ethics, ways of behaviour, means of communication, rules and regulations, and all of them are bound to be broken and usurped by individuals seeking to make profit in an illegal way. Crime prevention and prosecution shall inevitably follow, and keep up with developments. Bearing this, however, in mind, it becomes even more important to try and draw analogies between the real world and Aml spaces: only in this way shall public trust be vested upon new Aml spaces. Also, because patterns of behaviour relate to real-world situations, legislation schemes will be able cope to better and more efficiently with crimes and issues that may arise in the Aml environment.

### 13. Mobility of citizens

#### **People-related aspects, continuity of tasks across heterogeneous spaces, privacy, mobility, adaptation**

The term mobility could be described well by the term: ‘accessibility everywhere’. Mobility requires a system that retains some form of continuity throughout journeys. Within this context, applications have to adapt to context. DT systems that support mobility should be adaptable and changeable. Change and alteration over time should be considered in the design of the DT.

Handling mobility / adaptation / change implies that one has effectively tackled the issue of security. For instance, a mobile phone user located in a single place covered by the base stations of his/her mobile phone company would, ideally, rely on the security of the company. When, however, the user moves to another country, he/she should, also, have protection mechanisms of his/her own or, at least, he could use those of the mobile company that he subscribes to. Thus, mobility involves dangers and the effective handling of these dangers is a crucial issue. Then one would be willing to distribute himself/herself outside his/her DT and this distribution is central to the nature of artificial communities as containing interacting entities.

In order to avoid the dependence on externally provided security mechanisms it is important to rely on Intrusion Detection Systems (IDS), which should be an integral part of any DT. IDS technology has devised ways to determine whether an ongoing attack is taking place, using data stemming from the DT under protection as well as neighboring DTs. Also, special evolution algorithms may predict the front of the attack using a set up of discrete differential equations.

An important issue here is that of interoperability. If DTs end up having an implementation of IDs akin to mobile telephony or conventional PKIs, then there would be several interoperability issues to solve (e.g. PKIs located in different countries are very difficult - technologically and legally - to interface with each other). It would be much better, perhaps, to have a DT centered security architecture relying on something much more transnational than traditional PKIs, say satellite technology – even using current GPS technology as a carrier of DT related information).

Mobility/adaptation/change themselves, as applied to the notion of a DT, can both be sensed and realised. Mobility can be sensed in relation to nearby points of reference but can also be achieved as a DT moves in space. Adaptation, as goal-directed change, can be sensed by nearby DTs who sense another DT's desire for change, but can also be realized by an internal change of states (generated, in turn, by some external event) in a DT. Finally, change can be sensed as a state transition of a DT (e.g. movement in space or internal state transition), but can also be induced on nearby DTs by another DT (e.g. by generating a certain set of rules).

These three concepts may also have a cause-effect relationship. For instance, adaptation (to a new set of goals) may cause mobility (to achieve the goals). Also, change (of internal state of a DT) may cause mobility (as a reaction to this change). As another example, mobility can cause adaptation and/or change to nearby DTs. Thus the three concepts act complementarily and usually appear in conjunction with one another.

The technological factors that are involved in the concepts of mobility/adaptation/change range from proximity/movement/orientation sensors and feedback electronic circuits to complex finite state machines, complex decision support mechanisms (either machine or human based) and mechanical actuators (a DT may be either machine or human governed).

Mobility/adaptation/change can be thought of as the way in which single DTs can formulate common goals and activate executions of plans to achieve these goals. This collective function increases the significance of security and privacy intrusion detection as discussed above, since the DTs have to allocate part of their communication to the problem of collectively sense whether the community is under attack.

Factors that affect adaptation include:

- Physical factors (Environmental, Cultural etc), including goals of the environment, goals of the individual, stability, coupling, etc.
- Digital factors: combinations or superimpositions of data; application of data in unanticipated context.
- Ease of replication: How easy it is to use a tool to replicate a process or develop the same service.
- Gain: what's the gain from adaptation?
- The dynamic of standard or regulatory framework, ID sensors.
- Change in one's goals:
  - Inability to sustain current state successfully
  - Desire to extend identity to a different environment
  - Change in external circumstances
  - The more open the system, the easier it can adapt

- Adoption of organic models
- Profit, Sense of belonging / Community spirit, Cultural / ideological changes

Regarding the ability and extent to which change should be perceivable, there can be many responses:

- The perception of change must be either: 1. not perceptible to all (people experimenting); 2. Perceptible to all (outcome of the experimentation).
- Community change will always have pros and cons for different number of beings in the DT. More conservative ones want to prevent change, where new users and “free thinkers” welcome change. Depending on the community it is necessary to visualize or communicate change as based on the member’s collective development and opinions.
- Only relevant elements should be noticeable for the well being of the user.
- It really depends on what these changes affect... Intentions, power structures and surveillance models ought to be perceivable as to make participants aware of the power distribution. Complete transparency entails loss of control.

An important issue in question is that of *Trust*. Mobility within DTs depends on the level of trust one has of those DTs visited. The DT owner of the visited location provides access privileges according to the level of trust they have of the visitor. We can say that the access level is defined by people’s trust. Therefore the level of privacy (s)he wants to adopt is varied, according to the nature of the relationship to the DT. Privacy levels can be varying at different visits over time, as living in DT and relationships between DTs evolves over time.

Mobility has thus two different viewing angles: mobility between different DTs and mobility between different privacy / access levels in these DTs (resulting from changes over time in people’s trust).

### Technologies involved to support or breach privacy

Since mobility of an entity involves secure communication with other entities as well as ro-

bustness against attack efforts coming from other malicious entities, it is important to establish methods for the support of secure exchange of information between entities in a, possibly, hostile environment with threats against secure communication.

In this chapter, we explain the fundamentals of the most widely used cryptographic primitives for the support of secure communication. Our approach describes the basic characteristics of the techniques and avoids technical details, giving references for more details if necessary.

Mobility thus needs to be achieved in the following:

- between DTs,
- within a DT between different levels.

Adaptation and change are inherent in the system model of DT. Mobility can be considered as a fixed environment with a changeable timeline and borders. Mobility requires a system that:

- retains continuity throughout journeys,
- facilitates identification, accessibility, rights and privacy management, compatibility (e.g. resonant types across all forms), archiving,
- is dynamic (time), highly adaptable and fluid (changeable).

An issue not addressed in mobility, is that of leaving traces that are perceptible and visible to other DT residents.

### Special methods for mobile security

A mobile ad hoc network is a self-organising, autonomous system of wireless nodes which move around freely giving an unpredictable and changeable nature to the network topology. Security is a key concern in mobile ad hoc networks due to the impromptu membership of nodes, which raises trust issues amongst them. The use of wireless links also poses a major security matter in that there is less effort involved in compromising them than wired links. The aforementioned, coupled with computational and energy constraints of the devices which comprise a mobile ad hoc network, render the achievement of security a difficult problem.

Vital issues of security, such as authentication, integrity and confidentiality are dealt with using a



symmetric key scheme; however the lack of a superior key management framework renders the whole security of the system ineffective since attacks are made on the key management infrastructure of a system.

## 14. Suggestions for raising awareness

Raising awareness on the concept of DT is a major objective of the study. To this effect, from the beginning an interaction with individuals, communities, networks, and domain experts was achieved mainly through the study's tools (i.e. interviews, forum, etc). Discussions in mailing lists and other web forums by the core team experts, as well as the validation workshop were also used to serve this purpose.

The core experts consider raising awareness as an on-going activity. More specifically:

- Follow-up activities to elaborate on specific DT concepts will be pursued by organizing special workshops and sessions in conferences and events; At least one such workshop will be organized within 2006, in the context of the 2<sup>nd</sup> IEE Conference on Intelligent Environments that will take place in Athens on July 5-6 2006;
- Promotion and raising awareness on DT and study outcomes will also be done via the CONVIVIO web-zine ([www.convivionet.net](http://www.convivionet.net)), where one of the core team members, Dr. Achilles Kameas, serves as Editor-in-chief. Specifically, a special peer-reviewed section is planned for 2007 on topics related to DT;
- Articles will be published by the core expert team to various scientific journals and publications;
- Synergies with other projects and studies that were implemented by IPTS/ IST Unit will be pursued in order to create follow up projects under the same concept and scope;
- Workshops and seminars can be organized in central European cities (e.g. Brussels, Athens, etc.) promoting the results of the study. As the current and coming years are going to be very important for RFID development and the privacy and security issues

for the European Union are critical and considered as emerging, the DT concept could serve to bring all parties together to discuss concrete scenarios.

(<http://www.physorg.com/news9221.html>);

- The study will be presented in the SWAMI study Conference to be organized in Brussels on the 21st and 22nd of March 2006 by two members of the core team of the DT study. (Rob van Kranenburg & Achilles Kameas) <http://swami.jrc.es/pages/index.htm>.

## 15. Conclusions

This first study on the Digital Territories has showed that it is a valid metaphor, capable of supporting powerful concepts and analysis tools. The study has succeeded in promoting understanding of the DT concepts. Some of its key findings are:

- A DT is an ephemeral Aml space: it is created for a specific purpose and integrates the will of the owner (an individual or group operator) with the means to achieve it (including infrastructure, properties, services and objects) within an Aml space.
- Two illustrative examples of DTs are the home and the park. The home is a private place created to protect the individual and the family. In the Aml vision, home becomes a Virtual Residence, which offers its inhabitants services that relate to data management and protection, entertainment, privacy and trust, etc. The park is a conceptualization of a public Aml space, within which private transactions may take place. Services include entertainment, negotiation, relationships, identity building and creating a "local" or "national" shared identity.
- DT should always have a recognized owner and a purpose. Identity is the core property of DTs and is marked or discerned much in the same way as this happens in physical territories. It generally reflects the identity of the owners or inhabitants. The owner of a DT can be a single person, a group, or an agent. The responsibility share should be defined by a set of "laws" on which there is consent from all parties.



- While boundaries are often recognised both socially and legally in the physical world, the digital environment clearly lacks such a definition of borders. As a result, any abuse or violation of these borders would not even be noticed.
- Digital objects tend to leave traces in every territory they have been to: data not properly erased, state information, registry entries, timestamps on servers etc. Thus, in Aml applications an important consideration should be that of security, during the entire life cycle of the development process.
- DTs and their components including the whole infrastructure they rely on are exposed to security, privacy, identity and copyright related threats. These threats range from unauthorized information manipulation and disclosure (violations of personal or corporate confidentiality), to forgery, denial of service, profiling, and piracy or cloning. To cope with, suitable measures have to be taken which include organizational, procedural and technical measures, such as entity and data authentication, data and network traffic confidentiality, authorization and access control, digital signatures, privacy and copyright protection.
- Study of the legal framework with concern to DTs and bubbles must necessarily follow the clarification of open definition issues. The problem with Aml is that notions that are apparent and self-evident in the real world need to be re-defined, in a way that shall bring general consensus. A regulatory framework is needed. Consequently research should concentrate on two topics: first, definition of the fundamental notions in the digital environment, and, then, elaboration of certain legal issues pertaining to them.
- Towards the realisation of DT, key technologies need to progress and technological challenges and bottlenecks need to be addressed. These include technologies for location-based services, mobile devices, wireless networks, sensors and actuators, RFID tags, wearable computers, bio-implants, etc.

## 16. References

1. Michelle Addington, Daniel Shodek, *Smart Materials and New Technologies*, Elsevier / Architectural Press, Oxford, 2005.
2. Article 29 Data Protection Working Group, 'Working Document on Data Protection Issues Related to RFID Technology', January 19, 2005.
3. Michael Atighetchi et al., "Adaptive Cyberdefense for Survival and Intrusion Tolerance", *IEEE Internet Computing*, Vol. 8, No 6, pp. 25-33, 2004.
4. Algirdas Avizienis et al., "Basic Concepts and Taxonomy of Dependable and Secure Computing", *IEEE Transactions on Dependable and Secure Computing*, Vol. 1, No. 1, pp. 11-33, 2004.
5. David E. Bakken et al., "Data Obfuscation: Providing Anonymity and Desensitization of Usable Data Sets", *IEEE Security & Privacy*, Vol. 2, No 6, pp. 34-41, 2004.
6. Reyner Banham, "A Home is not a House", *Art in America*, April 1965, p. 70-79.
7. L. Barkhaus and A. Dey, "Location-Based Services for Mobile Telephony: A Study of User's Privacy Concerns", in *Proc. INTERACT, 9th IFIP TC13 International Conference on Human-Computer Interaction*, 2003.
8. C. Becker, G. Schiele, H. Gubbels, and K. Roethermel, "BASE - A Micro-broker-based Middleware For Pervasive Computing", in *Proc 1st IEEE Inter. Conf. on Pervasive Computing and Communications (PerCom03)*, Fort Worth, Texas, March 2003, pp. 443-451.
9. Walter Benjamin, *Reflexions: Essays, Aphorisms, Autobiographical Writings*, Schocken Books, 1978.
10. M. Chalmers, "Theory and Practice in the City Project, Theory and Practice in the City Project", in *Proc Conference for Content Integrated Research in Creative User Systems (CIRCUS 2001)*, Glasgow, September 2001
11. C-F Chan, E. S. Rogers Sr., "Distributed Symmetric Key Management for Mobile Ad hoc Networks", *INFOCOM 2004. 23rd Annual Conference of the IEEE Computer and Com-*

- munications Societies, Vol. 4, 7-11 March, 2004. pp. 2414-2424.
12. H. Chan, A. Perrig, D. Song, "Random Key Predistribution Schemes for Sensor Networks", in Proc the IEE Symposium of Privacy and Security", 11-14 May, 2003, pp.197-213.
  13. E. Christopoulou, and A. Kameas, "GAS Ontology: an ontology for collaboration among ubiquitous computing devices", International Journal of Human-Computer Studies (special issue on Protégé), Academic Press, vol. 62 no. 5, pp. 664-685, May 2005.
  14. E. Damiani, S. De Capitani di Vimercati, P. Samarati, "Managing Multiple and Dependable Identities", IEEE Internet Computing, Nov.-Dec. 2003, pp. 29-37.
  15. B. DeCleene, L. Dondeti, S. Griffin, T. Hardhonio, D.; Kiwior, J. Kurose, D. Towsley, S. Vasudevan, C. Zhang, "Secure Group Communication for Wireless Networks", Military Communications Conference (MILCOM) 2001. Network-Centric Operations: Creating the Information Force. IEEE. Vol. 1, 28-31 Oct. 2001, pp. 113-117.
  16. W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. 22, Issue 6. November 1976, pp. 644-654.
  17. W.K. Edwards, M.W. Newman, J. Sedivy, T. Smith, S. Izadi, "Challenge: Recombinant Computing and the Speakeasy Approach", in Proc. 8th Annual Inter. Conf. on Mobile Computing and Networking (MobiCom 2002), ACM Press, New York September 2002, pp. 279-286.
  18. L. Eschenauer, V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks", in Proc the 9th ACM Conference on Computer and Communication Security, November 2002, pp. 41-47.
  19. European Group on Ethics in Science and New Technology, 'Ethical Aspects of ICT Implants in the Human Boody', 2005.
  20. European Group on Ethics in Science and New Technology, 'Citizens Rights and New Technologies: A European Challenge', 2000.
  21. Simson L. Garfinkel, Ari Juels, Ravi Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions", IEEE Security & Privacy Magazine, Vol. 3, No 3, 2005, pp. 34-43.
  22. D. Garlan, D. P. Siewiorek, A. Smailagic, and P. Steenkistie, "Project Aura: Toward Distraction-Free Pervasive Computing", IEEE Pervasive Computing, vol. 1 no. 2, April-June 2002, pp. 22-31.
  23. H. Harney, C. Muchenhirn, "Group Key Management Protocol (GKMP) Specification", Internet Engineering Task Force – Network Working Group, Request for Comment No. 2093, July 1997.
  24. Martin Heidegger, "The Thing", in Heidegger, Poetry, Language, Thought, Harper & Row, 1975.
  25. L.E. Holmquist, et al., "Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart artefacts", in Proc UBIComp 2001, Atlanta, GA, September 2001, pp. 116-122.
  26. J. Humble, et al., "Playing with the Bits – User-Configuration of Ubiquitous Domestic Environments", in Proc the 5th Annual Conference on Ubiquitous Computing (UBICOMP 2003), Springer-Verlag, Seattle, Washington, October 2003, pp. 256-263
  27. B. Johanson, A. Fox, and T. Winograd, "Experiences with Ubiquitous Computing Rooms", IEEE Pervasive Computing, vol. 1 no.2, April-June 2002, pp. 67-74.
  28. Iris A. Junglas, Cristiane Spitzmueller, "A Research Model for Studying Privacy Concerns Pertaining to Location Based Services", in Proc the 38th Hawaii International Conference on System Sciences, 2005.
  29. Nikolas Kalogeras, Man + Habitat, Athens, 1979.
  30. Kameas, et al., "An Architecture that Treats Everyday Objects as Communicating Tangible Components", in Proc. 1st IEEE Inter. Conf. on Pervasive Computing and Communications (PerCom03), Fort Worth, Texas, March 2003, pp. 115-122.

31. Guenter Karjoth, Paul A. Moskowitz, "Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced" in Proc. ACM WPES'05, 2005, Alexandria, Virginia, USA.
32. Y. Kim, A. Perrig, G. Tsudik, "Communication-Efficient Group Key Agreement", IFIP SEC 2001, June 2001.
33. T. Kindberg and J. Barton, "The Cooltown User Experience", Tech. Rep. HPL-2001-22, HP Labs, Feb 2001.
34. Spiro Kostof, A History of Architecture, Settings and Rituals, Oxford University Press, 1985.
35. Neil Leach, David Turnbull, Chris Williams, Digital Tectonics, Willey – Academy, 2004.
36. B. Lehane, Ad Hoc Key Management, PhD Thesis, Department of Electronic and Electrical Engineering, Trinity College Dublin, 2004.
37. Thomas Leslie, "Capsule / Gantry: The New Domestic Archetypes in the Architecture of the 1960's", Universal Versus Individual, international Conference, Finland, 2002.
38. I. Mavrommati, A. Kameas, and P. Markopoulos, "An editing tool that manages the device associations", Personal and Ubiquitous Computing J., ACM, Springer-Verlag London Ltd., vol. 8 no. 3-4, pp. 255-263, May 2004.
39. I. Mavrommati, P. Markopoulos, J. Calemis and A. Kameas, "Experiencing Extrovert Gadgets", in Proc. BCS HCI, Johnson, H., Gray, P. and O'Neil, E. (Eds), vol. 2, Research Press International, 2003, pp. 179-182.
40. I. Mavrommati, A. Kameas and P. Markopoulos, "Visibility and accessibility of a component-based approach for Ubiquitous Computing applications", in Proc. HCI International, Stephanidis, C. & Jacko, J., (Eds), Vol. III, Human Computer Interaction, Theory and Practice, Lawrence Erlbaum and Associates, 2003, pp. 178-182.
41. Malcom McCullough, Digital Ground, Architecture, Pervasive Computer and Environmental Knowledge, MIT, 2004.
42. D. A. McGrew, A. T. Sherman, "Key Establishment in Large Dynamic Groups Using One-Way Function Trees", IEEE Transactions on Software Engineering, Vol. 29, Issue 5, May 2003, pp. 444-458.
43. R. P. Minch, "Privacy Issues in Location-Aware Mobile Devices", in Proc. the 37th Hawaii International Conference on System Sciences, 2004.
44. D. A. Norman, The Invisible Computer. MIT press, 1998.
45. F. Nsanze, "ICT implants in human body – a review", 2005.
46. Kas Oosterhuis, Hyperbodies, The IT Revolution in Architecture, Birkhauser, 2003.
47. Dimitris Papalexopoulos, Eleni Kalafati, Takis Zenetos, Digital Visions and Constructed Works, Edil Stampa, (to appear in 2006).
48. Dimitris Papalexopoulos, "The Design – Construction Continuum. For a non-linear, not-fragmented and not limited in time design and construction continuum", Workshop EAAE (Re)searching and Redefining the Content and Methods of Teaching Construction in the New Digital Era, Barcelona Spain, 22-24 September 2005.
49. Terence Riley, "The Un-Private House", The Un-Private House, MOMA, 1999.
50. K.S. Shankar and Helmut Kurth, "Certifying Open Source – The Linux Experience", IEEE Security & Privacy, Vol. 2, No 6, pp. 28-33, 2004.
51. J. Skaburskis, "Territoriality and its relevance to neighbourhood design: a review", J.A.R., vol 3 No1, p. 39-44.
52. R. Sommer, "Man's proximate environment", J.S.I., no 22, 1966, p.59-70.
53. M. Steiner, G. Tsudik, M. Waidner, "CLIQUE: A New Approach to Group Key Agreement", in Proc. the 18th International Conference on Distributed Computing Systems (ICDCS '98), 26-29 May, 1998, pp. 380-387.
54. N. Streitz, A. Kameas and I. Mavrommati, eds, "The disappearing computer handbook". Springer, to be published in 2006.
55. K. N. Truong, E. M. Huang, and G. D. Abowd, "CAMP: A Magnetic Poetry Interface for End-

- User Programming of Capture Applications for the Home", in Proc. 6th Annual Conference on Ubiquitous Computing (UBICOMP 2004), Springer-Verlag, Nottingham, UK, September 2004, pp. 143-160.
56. Jaideep Vaidya and Chris Clifton, "Privacy – Preserving Data Mining: Why, How, and When", IEEE Security & Privacy, Vol. 2, No 6, pp.19-27, 2004.
  57. M. Weiser, "Some Computer Science Issues in Ubiquitous Computing", Communications of the ACM, vol. 36 no. 7, pp. 74-84, July 1993.
  58. M. Weiser, "The computer for the 21st century", Scientific American, vol. 265 no. 3, September 1991, pp. 66-73.
  59. C. K. Wong, M. Gouda, S. S. Lam, "Secure Group Communications Using Key Graphs", IEEE/ACM Transactions on Networking, Vol. 8, Issue. 1, February 2000, pp. 16-30.
  60. V. Zorkadis and P. Donos, "On Biometrics-based Authentication and Identification from a Privacy Protection Perspective: Deriving Privacy Enhancing Requirements. J. " Information Management & Computer Security, Vol. 12, Issue 1, 2004, pp. 125-137.
  61. V. Zorkadis, D.A. Karras, M. Panayotou, "Efficient information theoretic strategies for classifier combination and performance evaluation in improving false positives and false negatives for spam e—mail filtering", J. Neural Network, Elsevier, 18 (2005), pp. 799-807.
  62. J. Zweig and J Webster, "Where is the Line between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Monitoring Systems", J. of Organizational Behavior, Vol. 23, 2002, pp. 605-633.
  63. "4D Space, Interactive Architecture", Architectural Design, Wiley –Academy, Vol 75, No 1, Jan / Feb 2005.

European Commission

**EUR 22765 EN – Joint Research Centre – Institute for Prospective Technological Studies**

Title: Digital Territories - Towards the protection of public and private space in a digital and Ambient Intelligence environment

Authors: Barbara Daskala and Ioannis Maghiros

Luxembourg: Office for Official Publications of the European Communities

2007

EUR – Scientific and Technical Research series – ISSN 1018-5593

ISBN 978-92-79-05653-6

**Abstract**

The advent of a 'whole new world', a virtual or a 'digital' one, the Net, which seems to run almost in parallel to our 'normal' physical world, has already generated heated discussions on its numerous and often ambiguous impacts on our lives and our society at large. In this new reality and as technology becomes more ubiquitous and seamless, one thing is certain: more and more personal data would be required to be collected, stored and exchanged and our 'online'/ digital lives would be even more difficult to separate from our physical ones. Towards addressing this issue, the Digital Territories concept envisages to enable 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. The publication provides an overview of the DT concept and defines its basic categories and components. Furthermore, with a view to clarify and better understand the DT concept and its application, the authors consider some examples of certain online services and applications (current and future) that have already raised serious privacy considerations and discuss the benefits of applying DT application in these cases. Finally, specific considerations with regard to the application of the concept are identified, as well as future steps that could be made towards evolving and applying the concept.



# Digital Territories

EUR 22765 EN



INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES

*ipts*

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.



Publications Office  
[Publications.eu.int](http://Publications.eu.int)

EN  
LF-NA-22765-EN-C

ISBN 978-92-79-05653-6



9 789279 056536