



Digital Territories

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

Executive Summary

Barbara Daskala and Ioannis Maghiros



EUR 22765 EN

2007

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'. 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 (AmI) 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 AmI 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 AmI 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.