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. Living in AmI 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 and protection against discrimination, protection of identity, and protection against intrusions by public and private actors.

Privacy, often 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. Security and privacy concerns are associated with all categories of DT, such as location based systems and services, virtual residencies, and mobile phone networks. Elements of DT 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. These include organizational, procedural, and technical measures, such as - inter alia - 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 who are 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.

The aim of this Workshop is to bring forward into discussion issues relating to privacy, security, and trust in the Digital Territories of the near future, whether these are open or closed spaces, private or public uses, processes or data, etc. The first paper, co-authored by

Dimitris Gritzalis, Athens University of Economics and Business, Hellas
Achilles Kameas, Hellenic Open University, Patras, Hellas
Vangelis Papakonstantinou, PKpartners & Univ. of Patras, Hellas

Workshop on “Framing the Digital Territories”

Editorial

Ambient Intelligence (AmI) is a vision that places human beings at the centre of the development of the emerging knowledge-based society. AmI space consists of a set of technologies, infrastructures, applications, and services operating seamlessly across various physical environments (e.g. office, neighbourhood, home, car, etc.), and thus spanning almost all of 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, a term capable of capturing 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 it will be realised at a pace affected by specific factors; once adopted, it shall cause an imbalance to existing personal and social structures [1,2].

A Digital Territory is an ephemeral AmI space: it is created for a specific purpose, and it 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 AmI 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-disc 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.

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. Living in AmI 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 and protection against discrimination, protection of identity, and protection against intrusions by public and private actors.

Privacy, often 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. Security and privacy concerns are associated with all categories of DT, such as location based systems and services, virtual residencies, and mobile phone networks. Elements of DT 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. These include organizational, procedural, and technical measures, such as - inter alia - 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 who are 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.

The aim of this Workshop is to bring forward into discussion issues relating to privacy, security, and trust in the Digital Territories of the near future, whether these are open or closed spaces, private or public uses, processes or data, etc. The first paper, co-authored by

Dimitris Gritzalis, Athens University of Economics and Business, Hellas
Achilles Kameas, Hellenic Open University, Patras, Hellas
Vangelis Papakonstantinou, PKpartners & Univ. of Patras, Hellas

Workshop on “Framing the Digital Territories”

Editorial

Ambient Intelligence (AmI) is a vision that places human beings at the centre of the development of the emerging knowledge-based society. AmI space consists of a set of technologies, infrastructures, applications, and services operating seamlessly across various physical environments (e.g. office, neighbourhood, home, car, etc.), and thus spanning almost all of 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, a term capable of capturing 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 it will be realised at a pace affected by specific factors; once adopted, it shall cause an imbalance to existing personal and social structures [1,2].

A Digital Territory is an ephemeral AmI space: it is created for a specific purpose, and it 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 AmI 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-disc 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.

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. Living in AmI 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 and protection against discrimination, protection of identity, and protection against intrusions by public and private actors.

Privacy, often 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. Security and privacy concerns are associated with all categories of DT, such as location based systems and services, virtual residencies, and mobile phone networks. Elements of DT 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. These include organizational, procedural, and technical measures, such as - inter alia - 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 who are 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.

The aim of this Workshop is to bring forward into discussion issues relating to privacy, security, and trust in the Digital Territories of the near future, whether these are open or closed spaces, private or public uses, processes or data, etc. The first paper, co-authored by
Finally, the SWAMI (Safeguards in a World of Ambient Intelligence) consortium presents the findings of their project in the paper “Safeguards in a World of Ambient Intelligence (SWAMI)”. The authors present the need to develop safeguards in order to protect valuable assets, if society at large is to benefit from the realisation of AmI vision. Since the challenge lies in identifying safeguards for threats and vulnerabilities, that are yet to be defined, the dark scenarios developed by the SWAMI project are presented as a tool to help illustrate risks that need to be mediated, if AmI is to be a future success story and against which safeguards will need to be drawn.

In order to validate the vision of DT and its associated concepts and to assess their impact to society and technology, a study has been carried out under the supervision and funding of JRC/IPTS. The study was carried out by a Core Expert Group, with the assistance of outside experts [3]. The Workshop builds on the results of this study and aims to provide the fertile ground that will allow the concepts underlying DT to grow and flourish into a useful tool for contemplating the factors that affect the realisation of DTs. We would like to thank those who contributed to this workshop, either by submitting a paper, or by participating in the study and the discussions.

References