

CONVERGING TECHNOLOGIES

2nd Focus Group meeting report



HIDE PROJECT

Project funded by the European Commission-FP7

Contract: 217762

Co-ordination and Support Action (CSA)

Start date of the project: 1 Feb 2008

Duration 36 months

FOCUS GROUP ON TECHNOLOGY CONVERGENCE – HIDE meeting
17 November, 2009
Brussels

This second Focus Group meeting on Technology Convergence was organised in Brussels, on November 2009. This aims was to convene experts from different fields of competencies to trigger the discussions. In that respect, the meeting was structured around three round tables, each of them focusing on different perspectives: industrial, sociological and legal. The meeting was introduced with a short presentation recalling the objectives of this Focus Group.

1st round table: The industrial perspective

Carole Pellegrino and Nicolas Delvaux's presentations¹ both stressed the current problem of individual identification in the real world and in the digital world. Multiple factors, in particular dematerialisation and globalisation, are contributing to undermining Identity, in such a way that it becomes more and more difficult to verify that someone is who he pretends he is.

In the real world, Europe has to face the challenge of protecting its external borders. To that end, various initiatives have taken place, up to now- such as biometric visas and biometric passports - or are being envisaged- such as registered traveller, entry-exit or ETSA. In all these initiatives, the objective is to strike the balance between the fight of illegal immigration and border crossing facilitation for bona fide travelers.

In the digital real, users have the ability to generate and manage one or several identities, providing attributes (name, age, sex, login, and password) they choose. There is no mean to ensure that this information is true, to impede the use of a fake identity or the identity of a third person. Today no tangible element can help to link virtual identity to a given person. At the same time a secure and reliable identity management is vital to prevent security threats and identity fraud. The development of new e-government services and irrevocable transactions require that a digital identity is with no doubt linked to a physical individual. Biometrics is a good candidate to establish this connection.

The discussions stressed that although a lot of efforts are being deployed in the field of research, no industrial policy initiative has been undertaken by the European Commission regarding identity management. For some participants, before considering such an initiative, one should question the strength or the lack of strength of the e-signature's solution, deployed in the European Union. For others, identification in the real world and in the virtual world is the same problem: the proof of identity can only be made if a strong link with a data body is made. This can explain the choice of the EU to use biometrics for passports and visas. However, some stressed that the issue of entry-exit is more questionable. On the internet, ID is different than the one given by the State. Using biometrics could help to proof one's identity. But which biometrics would be appropriate? Face is weak given the number of pictures available on the internet, and fingerprint can be compromised. Therefore technological tools should be put into place to avoid risks.

Technology Convergence: The sociological perspective

In this second round table, *Irma van den Ploeg* addressed the issue of identity, biometrics and behaviour predictability. She stressed the paradox of identification: when a unique ID is attributed it is always assigned to a category, which leads to a double function of identification. As for

¹ Presentations are available on HIDE website.

behavioural prediction, it classifies individual (low risk/high risk). She questioned the objective nature of those systems that are based on cultural assumptions. Recent developments in biometry (multibiometric, distant sensing, under the skin, “soft bio”) are raising the issues of consent and user empowerment: which “normality” is introduced in the system? How the fact of being watched will influence behaviour?

Paul De Herd presentation focused on how education awareness can help citizens to protect their data and ensure a trusted identity. Currently, different ways are foreseen: (i) a way where legislation restricts personal data divulgation (ii) a way where citizens publish personal data and (iii) a way where users are systematically educated to manage personal information.

A pure restrictive legislation approach will be rapidly inefficient because citizens will not accept liberty restriction. The current approach which consists in opening the door to any publication will deliver situation where personal data are misused. Then, citizens may restrict definitively any data sharing to protect their privacy. Education is probably the best way but it is time and effort consuming to provide an adequate education level to all stakeholders. He took a critical approach towards education, as it cannot be neutral: education for what purpose? By whom? what is education aiming at? The voluntary perspective, considers capability of individual to handle properly their data should be based on empirical research. The second perspective would be to take into account the technology where relationship with the technology cannot be predicted in advance. He highlighted the “Pulcinella theory” developed by Emilio Mordini according to which we would suffocate if we had to keep our secret, that why we have to find a way to share our secrets. That is the case with identity.

Education should not be the unique instrument; governments and technology companies should assume their responsibility in particular regarding the right to forgetfulness

Technology Convergence: The legal perspective

Baroness Sarah Ludford addressed the ability of the current legal Framework (95/46 directive) to address the Risk of a Surveillance Society driven by the Private Sector. She stressed the changes with the entry into force of the Lisbon Treaty as of 1st December, as the European Parliament will gain more power in the field of justice and security. She expressed her concerns with the risks of a surveillance society with RFID chips anywhere and the multiplication of databases. She was doubtful about the benefit that the revision of the directive could bring. She considers that the existing framework enables enough flexibility and that a modification could lead in fine to undermine data protection. She stressed that we do not give enough value to privacy, as the sanction are not strong enough comparing for example with antitrust sanctions.

Henriette Tielmans (Covington & Burling) ²exposed the functioning of the current legal framework and mentioned the weaknesses that should be addressed in the revision process. A reflexion shall be conducted on the need to streamline a legal framework that is fragmented (commercial use versus law enforcement, telecommunications versus other sectors). The Lisbon Treaty sets the conditions for a single legal basis. Another issue that should be further investigated is the adequacy of the texts with the technological developments: ubiquitous computing, cloud computing, Biometrics, RFID chips, nanotechnologies.

Patricia Josselin (Hass société d’avocat) questioned the need to include the right to forgetfulness in the new legal framework, i.e to ensure that information is completely and once and for all delete after a given period of time. However how to assent or dissent when you do not know that your data are being held or published? Technical tools shall assist the implementation of this right. This

² Presentation available on HIDE website

would mean an automated deletion or anonymisation of data after a given time. The issue of the retention period is not easy to answer. Shall this right be specific or also concern police files? Shall this right be defined at EU level or by Member States ? To be efficient, this right should be complemented by technical tools.

During the discussions, the need to adjust the current legal framework was raised. It has proven its flexibility and its capacity to adjust to technology evolution. However, it fails somehow to effectively protect personal data, in particular as regards data published on the internet. Another issue that can be of concern is the right to identity that is the core element of personal data: some participants mentioned that this right is not sufficiently protected. Another issue which was lengthily debated is the right to forgetfulness. It was broadly admitted that the revision of the directive should be an opportunity to debate in-depth this issue and to evaluate whether it would be relevant to create such a right. The issue of a better harmonisation amongst the Member States was also addressed. As a matter of fact, Data Protection Authorities are given a considerable margin of interpretation, in particular regarding the proportionality principle, which gives rise to very different applications. This lack of harmonisation does not enable enough visibility for the industry. Certification mechanisms, based on “common criteria”, could be an appropriate answer to this problem: this methodology used in the IT sector to measure security performances is internationally recognised, and has proven its efficiency. It could be duplicated to ensure that a product or a system is “data protection compliant”.

Results: The participants’ contributions to this focus group meeting will be used as input to produce a ethical brief on technology convergence. This ethical brief will be further discussed, developed and finalised with the next meetings as the main FG deliverable.