

MINUTES
FOCUS GROUP TECHNOLOGY CONVERGENCE
PARIS 9th SEPTEMBER 2008

The three speakers conducted presentations highlighting the various features of technology convergence: technical, legal and ethical aspects (see the presentations published on the website). A lively discussion took place amongst the participants, which drew the attention to a number of issues that need to be further investigated by the Focus Group:

- The first main topic relates to the **need for a better understanding of the state of art of the technology, its potential evolution and future applications**. Today, technology convergence is a reality. However, one should recall that the surveillance society and facial recognition has not yet converged. In this domain, the technology is at an emerging stage and far from being mature. Research is still underway, a lot of demos are presented but one should have in mind that they only function in ideal situations. They are not ready to be implemented in real life situations, where lighting conditions are poor. Today, the technology does not enable the identification of a single person in large public space, such as large international airports. It was recalled that the technology is as such neutral; it cannot be presumed whether its applications will be positive or negative.

- As stated in the background paper, the Focus Group (FG) recognised the potential benefits for the citizen as far as security is concerned. The capability of human surveillance is weak in public open spaces, such as large international airports. In those environments, the technology could complement and enhance human observation and identification (by sending an alert, for example, where a critical behaviour is presumed). In parallel, the FG considered that the **risks of misuse shall be indentified**. The discussions enumerate a number of concerns to that respect:

- Personal data can be used to construct profiles, resulting potentially in **discrimination**. The surveillance system could establish some correlations to classify people, the level of surveillance could therefore vary according to the ethnic, social or religious origins, age, gender, sexual preferences etc. This differentiation could lead to segregate certain categories of people. In order to avoid systematic suspicion, there is therefore a strong need to ensure that the system does not impact vulnerable groups. In addition, the risk of monetarisation should be considered as it could widen the **social divide**. Some people could accept to pay to be classified in a “positive list” This is for example the case at Schipol Airport, where the use of automatic gate costs a traveller 100 Euros a year.

Technological paternalism was another risk mentioned during the meeting.

The FG underlined that multimodal surveillance may constitute a potential **threat to individual freedoms**: the mix of storage capacity, identification in public spaces and data mining creates new information that may affect individual civil liberty. The identity of individuals participating in a demonstration could be stored. How to ensure that anonymity is respected in public places was questioned.

- The **adequacy of the legal Framework** was another issue discussed by the FG. The need to apply the fundamental principles of data protection as strictly as possible was

underlined, while at the same time some loopholes of the current legal framework were identified; how can people access and modify stored data if they are not aware of the type of recorded data that has been collected? In addition to citizen empowerment, the core of the EU directive could be jeopardized if the individual were unable to give clear consent/dissent about which of his/her personal data are stored. How far can individuals choose their exposure to surveillance and limit personal information collected and used? This issue is crucial when those systems are self-generating data. Therefore, the consent should be given not only for stored data but also for the processing of data. In addition, the right of access and modification should be guaranteed. The FG also questioned whether or not the current definitions of “data” and “sensitive data” are appropriate, when looking at the processing of data that could generate a profile. For example, buying a Bible, a Torah or a Koran could reveal information on the religious affiliation.

- **Intention** is another crucial question: the detection of criminal intent could lead authorities to consider a person as a suspect and arrested him/her, when no criminal act had been committed. The principle of the presumption of innocence would thus be infringed. This raises the question, “to what extent should an intention should be considered as proof?”
- **The shift from human to technological surveillance has a number of social impacts.** For example, the quantitative increase of collected data due to the multiplication of sensors has lead to a qualitative revolution. The amount and concentration of data has changed the nature of the control. Moreover, ubiquitous surveillance could have perverse effects and could drive behaviours of stigmatised social or ethnical groups causing them to behave inappropriately. T
- **The FG also agreed on the need to identify measures to prevent risks, and stressed that future work and discussions should address this point.** In the post 9/11 environment, public acceptance of security measures has tremendously dropped, followed by the adoption and implementation of public policy measures. In the meantime, with the booming of web 2.0, citizens are voluntarily posting a huge amount of personal information on the Internet, revealing sensitive data (religion, marital status, music they are listing to, etc). The emergence of the “internet of the things” will accelerate this phenomenon. In this context, one should examine if individuals should be protected against themselves. In addition, the identification of measures to prevent risks of abuse, ex ante regulatory monitoring and privacy enhancing technologies were addressed as appropriate tools.
- To conclude, the Group agreed upon the fact that this project should be used as an opportunity to participate in the decision making process, and should be used not only as a proactive tool to launch prospective reflexion on how CT should be tackled, but also as a leverage to propose a funding policy.