



FOCUS GROUP MEETING ON

Technology convergence

FG COORDINATOR

Sagem Sécurité

DATE

9th September

PLACE

Rodchester Hotel, Champs Elysées, Paris

Overview:

The Homeland identification and Technology Ethics project is a Co-ordinated action promoted by the Commission within the 7th Framework Programme. As part of the core activities of this project a series of technological orientated focus groups are planned to explore significant issues in relation to the ethics of particular technologies. These four technological areas are: technology convergence, outsourcing security, interoperability and Privacy Enhancing Technologies. The activities on technology convergence are organised by Sagem Sécurité, this focus group being the first of three planned on this topic. The ultimate objective of this focus group is to use the insights, data and discussions generated therein in contributing to the writing and presentation of an ethical brief on Convergence that will serve as an informative appraisal for the European Commission, policymakers and the general public.

Venue: **Rochester Hôtel**, 92 rue La Boétie, 75008 Paris (metro station : Saint Philippe du Roule, line 9)

<http://www.paris-hotel-rochester.com/index.html>

Time: 10a.m – 4p.m

You can contact *Brenda Rose* +33 1 58 11 87 28, should you encounter any problem on the day of the meeting.

Discussion Note:

Over recent years the level of surveillance has mushroomed and continues to grow. Video surveillance cameras have become part of the urban environment and have been installed to protect not only critical infrastructures but also shopping malls, public transports, public buildings, parking areas; in addition, law enforcement cameras (for speed and red light control and number plates recognition) are being installed on road junctions, highways or tunnels. With the rapid shifting from analogue closed circuit to digital technology, capabilities of video surveillance has been improved tremendously as it has enhanced storage capacities, archives searching, processing and capturing as well as footage analyses.

The most sophisticated cameras can capture the entire dynamic range of a scene regardless of the light conditions. Other features, such as miniaturisation, motion detection, day/night operation, backlight compensation, dynamic noise reduction, remote and automatic lens control, further enhance the functionality of cameras. With the combination of surveillance camera and face recognition software, a face caught up by a CCTV can be matched up with one of several thousand suspects in a data bank.

This makes it possible for law enforcement officials to proactively identify and monitor persons of interest. It can also be used by immigration officials to screen travellers arriving in an airport. Next-generation facial recognition software will possibly allow discerning an individual's emotional state. Research in video content analysis is ongoing not only to enable age and gender identification, but also to facilitate socioeconomic status based on clothing. This could raise the question of whether technology could lead to discrimination against individuals or groups.

Thermal imaging is another illustration of converging technologies, which has been used during the SARS episode. At that time, the UK firm Land Instruments sold about 50 of its thermal imaging systems to airports in Asia and Middle East. The equipment, which includes a finely tuned infra-red camera, was used to quickly scan passengers and identify anyone with even the slightest hint of a fever.

Another UK company is marketing a CCTV camera that can see objects under a person's clothing at a range up to 25 meters, with the ability to distinguish between metallic and non metallic items.

Locating, tracking and tagging

In parallel with the proliferation of surveillance cameras, positioning technologies are developing: mobile phones, GPS enabled devices and RFID tags allow geographical tracking of goods and individuals in real time.

Location information can effectively turn mobile phones into tracking or surveillance devices, as they allow the carriers to know where the user is located, not only when making or receiving a call, but also when the phone is idle. With a penetration rate exceeding 100% in the EU, there is frequently no differentiation between the mobile as a device and the mobile user: any EU citizen could be traced and located any time. Communication data thus play an important role in law enforcement operations, as they allow the police to establish links between suspected persons, or ascertain where a person was at a given time, thereby confirming or disproving an alibi. They can also bring important safety benefits, like helping emergency services locating an accident.

As GPS devices (including cars' and phones') are taking off, they potentially offer a tool for invasion of privacy, as the accuracy of the location is more precise than the location provided by a base station, or via triangulation or E-OTD. GPS embedded-devices could be easily used by employers or car rental companies to track a person or a vehicle's route.

Radio-frequency identification (RFID) chips are another potential location tracking technology. The declining cost of RFID systems along with improved sensitivity and durability has increased its usage. Applications range from areas such as security, manufacturing, logistics, animal tagging, waste or storage management, postal tracking, airline luggage and road toll management. RFID chips and tags are proliferating and are embedded in cars, clothes, identification documents, travel documents, public transports cards, loyalties cards, sub-skin implants enabling new

commercial applications such as contactless payment, counterfeiting prevention, access to VIP clubs, etc. Some RFID tags can be "active" (i.e. incorporate a battery) and can communicate with a reader that is several tens of meters away. As a consequence, an individual might not be aware that an RFID tag in a product they have bought is transmitting information, nor will they be aware of who is able to pick up the data.

On its own terms pervasive video surveillance threatens privacy, but when combined with other technologies such as those above mentioned, this could lead to an Orwellian society. At the same time as recording images, detailed information on anyone who came within the cameras range could be captured via a sensor: name, address, biometric features embedded in RFID chips. This means that video surveillance could provide a critical pillar of a surveillance infrastructure and create potentials to monitor citizens any time any place.

On the one hand, those location based-services provide convenience and benefits for users (such as navigation, live traffic reports, m-commerce), but on the other end they could reveal significant information on a person habits or consumption usages. To which extend consumer have to be protected against their own will to provide information? The "pay-as-you drive" scheme relying on GPS technology and mobile phone networks to track individual car usage to offer cheaper premiums to drivers who avoided high risks periods can illustrate this concern.

While this offer has been rejected by the CNIL on the French market, in the UK this offer launched in 2006 has not taken off and was recently withdrawn by Norwich Union.

Convergence and behaviour detection to prevent criminal acts

As the use of digital video for surveillance augments, there remains a need to automatisation in order to decrease the amount of manpower required to operate surveillance systems. Studies on human observations raise serious concerns regarding boredom, distractions, multitasking, and "change blindness"(i.e. looking but not seeing or losing connection with reality). Studies in the USA have demonstrated that a human observer viewing two monitors with automatic image switchover will miss up to 45% of all activity in scenes after only 12 minutes. This raises up to 95 percent after 22 minutes.

In order to alleviate the need for human resources solutions are being developed to automate video surveillance. Intelligent video surveillance enables to detect unexpected movement or unusual behaviour that may pose a threat to people, property and infrastructure. The software filters and interprets data captured by cameras in circumstances where a human observer would not be able to assess developments as they arise. The analysis can be performed in real-time or retrospectively in playback for evidential purposes. Accurate and efficient automatic video analysis system will allow detecting unusual unexpected, suspicious or unusual

behaviour or events in real time and. Potential risks or situation requiring attention of security officers will trigger an alert, thus enabling them to take preventive actions.

While video surveillance remains mainly utilised in the investigation phase, the ultimate goal of intelligent video security system using image processing is to improve the prevention of incidents and accelerate action triggering. As they will become a more effective security tool, video cameras will be used to interrupt acts of crime or terrorism, raising a number of ethics and legal concerns:

- Can it be considered "reasonable" to impinge upon the freedom of someone who is merely suspected of committing a crime?
- To which extent the intentions of an individual can be inferred from their visible behaviour?
- What are the criteria to be defined to consider a suspicion as "reasonable"? Are there reliable indicators of intention to engage in hostile actions?
- Is it possible to segregate dangerous behaviour from normal behaviour? Does the technology differentiate between a hug and an aggression?
- Does the "objectivity" of the technology can help to define a subjective element such as an intention?

Balancing privacy and security

From a law enforcement and investigative standpoint, the potential benefits offered through new electronic technologies may be substantial, e. g., the development of more accurate and complete information on suspects, the possible reduction in time and manpower required for case investigation, and the expansion of the options for preventing and deterring crimes. While providing increased security, the use of sophisticated technologies for surveillance purposes also presents possible dangers to society. Over time, the cumulative effects of widespread surveillance for law enforcement, intelligence, or other investigatory purposes could infringe privacy rights.

Before networked CCTV, people scrutinised by a camera were anonymous, they were being looked at but not tracked. New technology can connect a person's name and database records to their name or biometrics. In the same time, technologies for collecting, storing, transmitting and processing data are developing rapidly; these technologies could make a significant impact on privacy.

Ethical and operational questions surround the collection and use of video images used in conjunction with data bases and raise concerns that personal data collected will not be used in an unreasonable and accountable ways (such as data matching, aggregation, and profiling of electronic footprints with multiple data bases)

The evolution of risk perception since September 11th has led to a greater acceptance of security measures. The collection of data in public places, with the camera as the dominant form of data input device, is coupled with the integration of surveillance with statistical monitoring and security applications. The passive gathering of intelligence represents a challenge to privacy in public places that has been largely accepted. Ross Anderson, a professor at Cambridge University in Britain, has compared the present situation to a "boiled frog" -- which fails to jump out of the saucepan as the water gradually heats. If liberty is progressively eroded slowly, people will get used to it.

- How much privacy are we ready to give up for a more secure life?
- How can a balance of security and privacy be established without endangering the basis for our democratic societies?
- How can good solutions to protect privacy serve the European security industry?
- Is it possible to prevent surveillance abuse?
- What safeguards need to be put into place?
- Is the current legal framework satisfactory in the context of converging technologies?
- Who is the legitimate authority that can evaluate the risk and therefore decide which measures to be adopted? (State, DPA, the media, the public opinion?)

Agenda

10.30 – 10.45 coffee

10.45-11.00 Welcome / overview on convergent technologies and Ethics Focus Group
by Carole Pellegrino, Sagem Sécurité

11.00 -11.30 Presentation of the technical aspects involved by convergence
by Nicolas Delvaux, Sagem Sécurité

11.30- 12.00 Legal aspects involved by convergence
by Antoinette Rouvroy, Law professor at University of Namur

12.00- 12.30 ethical aspects involved by convergence,
by Emilio Mordini (to be confirmed)

12.30-14.00 lunch

14.00-15.30 Round panel – Are technologies able to detect intention?

The panel will consist of speakers and participants to the meeting. The aim of the discussion will be to have an informal idea-generated discussion based on the principal themes identified during the first session.

15h30-16h00 Wrap-up