

Note on the participation on the Roundtable “Ethics vs. efficiency in content extraction for digital evidence“, in the framework of the LASIE first Workshop. London 15-16 July

Alfonso Alfonsi, member of P-React Ethical Advisory Board, took part in the workshop “**LASIE: supporting forensic analysts in digital evidence retrieval and analysis**”, organised by the LASIE research project in London (UK), at the Queen Mary University of London premises on the 15th and 16th of July 2015.

The 1st LASIE Workshop aim was to promote the opportunity represented by LASIE in empowering forensic analyst and investigators in fighting against crime and in training operators in using technologies supporting them in dealing with digital evidence and facing ethics and privacy issues.

One distinctive aspect of the workshop was to facilitate the interaction of end users in the security field with security system developers, decision makers and ethical and privacy experts. The networking and knowledge sharing with other EU funded projects was also foreseen, hence the invitation to P-react to be present. The program of the workshop was articulated in three sessions, a **training session**, aimed at end users; a **Roundtable** with experts and end users, an “**EU session**”, in which relevant EU projects, including P-react, were presented.

Dr. Alfonsi took part as an ethical expert in the second panel Roundtable “**Ethics vs. efficiency in content extraction for digital evidence**“, held on the 15th July afternoon and whose main feature was the interaction and exchanges between end users of surveillance technologies and experts in the field of ethics with different backgrounds: law, philosophy, sociology, engineering.

The Roundtable was organised in the "Brussels style", i.e. each panelist was asked exactly the same question and had sharp **two minutes** to reply, which favored an intense and focused interaction. Also the discussion was held under the Chatham house rules. The Roundtable was divided in two panels, in the first one the discussants were all end users and was intended to give them the opportunity to present their needs and their problems in terms of compliance with privacy and ethics requirements.

The second panel of the Roundtable, in which Dr. Alfonsi was one of the discussants, was devoted to the perspective of social scientists. The major questions proposed were the following.

1. What technologies, fuelled by information, would never be accepted by the society? In other words where lies the thin red line between socially acceptable and unacceptable surveillance?
2. The surveillance industry continues to develop more and more invasive technologies but actually not many of them are fulfilling hopes vested therein, are not widely accepted and/or not used in practice. Can you analyse an example from your own experience?
3. What ethical values, principles and ideas other than privacy and personal data protection need to be taken into consideration in assessing surveillance? Is it ever possible to make an exhaustive list of these values for each (type) of surveillance technology?

4. Are the developers of surveillance technologies, policymakers, etc. taking ethics seriously? We have a number of actors in this saga: business, police, the society at large, individuals, etc. When it comes to ethics, what each of them is doing good and what each of them is doing bad? Any scope for improvement?

As mentioned above the discussion was animated and interesting argumentative, with a positive constructive critical interaction with the law enforcement actors, who showed a keen interest in the ethical and social issues and who manifested a strong demand for viable solutions to the army enforcement problems. It was also felt that the opposition “ethics vs. efficiency” might be a misrepresentation.

Among the many points raised one can name the discussion on social acceptance of surveillance technologies, or lack of it, as being not so much related to one technology with respect to another, but as a dynamic social construct, resulting from the complex interplay of ethical, social, psychological and political drives.

Also the overall social risks of poorly socialized surveillance systems were discussed, highlighting how they can affect public trust and the perceived quality of the democratic life. The risk of stigmatization and discrimination against specific vulnerable groups by abuse in data mining and profiling was also mentioned.

Finally one can mention that it was recognized that, while many difficulties remain, the diverse actors involved in the deployment of surveillance technologies (developers, law enforcement agencies, law specialists, ethical experts, etc.) are interacting and communicating much more than in the past and that this might be crucial for a healthier surveillance management system.