Statement to LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citzens

Dr. Reinhard Kreissl IRKS Vienna, Coordinator of IRISS

This is a report about first results from an FP7 research project on increasing resilience in surveillance societies (IRISS). Given the short time available I will restrict myself to address a few questions. A more comprehensive account can be found on the project website[1]:

(1) Can encompassing surveillance be considered as an adequate means to combat and prevent crime and terrorism?

(2) What are the effects of surveillance in the area of law enforcement?

(3) Can the spread of surveillance be governed in a politically accountable and rational way?

Contemporary societies are surveillance societies. Their citizens are machine-readable techno-social hybrids by default. So these societies lend themselves to large-scale surveillance based on electronic data processing technology. The idea of a private sphere becomes problematic under these conditions and can be addressed if at all as a problem of data protection.

(1) Surveillance technologies can be used to identify, locate and track individuals. They also can be used to screen populations and flows of goods, information and money. Different technologies are combined into assemblages increasing the power and intrusiveness of surveillance measures. Comprehensive surveillance can help to detect an incident. It also can help to prosecute offenders, but falls short of preventing crimes and acts of terrorism from happening. Surveillance is powerful to track a known individual under suspicion or a suspicious object. It is less useful to identify problematic situations or individuals in advance.

(2) Surveillance has different kinds of effects: it creates new categories of individuals (social sorting); it affects the behaviour of citizens (chilling effect); it shapes the operation of law enforcement work (intelligence-led policing) and it increases the risk of abuse (breach of privacy regulation). Under specific conditions surveillance triggers counter effects that can increase the resilience of civil society against illegitimate intrusions. A number of public reactions to the Snowdon revelation clearly demonstrate this. Making surveillance a topic of public debate on the basis of information about the strategies and technologies in operation can help to reach an informed societal consent about the use of surveillance.

(3) Governing surveillance in a rational and accountable way is difficult for several reasons. Governing surveillance amounts to governing what could be called a security-industrial complex. Different players with different interests sustain a situation with increasing demand for more technology. The application of new technologies requires changes in the law at different levels. Policy makers have to rely on threat assessments

[1] See: (http://irissproject.eu/wp-content/uploads/2013/04/Surveillance-fighting-crime-and-violence-report-D1.1-IRISS.pdf). See also Wright D., Kreissl R. (eds.): *Surveillance in Europe* Routledge 2014, forthcoming

produced by Law Enforcement and Security Agencies and there is almost no independent evidence available demonstrating the effectiveness of surveillance or weighing intended against unintended effects. Politicians are taken hostage by the security-industrial complex, producing worst-case threat scenarios and offering socio-technical solutions to prevent major incidents. It is far from clear though whether the assessments are valid and whether the proposed solutions live up to the promises made by providers.