Privacy and data protection aspects of European 'smart' security technologies and policies

Since 2006 'smart' surveillance has become a buzzword among computer scientists and European policy makers. While there is currently no accepted legal definition of 'smart' surveillance, the term generally refers to the use of computer vision and/or pattern recognition technology to analyse 'big data' in order to enable semi-automated decisions. This article intends to clarify how the right to privacy and the protection of personal data should affect the use of smart surveillance by analyzing two distinctive case studies: smart CCTV technologies and the EU's 'smart borders' initiative. Smart CCTV technologies generally alert CCTV operators to pre-defined cases of 'abnormal behaviour,' while the EU's 'smart border' package would replace the manual stamping of passports of third country nationals with an automated electronic registry in order to monitor the stay of these visitors.

On the basis of a detailed analysis of these two case studies, section 1 of this article will analyse whether 'smart' surveillance is different from 'mass' or 'targeted' surveillance. Section 2 will outline the relevant privacy and data protection framework that applies in the EU to the use of both smart CCTV technologies and the EU's border security policy. Section 3 will analyse which similarities and differences might exist in the application of this framework in order to attempt in section 4 a general conclusion on the privacy and data protection aspects of 'smart surveillance' in the EU.

Mathias Vermeulen
Research Fellow - European University Institute (IT)
Phd Candidate - Centre for Law, Science and Technology (LSTS) at VUB (BE)
Mobile: [+32] 472 966 017
http://www.eui.eu/law
http://www.vub.ac.be/LSTS
http://legalift.wordpress.com
http://twitter.com/legalift