

**RISE Workshop:**  
**Ethical and Policy Implications of Global Mobility and Security**

**Conference Presentations – Brussels, September 2010**

**Reviewed by Speakers:**

*Peter Hustinx, European Data Protection Supervisor, **Recent developments of the European Data Protection framework***

[Peter.hustinx@edps.europa.eu](mailto:Peter.hustinx@edps.europa.eu)

In his keynote speech, Mr Hustinx discusses the latest developments of the European Data Protection framework. After outlining the challenges and opportunities, emphasis is placed on the need to make data protection work in practice. The strength of The Lisbon Treaty and New Commission in building data protection is highlighted, after which the relevant trends and prospects for more effective data protection are outlined. The presentation discusses the implications for technology, controllers and data subjects and recommends increased supervision. It concludes by reflecting upon the increasing concerns for privacy and increasing awareness of citizens of the impact of technologies in a globalised world.

*Cagatay Karabat, Turkey National Research Institute of Electronics and Cryptology, **Biometrics and Biometric Security***

[cagatay@uekae.tubitak.gov.tr](mailto:cagatay@uekae.tubitak.gov.tr)

This presentation provides a technical overview of the practical application of biometrics for authentication and verification. After outlining the privacy and security problems from biometrics, Turkey's eID Project which uses a fingerprint verification model is discussed in detail. Mr Karabat proposes 'Biometric Hashing' as a means of mitigate such privacy concerns and reflects upon the challenges relating to privacy and people and security and systems. To conclude, the presentation suggests using biometric and cryptology protocols to ensure privacy and working towards a joint-signal processing cryptographic approach.

*Dimitrios Tzouvaras, ITI – Informatics and Telematics Institute, CERTH – Centre for Research and Technology Hellas, **Behavioural and Activity Related Biometrics: Policy and Technological Challenges***

[Dimitrios.Tzouvaras@iti.gr](mailto:Dimitrios.Tzouvaras@iti.gr)

This presentation explores the use of different behavioural and activity related biometric modalities and the associated challenges. The research objectives of ACTIBIO (Activity Related and Soft Biometrics) are outlined and three pilots are discussed in detail. Cutting-edge physiological activity-related biometrics are explored for 'on-the-move' authentication of personnel and unobtrusive methods for the collection of biometric data. The need for a transition from classic biometrics to the new concept of activity related biometrics is proposed and the latest advances in the field of behavioural biometrics are discussed. Dr Tzouvaras highlights developments in gait recognition and a bottom-up concept of behavioural recognition. The presentation considers ethical issues from data

collection and the course of policies, and concludes by presenting possible applications of behavioural biometrics.

*J.Peter Burgess, The Peace Research Institute Oslo (PRIO), **Trust, security and insecurity***

[jpb@jpeterburgess.com](mailto:jpb@jpeterburgess.com)

[jpeterburgess@me.com](mailto:jpeterburgess@me.com)

This presentation discusses the relationship between trust and technology. After outlining the concept of trust as a 'replacement for certainty', it provides a typology of trust comparing trust in things and trust in people. Professor Burgess discusses the contractual nature of trust and role in analysing security. It is nearly impossible to map trust to technological means, yet to mobilise biometrics we need to allow trust. A paradox of 'security and trust' is discussed as we cannot seek security in trust, yet trust is essential in security. An overview of the limitations of trust is followed by a discussion of the relationship of trust between risk, security institutions and technologies. Professor Burgess concludes his presentation by proposing that trust is a type of 'dependency' on technical and social systems and emphasises the growing importance of trust in ensuring security in Europe.

*Margit Sutrop, Centre for Ethics of the University of Tartu, **Identity management:***

**philosophical perspective**

[Margit.Sutrop@ut.ee](mailto:Margit.Sutrop@ut.ee)

This presentation discusses the pressing question of identity management from a philosophical standpoint. The concept of identity and morally problematic exclusion of 'moral identification' in biometrics is outlined. The presentation highlights the potential discrimination from biometrics looking at what 'type' of person rather than which person. Professor. Sutrop explores the notion of a 'morally autonomous person' and proposes several questions on informed consent and who actually defines what is in the public's interest. To conclude, the presentation proposes a public debate on biometrics to allow autonomous subjects to reflect on their best interests.

*Ioannis Tsoukalas, MEP, Committee on Industry, Research and Energy, **Privacy and anonymity in the Information Society***

[ioannis.tsoukalas@europarl.europa.eu](mailto:ioannis.tsoukalas@europarl.europa.eu)

In his key note speech, Professor Tsoukalas discusses key issues of privacy and anonymity in the information society. The EU Parliament should be adequately informed and must safeguard against issues surrounding the internet. Professor Tsoukalas explores changes in the definition and application of biometrics and proposes that the notion of individuality is at stake as the EU has made concessions as a matter of principle. After exploring the balance of privacy and security, the protection of privacy arms race is described as a '21<sup>st</sup> century cold war' between security and data protection. The presentation highlights the issue of technology design for quantity and not quality,

and calls for a complete 'framework' on data protection. To conclude, recommendations for privacy by education and the empowerment of individual citizens are outlined.

*Paul de Hert, Tilburg Law School, Travelling should be fun. A consumer perspective on mobility.*  
[paul.de.hert@uvt.nl](mailto:paul.de.hert@uvt.nl)

This presentation raises the importance of considering technologies when travelling from a consumer perspective. It first introduces the difficulty of not downplaying and yet not over-exaggerating technology in the 'double technology paradox.' Professor de Hert cautions against engaging in only one perspective and the concept of the 'trusted traveller' at border controls as we must ask what is the added value of the technology. The need for legitimacy based on consideration of the error rates of biometrics is discussed and an overall need for a 'consumer friendly perspective' in new security apparatus emphasised. The presentation concludes by highlighting the role of EU Passenger Rights to allow data protection principles to compliment consumer law.

*Andrzej Drygajlo, Speech Processing and Biometrics Group Swiss Federal Institute of Technology Lausanne (EPFL), Biometrics for Identity Documents and Smart Cards: policy and technological challenges*  
[andrzej.drygajlo@epfl.ch](mailto:andrzej.drygajlo@epfl.ch)

This presentation introduces a European perspective in advancing biometrics development as identified in the COST 2101 Action 'Biometrics for Identity Documents and Smart Cards.' The objective is to investigate novel technologies for unsupervised multimodal biometric authentication systems. After exploring the ePassport, the challenges associated with automated border controls are outlined, highlighting a lack of interoperability. Dr Drygajlo argues that systems should use multimodal biometrics and offers several policy recommendations to facilitate best practices. To conclude, it proposes that biometrics should be considered as a critical infrastructure if a global system for biometrics authentication is to be developed.

*Asbjorn Hovsto, Intelligent Transport Systems, Norway, Biometrics at seaborder and landcrossing points*  
[hovsto@online.no](mailto:hovsto@online.no)

This presentation discusses the use of biometrics at Border Crossing Points (BCPs) and how it is crucial to identify people and things throughout their passage within the border areas. After a description of 'passenger flow', BCPs are defined for airports, sea ports and landborders. It highlights the poor and inconsistent applications of biometric recognition at BCPs and suggests why biometric information protection for identity authentication scenarios is required. Differences in privacy cultures show variation between the EU and non-EU countries and biometric systems are seldom rolled out today. Mr. Hovsto recommends an integrated approach and standards-based technologies at BCPs and beyond in order to protect biometric reference data. The presentation concludes by considering threats to BCPs and goals to develop security metrics. A legal framework based on ethical and social implications should support BCP infrastructures at many levels.

*Aljosa Pasic, Atos Research & Innovation, Department Director, Challenges for Context-Aware Privacy Reconfiguration*

[aljosa.pasic@atosresearch.eu](mailto:aljosa.pasic@atosresearch.eu)

This presentation discusses the challenges associated with privacy in general and some directions for a possible solution such as context-awareness and privacy reconfiguration. Taken from a large industry perspective, the presentation stresses a requirement from the EU security industry to have more coherent EU legal framework and privacy properties assessment\evaluation as well as the clear guidelines that can be used in the design and development of privacy compliant solutions. The presentation introduces concerns expressed in a White Paper of EOS (European Organisation for Security) and emphasises the need to boost public-private dialogue. Mr Pasic argues that future privacy challenges are not only about personal integrity or identifiable information, but also about 'contextual information', such as location or online presence. After discussing three specific research projects, their results and challenges they brought forward, a possible solution that uses context information in order to optimise configurations of privacy components has been presented. To conclude, some remaining open challenges on ensuring privacy are listed.

*Jacques Bus, Centre for Security, Reliability and Trust, University of Luxembourg – Former Head of Unit Trust and Security ICT Program – Directorate-General for the Information Society and Media, European Commission, Consumers' Confidence and Trust in the Digital Environment*

[JB@digitrust.eu](mailto:JB@digitrust.eu)

This presentation discusses the concept of trust on the web. A brief history of the fundamental role of trust is given, followed by a comparison between trust in people and trust in systems. The transformational nature of the web with respect to relations and transactions raises new questions of trustworthiness and building trust. Authentication management must be met with an interdisciplinary approach to develop effective trust solutions. The presentation outlines the interplay between technology, policy and the end-user, and lists key recommendations from the RISEPTIS board. Dr Bus concludes by emphasising the role and risks of cloud computing on the development of a 'techno-legal ecosystem' to protect the consumer.

*V. C. Zorkadis, Hellenic Data Protection Authority, Biometrics-based Authentication and Identification from a Privacy Protection Perspective*

[zorkadis@dpa.gr](mailto:zorkadis@dpa.gr)

This presentation discusses issues on how authorities deal with biometrics in practice and the policy to facilitate research in biometrics in Greece. After presenting data protection requirements in the context of European legislation, the decisions taken on biometrics by the Hellenic Data Protection Authority (DPA) are discussed. A distinction is made between cases regarding biometric systems research and those concerning the operation of biometric systems in actual conditions. The former are normally approved, whereas the latter are examined with decisive criteria the crucial character

and safety requirements covered, the proportionality principle and the privacy friendliness and the security measures of the biometric systems. Furthermore, Mr. Zorkadis presents mechanisms to increase the privacy-friendliness of biometric systems. The presentation concludes by recommending the application of privacy by design by education and privacy impact assessments across the EU, and the possibility that pseudonyms derived from exploiting soft-biometrics may reach maturity and have a future.

*Carla Ilten, Centre for Technology and Society - Technical University Berlin, Germany, Security Organisations - Privacy and Accountability*  
[ilten@ztg.tu-berlin.de](mailto:ilten@ztg.tu-berlin.de)

This presentation discusses how privacy is handled in practice from a perspective going beyond law and technologies. Recent interview research findings from the PATS project are discussed in detail, focusing on different types of organisations such as security technology producers or service providers. Ms. Ilten discusses the different types of privacy awareness amongst the security organisations and levels of public communication. The findings reveal that in practice, privacy is not easily translated from the law. The presentation concludes by outlining differences in the notion of privacy and posing questions regarding the role of responsibility, and in particular accountability, as a key challenge in privacy practice.

---

**To be reviewed by Speakers:**

*Ioannis Vakalis, EC-JRC-Ispra, IPSC-STA Unit, Automatic Border Crossings*  
[ioannis.vakalis@jrc.ec.europa.eu](mailto:ioannis.vakalis@jrc.ec.europa.eu)

This presentation discusses existing Automated Border Crossing (ABC) systems which allow biometric authentication. Some installed, pilot and future examples for airports, land and ports in Europe are outlined, after which a brief background to ABCs and its predecessor 'registered traveller' schemes to fast-track airport security controls is provided. The EU ePassport as the basis for the design and use of ABCs is discussed in detail with concomitant security and data controls (Basic and Extended Access Controls). The presentation outlines innovations of EU ePassport including the integration of secondary biometric information. Dr. Vakalis identifies the key ABC operational stakeholders and lists the possible threats to security and privacy and types of attacks on ABC systems. The presentation concludes by recommending a redesign of the security and business model around ABC to incorporate the positive and negative aspects of their use. Additional measures must introduce protection features and procedures to safeguard data processing.

*Neil Robinson, RAND Europe, Is the trade off model of the relationship between security and privacy still tenable? Results from a pilot study.*  
[neilr@rand.org](mailto:neilr@rand.org)

This presentation discusses findings from a Pilot Study which looks at the trade-off between civil liberties, privacy and security, from an end-user individual perspective. The presentation outlines

the limitations of typical public opinion surveys in informing policy makers and introduces RAND's self-initiated research which uses a 'stated-preference' approach. Mr Robinson gives an overview of how this methodology was applied to assess the Biometric Passport in three scenarios in which security versus civil liberties trade-offs may arise. Key findings show a trend that people are willing to pay up to a point to sacrifice privacy and liberties after which the law of diminishing returns takes over. To conclude, the stated-preference approach is proposed as a viable methodology in the context of understanding trade-offs in the security domain.

*Pratap Reddy, Director, Cyber Security, NASSCOM, **Cyber Forensics Training in PPP mode to help LEA***  
[pratap@nasscom.in](mailto:pratap@nasscom.in)

This presentation provides an insight into the cyber security initiative of NASSCOM and DSCI (Data Security Council of India). After providing a background on IT growth in India, the challenge to spread awareness and build a culture of security is presented. Mr Reddy details the efforts to identify all Indian residents through issuing a unique identification number, 'Aadhaar', to create the world's largest IT database. The technology, legal and resource challenges are outlined with the need for a security and data privacy framework. Mr Reddy promotes PPP as the way forward and highlights a lack of cooperation and expertise. To conclude, the presentation reflects on India's position at the forefront of promoting data security and privacy working at a policy level.

*Max Snijder, European Biometric Forum, **Biometrics for public administrations: how do things connect?***  
[max.snijder@eubiometricsforum.com](mailto:max.snijder@eubiometricsforum.com)

This presentation discusses the use and wider impact of biometrics in public administrations. A brief overview of the history and future of biometrics in different systems is provided, after which wide variations in ID systems in Europe and the limitations of biometrics are explored. The collection of biometric data for use in a public administration database was approved under the Dutch Passport Act but there are questions surrounding the difference between criminal and biometric databases in terms of negative and positive data respectively. Mr Snijder outlines recommendations from the Council of Europe on document security and concludes with a list of questions on the handling of biometrics for public administrations.