
Privacy and Identity in the Information Society: Systemic Risks

*Report of the workshop held in Brussels
5-6th February, 2002*

1	INTRODUCTION	3
2	TECHNOLOGY ISSUES.....	3
3	DISCUSSION – R&D ROADMAPPING.....	4
4	CONCLUSIONS.....	5
5	ANNEX 1 - SUMMARY OF KEYNOTE PRESENTATIONS.....	6
5.1	PETS IN ENTERPRISE – ELS VAN HERREWEGHEN, IBM ZURICH	6
5.2	IDENTITY MANAGEMENT – SEBASTIAN CLAUSS, UNIV OF DRESDEN, GERMANY.....	6
5.3	IDENTITY MANAGEMENT – OTTO VERMEULEN, PWC, NETHERLANDS.....	6
5.4	END-TO-END PRIVACY INFRASTRUCTURE - STEPHAN ENGBERG, OPEN BUSINESS INNOVATION, DK	7
5.5	PETs IN THE INFRASTRUCTURE – ALBERTO ESCUDERO-PASCUAL, KTH,	7
5.6	EUROPEAN CYBERCRIME CONVENTION – JOOP VERBEEK, UNIVERSITEIT MAASTRICHT	7
6	ANNEX 2 - BIOMETRICS CLUSTER MEETING: SESSION 4 REPORT.....	8
7	ANNEX 3 - LIST OF PARTICIPANTS	10
8	ANNEX 4 - WORKSHOP AGENDA	12

1 Introduction

This document provides the report of a workshop on *Privacy and Identity in the Information Society: Systemic Risks*, held in Brussels on 5-6th February, 2002.

The workshop was organised by the Institute for the Protection and Security of the Citizen (IPSC) of the European Commission's Joint Research Centre (JRC), in the context of its R&D activities and policy support to DG Information Society in the area of cyber-security and e-Europe.

The objective of the Workshop was to debate the specific technological problem of end-to-end privacy management in both business and consumer domains. The output from the workshop will contribute to the categorisation research of priorities, and will specifically address the issues relating to the development of a research network in the Privacy domain for the Sixth Framework Programme.

It achieved these objectives via four workshop sessions:

1. Presentation of EC funded privacy related projects
2. Keynote presentations on the theme of Systemic Privacy risks
3. A technology related poster session
4. Debate session

Sixty experts in the field of privacy and privacy technologies, drawn from a cross-section of parties interested in these issues from industry, government and research organisations attended the workshop.

The keynote presentations are summarised in Annex 1. The list of workshop participants is attached as Annex 3. The workshop agenda is attached as Annex 4.

This report is also available on the eprivacy forum web site: <http://eprivacy.jrc.it>

2 Technology Issues

The opening session brought together project members of EC funded privacy related projects identify the range of research activities being carried out within EC funded projects, and to establish areas of synergy between them. The projects presented included the following:

- PISA - Privacy Incorporated Software Agent: Building a privacy guardian for the electronic age
- GUIDES - Guidelines for assessing technological compliance with Data Protection Directives
- PRIDEH - Privacy Enhancement in Data Management in E-health
- MAFTIA - Malicious and Accidental-Fault Tolerance for Internet Applications
- DRIVE - Drugs in Virtual Enterprise

It was noted that there is scope for stronger collaboration between these projects, as there are many points on which the technology issues are complimentary. The mechanisms for collaboration were discussed within the context of the roadmapping exercise which is discussed in a later section of this report.

It was hoped that representation from the EC funded Biometrics related projects would be made. Although no representation was actually made at the meeting, a report from the January 15th Biometrics cluster meeting on issues relating to privacy is attached as Appendix 3 of this report.

3 Discussion – R&D Roadmapping

The workshop consolidated issues raised in two prior workshop meetings:

- Privacy and Identity in the IS: Emerging Technological challenges; 4-5 October 2001
- Digital Identity; 10-11 December 2001: Focus on wider socio-economic, legal issues.

The definition a roadmap activity for the FWP 6 R&D programme was agreed. This roadmap will require the establishment of a constituency of stakeholders in the area of privacy and identity in the Information Society. It will also need the further elaboration of the research themes identified during the workshop by means of appropriate mechanisms such as networking of stakeholders.

The roadmap proposal has been called RAPID (Roadmap for Advanced Research in Privacy and Identity Management Technologies). It will become Proposal for a support measure under IST-FWP5

The proposed roadmap activity has three main objectives:

- **Community building**
 - Identify the key actors and form a critical mass of industrial and academic research players to lead and conduct future R&D.
 - Identify wider community of stakeholders (DPA, Citizen rights, ...)
 - Industry and international cooperation (Associations, W3C, ...)
- **Roadmapping**
 - Identify socio-economic, legal drivers for PETs and IM
 - Identify the R&D challenges and needs for PET and Identity Management technologies in the next 5 years.
- **Possible implementation models, including education/awareness**
 - Achieve consensus on RTD priorities with stakeholders
 - Coordinate with related roadmap initiatives (Dependability, Biometrics, Smart Cards, ...)

The research and thematic priorities for the research network have been largely defined by the workshop activities, and are summarised as follows:

- New computing paradigms: Ambient Intelligence, virtual identities, complex interactions of agents and systems, intelligence in infrastructure, m-commerce, e-health, e-gov
- Socio-economic-legal: crime prevention (identity theft), new legal entities for identities.
- Multiple and dependable identity management: user controlled identity disclosure
- PETs for Enterprise: Control disclosure in Multi-party complex organisations, data transfer
- PETs in infrastructure: privacy preserving authorisation schemes, secure comm., anonymity control, design for privacy

- Open Source PET solutions

4 Conclusions

The series of workshops over the period 2001-2002 have brought together a wide range of stakeholders in the privacy debate. The central focus of the meetings has been the issue of technology support for a privacy compliant information society, and a number of increasingly important technology, socio-economic and policy issues have been identified as a result of the discourse. The culmination of these activities has now been seen in the development of a proposal for a research network embracing privacy experts from diverse domains that can roadmap and prioritise research themes for the privacy aspects of the Cybersecurity theme within the imminent Framework 6 RTD programme.

It is clear that there is a continuing role for debate in this domain, and particularly debate that can produce closer harmonisation of the legal and technological approaches to privacy management.

5 Annex 1 - Summary of Keynote Presentations

5.1 Pets in Enterprise – Els Van Herreweghen, IBM Zurich

This presentation staked out the issues pertaining to privacy management in the B2B sector, and the role that PETs can play in achieving privacy compliant business processes. Some of the key issues stressed were:

- Process re-engineering – the challenge of integrating privacy and security management into the business process. Issues discussed included: B2B privacy policies, customer privacy services, privacy violation detection, auditing of services, codes, seals, standards;
- Technology requirements – the drivers in this area include secure/anonymous communication, trust establishment, payment delivery, anonymity, and an Intelligent infrastructure.

The IBM Business Privacy Architecture was discussed, as a framework to highlight how the diverse technology and process requirements might be harmonised. Recommendations for technology development in a number of areas was made, including; Dependable Identity Management, Dependable infrastructure, consolidated privacy and security solutions, and privacy enhancing PKI, incorporating blind certificates.

5.2 Identity Management – Sebastian Clauss, Univ of Dresden, Germany

This presentation contrasted diverse architectures and models for on-line Identity Management (such as MS passport, Liberty Alliance). The technology drivers in this area include; the need control personal data for end users, minimisation of data collection, transparency and track of data spread. The importance of user authentication was stressed to combat Identity theft, whilst maintaining the possibility for pseudonyms and partial anonymity. The speaker presented a model based upon a client server architecture which incorporates PKI, CA's, service for data access, and protocols: pseudonymous authentication, Negotiation, Data exchange, and communications protocols to access IDM essential services. A project proposal has recently been submitted to facilitate the development of the IDM architecture.

5.3 Identity Management – Otto Vermeulen, PwC, Netherlands

The speaker presented a state of the art review of commercial off the shelf solutions that can be integrated into a commercial business process for identity management. The presentation focused largely on internal business management, but also demonstrated principles for B2B Identity Management. The business benefits of integrating Identity Management processes within the Information Technology infrastructure of a business were highlighted, namely the potential for significantly reduced overheads associated with managing access rights, data flow and user accounts within a company.

5.4 End-to-End Privacy Infrastructure - Stephan Engberg, Open Business Innovation, DK

The speaker proposed the need for an alternate approach to the privacy management problem with the challenge of "Making Privacy Default". Three main issues were addressed:

- a) Identity Disclosure Management - The accountability vs. Anonymity issue
- b) Privacy in Pervasive Computing - The authentication issue.
- c) The Privacy Infrastructure - The Convenience/integration issue.

The speaker challenged the concept that Privacy Management must be based upon a trust framework, and questioned the real need for Identification over Authentication if accountability is ensured within a system. Existing approaches and priorities were challenged in favour of an alternate framework based on Privacy by Design.

5.5 PETs in the Infrastructure – Alberto Escudero-Pascual, KTH,

This presentation discussed the privacy vulnerabilities of the Internet and mobile communications. It addressed the emerging risks and vulnerabilities associated with third generation (3G) infrastructures and the use of the IPv6 protocol. The trend towards intelligent infrastructures and dumb terminals was highlighted. The data minimisation approach was again stressed as the key to facilitating privacy compliant systems. This argument was supported by examples from the location based services application domain, describing how these services can be implemented with minimal privacy invasion. The conclusion of the talk was that business models for Internet services should be developed which 'make money from the crowd' through the provision of services rather than on the exploitation of individual's personal data.

5.6 European Cybercrime Convention – Joop Verbeek, Universiteit Maastricht

The speaker presented a review of the new Cybercrime convention, drafted by the EC. The presentation charted the development of the Cybercrime Convention, and examined the balance between the requirements crime prevention and detection in cyberspace and the needs privacy and individual freedom. There are still a number of complex unresolved contradictions in the Convention, which the speaker elaborated on. A detailed paper was provided at the meeting and is available at the eprivacy website; <http://eprivacy.jrc.it>

6 Annex 2 - Biometrics Cluster Meeting: Session 4 Report

15 January 2002 Workshop: Paving the way for the adoption of biometrics Session 4: Biometric non-technical issues and national initiatives/ broad scope projects

Chairman: Henning Arendt Rapporteur: Marek Rejman-Greene

Project Officer: Alain Jaume Issue 1 (25 January 2002)

Summary: Four major presentations were made: B& L Management Consulting, Association for Biometrics (AfB), UK Government's Biometric Working Group (BWG) and TeleTrusT. In addition two short talks were given by representatives from the Dutch Biometrics Forum and the Irish Government.

The discussion that followed clearly noted that almost all of the non-technical issues were required to be addressed in the immediate future, as failure to solve these could impact on the success of any public deployment (and many implementations in closed groups). Two specific areas were noted: privacy concerns and robust testing methods to assess non-technical aspects of biometrics, e. g. acceptability, usability, trust in authorities handling biometric data doing so in a legal and open manner. The novelty of these security methods and their probable future ubiquity makes it imperative

that the biometric community develops solutions and informs the public in clear and direct ways. The importance of resolving the open human and societal issues was illustrated by the Irish Government's insistence on their resolution prior to embarking on any deployments. This could be by means of an agreed industry code of conduct.

The presentations had shown that (originally) national initiatives for development and sharing of knowledge, and networking were developing in Europe. Their success in attracting memberships outside of their home country made it clear that there was a need for a wider pan-European forum. The Biometrics Consortium in the USA (sponsored by government agencies) had been very successful and a European body based on this model (as adapted for our distinctive market and cultural diversity) could pick the best points from the BC, while avoiding some of those aspects that had not worked well.

Due the fragmentation of the European market, and the resulting need for effective networking and development of partnerships across the continent, such a body needed to be driven by the commercial sector and their needs. Of course, the academic community and specialist consultants would have key roles in supporting such an endeavour. The group commended this model of a European Biometr9cs

Consortium for the consideration of the European Commission.

Details.

A useful way of categorising the issues involved with the use of biometrics was offered by the BWG:

Technology (best practices, integration) Regulation and legislation

The User in Society (including the development of a dialogue with citizen's groups and in addressing the possible misuse of biometrics in excluding certain groups, such as the unwaged in

shopping malls and people with disabilities or falling outside of the standard range of human anthropometrics).

We noted a specific element outside of the group's remit, which extends to all security measures: how does the industry construct a meaningful business case,

when the benefits of using better security are largely unquantifiable (e. g. in the form of money saved by not having systems hacked), the risks to individuals of loss of personal privacy are equally unknown and unmeasurable while the costs of installing and maintaining the additional security are all too clear.

7 Annex 3 - List of Participants

Name	Organisation
Chris Bailey	Assoc for Progressive Communications, UK
Sebastian Clauss	TU Dresden
Paul De Hert	University of Tilburg
Yves Deswarte	LAAS-CNRS, Toulouse
Alberto Escudero Pascual	KTH/IMIT
Emile Etienne	Respect my Privacy asbl
Caroline Goemans	K.U. Leuven (ICRI)
David-Olivier Jaquet-Chiffelle	University of applied sciences Bern/CH
John Borking	Dutch D.P.A.
Steve Kenny	Dutch D.P.A.
Marc Langheinrich	Inst.of Information Systems
Yann Le Hegarat	CNIL (French DPA)
Helena Lindskog	Ericsson
Ludwig Oberendorff	Dutch Ministry of Interior Affairs
Maria Veronica Perez Asinari	University of Namur
Bart Preneel	K.U.Leuven
Marie Georges	CNIL
Yann Le Hegarat	CNIL
Jean marc Dinant	CRID, University of Namur
George Danezis	University of Cambridge
Jan Huizenga	TNO
Caspar Bowden	FIPR, UK
Alberto Sanna	Hospitale San Raffaele, IT
Joris Claessens	K U Leuven
Morten Borup Harning	Open Business Innovation
Stephan Engberg	Open Business Innovation
Sophie Louveaux	e-Consult, BE
Stefan Lindskog	Karlstad University
John Ketchell	CEN/ISSS
Henry J.F. Ryan	CEN/ISSS IPSE WG (ET)
Pierangela Samarati	University of Milan
Frank Schasfoort	Pricewaterhousecoopers
Otto Veremeulen	Pricewaterhousecoopers
Nicole Maarse	Pricewaterhousecoopers
Joop Verbeek	University Maastricht
A C Lacoste	Belgian Privacy Commission
Victor Car	Belgian PrivacyCommission
Karen Banks	Greenet/APC, UK
Juergen Tappe	Siemens AG

Bob Thibadeau	Carnegie Mellon University
Anne Verkuyt	Microsoft Europe-Brussels
Els Van Herreweghen	IBM Research Division
Rigo Wenning	W3C
Tom Jackson	Joint Research Centre-IPSC
Marc Wilikens	Joint Research Centre-IPSC
Giles Hogben	Joint Research Centre-IPSC
Laurent Beslay	Joint Research Centre-IPTS
Cecile Huet	DG INSO – C4
Alain Jaume	DG INFSO – C4
Andrea Servida	DG INFSO – C4
Yves Paindeveine	DG INFSO - B
Diana Alonso Blas	DG MARKT, Data Protection
N H Boulanger	DG MARKT
Cesar Santos	DG ENTERPRISE – D4
Corinna Schulze	DG ENTERPRISE – C3

8 Annex 4 - Workshop Agenda

Tuesday 5 February

13h30 – 13h45 Workshop Introduction – Andrea Servida, DG INFSO

13h45 – 14h30 Workshop Overview and Presentation of Previous Work
JRC Representatives: Tom Jackson, Marc Wilikens, Lauren Beslay

Session 1: EC Privacy Related Projects

14h30 – 16h30 Project Presentations:

- PISA - Privacy Incorporated Software Agent: Building a privacy guardian for the electronic age
- GUIDES - Guidelines for assessing technological compliance with Data Protection Directives
- PRIDEH - Privacy Enhancement in Data Management in E-health
- MAFTIA - Malicious and Accidental-Fault Tolerance for Internet Applications
- DRIVE - Drugs in Virtual Enterprise

16h30-17h30 Discussion and Summary

Wednesday 6th February

Session 2: Systemic Risks and Holistic Solutions

09h15 – 09h30 Introduction
Session Chair

09h30 – 12h00 Panel Presentations:

Pets in Enterprise – Els Van Herreweghen, IBM Zurich

Identity Management – Sebastian Clauss, Univ of Dresden, Germany

Identity Management – Otto Vermeulen, PwC, Netherlands

End-to-End Privacy Infrastructure - Stephan Engberg, Open Business Innovation, DK

PETs in the Infrastructure – Alberto Escudero-Pascual, KTH, Sweden

12h00 – 12h30 Debate

12h30-14h00 Lunch and Poster Sessions

14h00 – 14h30 Invited presentation

European Cybercrime Convention – Joop Verbeek, Universiteit Maastricht

Session 3: Research Network on Privacy

14h45 - 1500 Introduction

Session Chair – Marc Wilikens, IPSC, JRC

15h00 – 16h30 Discussion – EU Privacy Research Network

16h30 – 17h00 Summary and Closing Remarks