

	<p><b>Dynamic Coalition on Privacy</b>  <b>IGF 2007, Workshop 28 (SEC)</b>  <b>Privacy in Internet Identity Management:</b>  <b>Emerging Issues and New Approaches</b>  <b>Workshop report</b></p>	<p><b>IGF</b>  <b>UN Internet</b>  <b>Governance</b>  <b>Forum</b></p>
---	--	--

### Organizers

The workshop was organised by Ralf Bendrath (Collaborative Research Center “Transformations of the State”, University of Bremen) and Mary Rundle (Harvard’s Berkman Center for Internet and Society, the Oxford Internet Institute, and Stanford’s Center for Internet and Society), with input from other members of the IGF Dynamic Coalition on Privacy. The organizers have been working together in the IGF Dynamic Coalition on Privacy since it was set up at the IGF 2006, with Ralf Bendrath being a co-facilitator.

### Panelists

- ◆ **Caspar Bowden**

Caspar Bowden is chief privacy advisor at Microsoft for Europe, the Middle East and Africa. He was formerly director of the Foundation for Information Policy Research, an independent British think-tank that studies the interaction between computers and society in the fields of e-commerce, copyright, law enforcement and national security, e-government, cryptography and digital signatures. Among other activities, he was expert adviser to the UK parliament on privacy issues.

- ◆ **Jan Schallaböck**

Jan Schallaböck is a lawyer with the Independent Center for privacy protection, which is also the office of the privacy commissioner of the state of Schleswig-Holstein in the very north of Germany. Jan has been working on issues of information regulation for several years now and has been participating in the WSIS and is representing his office in the dynamic coalition of privacy. He researches the use of privacy technology within the European PRIME-Project. Jan is also active in standardisation of IdM in W3C, ITU-T and ISO, where he has been acting secretary in the Working Group on Privacy and Identity of SC27 (Sub-Committee on Security).

- ◆ **Marcelo Thompson Mello Guimaraes**

Marcelo Thompson is a former Attorney General of the Brazilian Information Technology Institute - ITI, under the Office of the President of Brazil, where he worked on both the Brazilian Free Software Programme and the Brazilian Public Key Infrastructure. He is currently reading for a Doctorate of Philosophy in ‘Information, Communication and the Social Sciences’ at Kellogg College and the Oxford Internet Institute, University of Oxford.

- ◆ **Izumi Aizu**

Izumi Aizu is a senior research fellow at the Institute for InfoSocionomics, Tama University, Tokyo, Japan. He is also a member of ICANN's AtLarge Advisory Committee and has been active in the Civil Society Internet Governance Caucus since the early phases of the World Summit on the Information Society.

- ◆ **Moderator:** Ralf Bendrath, University of Bremen, Germany, co-facilitator of the IGF Dynamic Coalition on Privacy.

## Summary

The workshop's purpose was to facilitate a discussion on the emerging issues around internet identity management (IdM). It mainly focused on two aspects: the global public policy aspects and a need for international cooperation to ensure privacy in internet IdM; and new possibilities for users to express preferences for data protection in new IdM systems.

The workshop was well-attended. The audience's knowledge about the issue was very diverse, ranging from technology experts from the industry to interested diplomats and civil society members. This made understanding each other a bit tricky sometimes, but it also showed the great potential of the IGF as a forum for exchanging knowledge, ideas, and perspectives.

After a short introduction by the chair, Caspar Bowden introduced the topic and presented the current debate among internet identity management practitioners and innovators. It is clear now that "identity" is not something that is there and stays fixed, but is context-dependent and dynamic. Also, depending on the specific context and situation where one is asked to identify, a small subset of information is normally enough to proceed with a transaction. Different roles should not by default be linked to one another. This basic concept allows for the security and authenticity of online transactions and at the same time protects privacy. The "Laws of Identity", summarized by Microsoft's Chief Identity Architect Kim Cameron, have so far been the most popular summary of these conceptual ideas. An interesting development in this field is the trend towards open standards and protocols for identity management, CardSpace and OpenID being the most relevant ones at the moment.

Izumi Aizu then linked these technical developments to the international policy arena. He gave an overview of the different standardization bodies and international organizations that deal with internet identity at the moment: ISO, ITU, Identity Gang, OECD, OpenID Foundation, CEN, ANSI, Identity Gang, W3C - just to name a few. His presentation made clear that there is a need for better coordination in order to avoid duplication. At the same time, the complexity even of this narrow field illustrates that important technical design decisions are made in a landscape of bodies and arenas that only experts really can follow and understand. This is a political and democratic problem, because the emerging standards for internet identity management will affect hundreds of millions of internet users worldwide, and the way they are built is having a huge impact on their privacy-preserving properties.

Marcelo Thompson made this point perfectly clear in his presentation, where he summarized a report he had co-authored for the OECD. The main point is: In an electronic environment, we all leave digital footprints, register with websites, and authenticate to numbers of different services, also with different identity properties. As a consequence, many of these services build a profile of us based on the information they have. This is then often used for categorization and automated decisions. However, it is important to understand that one central concept of modern philosophy is the idea of "personhood", including all facets of our life, especially those ones that are not easily represented in digital forms. We have human rights and freedoms because we are persons. Profiling and digital identification implies the risk that the online service providers see their users only as limited profiles, not as full persons. Therefore, decisions based on digital profiles which negatively affect real persons always have to be checked by a human. This is already part of European privacy legislation, but not always fully implemented and enforced. It also has to be taken into account by the technical standardization bodies in this field and ensure user control of all identity information.

Jan Schallaböck then described the conceptual findings of the project “Privacy and Identity Management for Europe” (PRIME). The multi-stakeholder network collaborating in this project has taken the discussions by Kim Cameron and others one step further, in two ways: Conceptually, they have built a stronger link between identity management and European privacy legislation and fundamental rights. This was also translated into technical designs and proof-of-concept applications. With modern cryptography, it is now possible to digitally authenticate with, for example, a government-issued electronic ID card in such a way that the issuing authority does not find out about the authentication activity – just as our governments do not have to know to whom we show our paper-based passports.

The discussion mostly circled around two questions:

1. What is technically possible? How can identity management be built in a way that enhances security and privacy at the same time? Here, it became clear that many policy-makers and regulators still have the impression that there is a necessary trade-off between security and privacy, while modern cryptography can actually enhance both at the same time. This is especially relevant in the growing field of government-issued digital identifiers for their citizens, which will in the mid-term also be used widely for electronic commerce and other internet applications. The workshop participants agreed that more informative sessions like this would be helpful in the future, in order to ensure that political debates and decisions are enlightened by knowledge of the most recent technically possible and privacy-enhancing solutions.
2. What are the global public policy implications? The plethora of IdM standardization bodies makes clear that there needs to be more coordination, especially on the international level. While most of the technical details can be left to the experts, a political message and agreement on the underlying norms and values guiding the technical developments would certainly be helpful. It was unclear if the IGF was the right forum for doing this, but most participants agreed that it certainly is a good forum for starting these discussions.

### **Follow-Up**

The workshop and the discussion led a few of the participants to start further collaboration in this field as a subset of the work of the Dynamic Coalition on Privacy. They agreed to jointly submit a workshop proposal for the IGF 2008 under the title “Policy aspects of Privacy Enhancing Technologies”.