

# Facing good security, we need better privacy

---

Yves Deswarte

LAAS-CNRS, France



## Network security is improving

---

- ❖ Laws on digital signatures -> PKIs
- ❖ IP-Sec -> IPv6
- ❖ Deployment of Intrusion Detection Systems

... but threats are growing

---

- ❖ DDoS (distributed denial of services)
- ❖ e-commerce fraud
- ❖ Transnational e-criminality

...thus the need for more security

---

- ❖ e.g., ingress traffic filtering by ISPs
- ❖ more audits, more records, ...

## ... which undermines privacy

---

- ❖ It is more and more practical and easy to collect private information: accurate, non-repudiatable.
- ❖ Laws on the protection of personal data are inefficient: voluntarily basis, rather than technically enforced (same for P3P).

## In privacy area, research is weak

---

- ❖ There is no economic pressure for privacy
- ❖ Historically, research on security has been funded by defence agencies, and later by financial organisations
- ❖ Governments are more interested in nation security and law-enforcement rather than citizen's privacy

## Research should be funded

---

- ❖ Development of Privacy-Enhancing Technologies (PETs)
- ❖ Pseudonymization, restricted certificates, anonymity relays, ...
- ❖ Privacy-preserving authorization schemes

## Need-to-know: Example

---

- ❖ A merchant does not need to know the real identity of a customer, only the validity of the money order
- ❖ The customer's bank does not need to know the identity of the merchant, only the reference of his bank account
- ❖ Etc.

... of course

---

- ❖ Real identities would be disclosed to a judge in case of dispute, or on request by judicial authorities (to prevent money laundering, for instance)