

A world without PETs

A summary of the presentation given by Stephan Engberg at the conference 'A Fine Balance 2007'

Stephan Engberg, founder and CEO of Priway has spent the last eight years researching and developing privacy and security enabling systems and mechanisms. He started his presentation by stressing the need for people involved in security and privacy to set aside their previous ways of thinking as digital integration forces us to rethink.

First he suggested a more operational approach to definition of terms. Privacy is security from the point of view of a single stakeholder. In a networked economy, the design of balances are important as - due to interdependence - security of one stakeholder is an illusion unless it also improves security of other stakeholders in cases of breach. Trust is willingness to accept risk in a certain context and as such a growing cost element as risk acceptance continue to drop. A root requirement of a PET is that it breaks the assumption of a zero-sum trade-off by enabling value functionality such as sharing data without compromising on stakeholder security rights and needs in cases of failure.

He then suggested there is no reason to accept losses of privacy – on the contrary individual security and control is the root source of security, innovation and effective society processes – especially government processes. Security deteriorates because identification concentrates risks, creates interdependence and new data vulnerabilities and identity theft. Command controlled models for complex economic systems such as government accumulates inefficiencies as it cannot adapt to the sophisticated needs and requirements of end-customers. Open market innovation deteriorates as attention moves from servicing customer needs to profiling to maximize marketing communication and short-term sales on the expense of overall value creation. An attacker can easily turn a surveillance system into an attack on its purpose exemplified by attaching a bomb triggered by automatic face recognition to a surveillance camera. Surveillance is not part of a security system except as an response to a previous non-invasive mechanisms which have detected a non-responding potential threat.

He pointed towards Government as the critical enabler of privacy and security through the monopoly on the identity structure and regulation of infrastructure. He presented the basics of National ID 2.0 and a Citizen ID Card where root identification is only used to create new keys and identifiers adapted to the specific purpose. By maximizing attention to fall back and the correct distribution of controls, can we protect the increasingly more vulnerable server systems and data bases – as the most critical element of critical infrastructure. Identity has to build in security balances even before a new process even starts in order to maintain security after the transaction. We can no longer protect data in databases, but we can prevent an attacker – internal or external, deliberate or accidental – getting access to utilize the data and keys for attacks elsewhere.

A service provider would have better security and access to better data if an attacker cannot launch or scale an attack based on knowledge in the systems. Data can be shared without establishing risks towards the system owner or end-customer increasing willingness to share. And most importantly value chain attention would be directed towards servicing real and actual customer needs instead of using the continuous profiling for control, persuasion or the use of illegitimate force. In other words, even though a specific entity may prefer lock-in, may desire to control to further selfish objectives or may prefer to be in a position of power over a citizen and such gain a short term gain on the expense of longer term losses – all society interests points

towards the values, needs and possibilities to empower the citizen to pull the value chains for security, efficiency and competitiveness through innovation.

As a simple example to document this is almost always be done, Stephan Engberg, then demonstrated how to maintain security and privacy without the use of trusted third parties even in a Healthcare Emergency situation where the patient is unconscious. It was based on one the many recent PET breakthroughs in the form of RFIDs with built-in end user PET that does not leak identifiers, one-time-only mechanisms and a gradual linkage to first anonymous patient summaries and then gradually to the patient health care file itself. This also provide the basis to securing Healthcare as such as patient controls can be optimized for mutual benefit.

A world without PETs is a world where security, government efficiency and market innovation continue to erode. Data protection cannot compensate for bad security and with good security, data protection and anti-identity theft is build into the root structures. The PET tools are or can be made available, but Government controls the demand. Responsible governments cannot afford or defend not to incorporate PETs as part of critical infrastructure. Research is always needed, but the core problem is the government demand to focus on surveillance and control instead of security and risk mitigation. If the demand-side works, research in outstanding issues will follow.