Contributions of the Parliaments in Europe to the eMergence: Merging and eMerging Technologies, Processes, and Institutions

Tomaž Štebe
THE NATIONAL ASSEMBLY OF REPUBLIC OF SLOVENIA

What can MPs do to enhance public and political trust into the (information) systems managing sensitive data and documents?

Where should MPs (and NGOs, why not) be involved in this effort to explain and develop trust? ICT is in fact a significant opportunity for trustworthy D&D processing. How and where to be active? Shall we be YES or NO promoters?

What can be done? What can MPs do as humans / citizens and as a legislative and supervisory body?

Which positive results can be expected from the modern information technology, appropriate organisation and supervision? Could there be a non-human involved - trustworthy, verifiable systems and organisations? The simplicity and functionality of many systems depending on sensitive data collection and processing.

Typical reaction; the question still and often asked today is:

What happened with sensitive data? Is there any snooping of privacy???

Big Brother / (Big Sister (!?) ... Government) – is watching you!

There are always humans, i.e. bad guys, involved;

Could past and present justified public distrust be overcome?

Situation / Problem:

Yes, it is true. Many governments do. The public has quite negative past as well as everyday experience with intrusion of their privacy. The prevailing opinion is that there is no perfect system or fully honest organisation – to be trusted 100%. 
The systems with sensitive data and documents do and will exist also for very normal, not only secret/intelligent services, organisations or governmental or public services.

Citizens, healthcare, social, police, courts, customs, communication personal and business, technology sensitive data are still mainly available on classical media (archive/communication-paper/computer), spread around at different (non)secured locations and in different copies. Data and documents are presented, copied, re-entered, and viewed by many (different) people. Accesses are not registered in a non-destructible manner. Supervision is managed by people again. Control is exercised by authorised groups, guards and recorded with electronic/computer systems (cameras). We trust (?!?) / we somehow accept this classical, well experienced systems. More or less, at least there are no great, excessively oriented, feared and emotional discussions.

Worried and seriously concerned people (NGOs) / politicians on one side and the information system experts and companies on the other are not trying enough to listen to each other's explanations and fears to reach common sense.

We are definitely becoming a super tightly meshed-coupled society, especially with the broad involvement of internet. There are new trends, not having one's individual storage at home or desk PC. SW is not installed on one's own computer but in service companies and paid by usage time. Privacy policy is accepted and trust is given to companies such as Microsoft or Google. And there are scanning systems for early detection of suspicious, terrorist-like activities.

Intelligence services, the military, and the customs are all examples of highly protected and secure information systems in accordance with the specifics of the organisation and its traditional exclusive operations.

**What do we need?**

We need to build on trust into the (computer) systems collecting, storing and processing sensitive (private and business) data and documents (D&D). They are important (indispensable) for the quality and, we should say, for the security of our lives. But the information technology needs strict organisational mechanisms, appropriate fire walled applications and objectively non-human dependent supervision. Technology and experiences are indeed available. What they need is legislative and human higher trust background, authenticity, credibility, trustworthiness, and promotion by a good authority.

Modern database information systems could most significantly contribute to the development of trust: through explanations and discussions as well as NGOs' and other supervisory parts' involvement in the development of sensitive D&D fire walled applications and systems. Social, cultural, political and technical discussions could contribute to the understanding and acceptance. Instead of having many local (video camera & sensors, etc.) systems backed by local staff and other humans involved, the system for storage and processing could be more centralized and D&D
"hermetically closed" - available only to the application processing, to the owners or to authorities on the basis of a court order.

**Discussion Topic Summary:**

Trustful management of sensitive matters in the information systems - their effectiveness, functionality, simplicity, supervision, the owner's data and public representative's authorised control need to trust in technology and in organisational solutions.

What can or should the parliaments (the MPs, institutions, the experts) do to change the often publicly simplified, unilaterally promoted and accepted generalised explanation, characterised by the slogan "big brother is watching you"?

Such opinions generate opposition to the collection, processing and distribution of sensitive data by the authorities (or businesses) that could be managed effectively using modern ICT, data management and organisation mechanisms, enabling the highest possible trustworthiness, security, reliability and - last but not least - functionality and efficiency incomparable with the classical methods and medias?

The fears and oppositions are present even if the above operations are implemented by modern, reliable and credible information systems and accompanied organisations, and even if that is the only way to effectively perceive, trace and prove criminal activities or manage business operations.

How to gain acceptance and understanding in the trust of the modern information organisations and systems? Hermetically fire walled sensitive databases, with strict and no person registered authorised accesses should be presented, explained and discussed as a safe, secure, trustful and effective solution, where the only possible access is allowed to a public elected commission.