

Trust in Digital Life, Inaugural Meeting (December 8, 2009)
Proposed Working Group 4

Topic

How an agenda for research and innovation might factor in democratic values.

Initial Framing of Issue

Democratic Protections in Technology:

1. Should technology be designed to:
 - (a) Enable checks and balances and separation of powers?
 - Should ICTs be designed for checks and balances and separation of powers? (How?)
 - What is the role of transparency and accountability?
 - (b) Honour values such as privacy, freedom of expression, protection of minorities, freedom of association, and freedom of belief?
 - How can we achieve effective privacy and data protection across jurisdictions?
 - And would the same cross-jurisdictional approaches work to support the other democratic values noted here?
2. Are there economic, social, and legislative or regulatory initiatives that may help in this effort?

Results of in Discussion (in bullet points)

Democratic Protections in Technology:

1. Should technology be designed to:
 - (a) Enable checks and balances and separation of powers?
 - Should ICTs be designed for checks and balances and separation of powers? (How?)
 - Privacy engineering comes with a cost.
 - What is the role of transparency and accountability?
 - Lack of accountability around breach notification legislation.
 - Liability issues around smart devices (if decisions are based on them, but the device has provided incorrect data who is liable? Would the liability model be the same as for say a "Use by Date" that is wrong?)
 - How would consumers know if embedded devices are functioning as expected? That they are not tampered with?
 - In practice there are not many data subject access requests. Because these requests are expensive to respond to, why not design all new systems with the requirement in mind so that people can automate their own access to their own data (including behavioural data)? How to design usable privacy/data access controls?

- (b) Honour values such as privacy, freedom of expression, protection of minorities, freedom of association, and freedom of belief?
- How can we achieve effective privacy and data protection across jurisdictions?
 - Perceived value and real value of trust need to be brought together.
 - Damaging fallout of failure in terms of perceived trust (at company or country level).
 - Definitions are in flux, for example: Romanian Court ruling on data retention and privacy protection; communications data versus content, and how the distinction is becoming arbitrary; what does "sensitive data" mean nowadays?!
 - The more that users understand about their privacy and the risks, the less likely they are to carry out the transaction. So is the pragmatic lesson for an IT company to downplay privacy? And maybe spend the money on PR instead? Does this mean there is an incentive to "design for perception not reality"?
 - Because there are different meanings of the word "trust", the focus should be on "trustworthy".
 - And would the same cross-jurisdictional approaches work to support the other democratic values noted here?

2. Are there economic, social, and legislative or regulatory initiatives that may help in this effort?

- Business perspective
 - Issues of business compliance with diverse regimes and regulations.
 - Need clear rules and principles around privacy, a stable environment that works well for business.
 - Consistency of rules and principles across boundaries would be useful.
 - Part of the challenge is to provide an incentive to innovation in privacy-enhancing technologies (PETS) in line with how data protection law is framed.
- Jurisdictional and political economy perspective
 - EU should be able to achieve competitive and economic advantage in this area.
 - Need to compile a list of all existing legislation/regulations and consider the national and sub-national levels.
- Citizen/consumer perspective
 - Regarding the ability to "delete" data, we need systems that forget (more akin to human memory). Every piece of data should have an expiry date and self-delete when reached; maybe we should have the right to delete?
 - Psychology plays a big role.
 - Need clear "SLA of citizen/consumer rights" around trust.
- Complexity of issues spanning political, technical, social boundaries
 - Legislation is out of step with technology, a more agnostic approach is required (based around principles rather than specific technologies). The law

should not be prescriptive about specific technologies, but it should help spell out or support the best principles to be applied.

- Factor in the role of privacy impact assessments (PIAs) and data subject perception (about lower level risks being discounted for example). What is the degree of compulsion around PIAs, and where in the data lifecycle do they exist?
 - Technical standards (ETSI etc) can have quite a similar effect as legislation/statutes.
 - Data is growing in value to the systems operators (much richer, more detailed, more pervasive).
3. Other: In thinking about other Working Groups of the Trust in Digital Life initiative, use cases need to take account of regulatory issues (e.g., law and enforcement requirements).