

**ENISA**  
**4<sup>th</sup> Summer School on NIS'11**  
**Deploying Privacy and Trust**  
**in Operational Environments**

**Jacques Bus**  
**SnT – Univ Luxembourg**

**30 June 2011, Heraklion**

# Role of Trust and Security in Society

*Trust pervades daily life. If we take only a small sample from the bewildering array of occasions where trust plays a role, we can see that, of all social phenomena, it is surely one of the most vital. But this very centrality brings problems for the study of trust. How can one even begin to understand such a protean social force? (Kieron O'Hara in **Trust: From Socrates to Spin**)*

Complex systems, self-organisation, dynamic local feedback control (Prigogine e.a.)

- The future is not given but under perpetual construction due to self-organisation, self-learning and dynamic local feedback control loops in the complex system "society".
- Human communication is a flow of correlations ordered in time, leading to better understanding and self-organisation.
- The Internet/Web (Digital Environment) is a complex tool for society in the process of further self-organisaton.

**Security and Trust are essential drivers in the process of societal self-organisation**

# Trust and Security

- Security (safety) of people and societies is essential for humankind
- Trust is a peaceful mechanism to create a feeling of security.  
*(Feeling secure in a context means trusting the context in some way. But of course it could be wrong to trust.)*
- We need trust to implement a transaction or relation.
- Trust can be there: naturally or naively, not at all, to be build up through introduction or through contract or law information,
- Trust can be **rational**, **intuitive** or **irrational**



# Trust and Trustworthiness

**Luhmann** sees trust as a mechanism to reduce complexity in one's life (to cope with uncertainty).

**Nissenbaum** discusses trust only between persons and distinguishes the following factors to which it is responsive:

1. History and reputation (learning from experience)
2. Inferences based on personal characteristics (virtue, loyalty, behaviour, clothing, ..)
3. Relationships (mutuality, reciprocity, family, common goals, colleagues)
4. Role fulfillment (docter, pilot, bus driver, ...)
5. Context (group, community, social norms, law and punishment, insurance)

At least three factors create differences **on the Web** in assessment of Trust

1. Missing Identities (but note the right to anonimity)
2. Missing personal characateristics (but note the right to privacy)
3. Inscrutable, perplexing, confusing, obscure contexts (gives freedom too)

Note it is not black/white. Factors are normally built up in a trust relation.

# Trust and Trustworthiness

**Hardin:** trust is in cognitive category with knowledge and belief.

**O'Hara:** uses "belief" as an important aspect:

1. Y is Trustworthy (in T)  $\equiv$  Tw(Y, Z, R, T)  $\equiv$  Y's behaviour within context T confirms to representation R published by accredited agent Z
  2. X trusts Y (in T)  $\equiv$  Tr(X, Y, Z, R, T)  $\equiv$  X believes Tw(Y, Z, R, T).
- Trustworthiness can be verified ex-post, but trust is an ex-ante belief. Trust is therefore (if rational) based on learning.
  - Tw is not 0 or 1, nor is it measurable, but it can be compared (X trusts Y more than Y' in T).
  - Tr is not measurable, nor symmetric or transitive in X and Y.

# Trusting Technology

Following O'Hara's formulation we may say:

Technology is trustworthy if its behaviour within a given context is in conformity with its representation as published by the accredited agent (e.g. the specs published by the supplier).

E.g. secure, robust, reliable and compliant with regulation.

Some examples:

- UK introduction of ID card
- NL introduction of fingerprints on passport



# Trusting Technology – the Problem

Agent Z introduces a biometric identification system Y, extensively tested in the context T by a high reputation company against specifications R, which are developed according to state of the art (PbD).

So  $Tw(Y, Z, R, T)$  seems reasonable to believe for citizen X, hence:

(1)  $Tr(X, Y, Z, R, T) \equiv X \text{ believes } Tw(Y, Z, R, T)$

BUT: this does not necessarily (not even likely) mean in reality:

(2) “X trusts the biometric ID system Y” in the normal semantic meaning

This could be for many reasons. For ex. X feels:

- Gov has no right to take her fingerprints and shows to distrust her
- Gov has not specified good enough security and X fears ID theft
- Gov uses always function creep techniques and she fears next step
- Gov uses its power position to push a system on X that X considers not beneficial for her and for society

# Trusting Technology – the Problem

The reason for this perceived paradox is in fact simple:

- In moving from statements (1) to (2) we changed the context  $T$  into  $T' \supset T$ .
- $T'$  includes  $X$ 's general beliefs on government, its norms in this context, worries on society and on financial security, ...
- The representation  $R$  does not cover these additional elements and hence gives insufficient information to judge  $Y$  on  $T'$
- The Agent, being the supplier, or even the Gov as designer of requirements, is not always considered trustworthy on such societal or personal issues.

**With the same words we moved in fact from the deterministic technology realm into the complex societal realm**

# Trusting which Technology?

What about the system Y

- More and more complex
- More and more opaque
- More and more interacting with other systems
- More and more invisible and intangible



Hence:

- Impossible to define properly the system that we want to assess on its trustworthiness
- Better to talk about the overall Internet/Web (or ICT) infrastructure – or “the Cloud” in a broad sense

# Trusting Technology - Complexity

Summarizing:

In the daily discussion on Trusting Technology:

- Y: the technology, is often a complex system (the Cloud, ..)
- T: the context extends to the complexity of our life
- R: the representation cannot cover or model T reasonably
- Z: the Agent(s) must have credibility in Y and T and a good reputation on their representations (transparency, accountability)

Moreover:

- The belief of X in  $T_w(Y, Z, R, T)$  might change over time due to learning

# Trusting Technology – Deployment(1)

How to deal with it:

- Ensure transparency, accountability and open discussion from the start (Trust by Design)
- Think in terms of **Ecosystem**, but develop sector-dependent tools and systems first, and link later.
- Develop Trust Platforms per sector, with its trust marks, certification, reputation system, and governance including all stakeholders (e.g. for ID/claim Providers, CAB Forum, Social Networks?, .. )
- Take into account normative systems and social organisation through compliance with existing law, institutions etc. E.g.
  - DP and Privacy regulation/law
  - Liability law
  - Consumer protection law
  - Contract law

But realise the jurisdictional differences

# Trusting Technology – Deployment (2)

- Develop tools and interfaces that focus on the effect and the results for the users, with an understandable, meaningful, but limited set of controls, to stimulate self-learning
- Try to make tools to understand user behaviour and develop “social trust” measures (statistical distribution functions, expressing use, acceptance, perception of security and privacy protection?)
- Summarizing: facilitate the social self-organising process

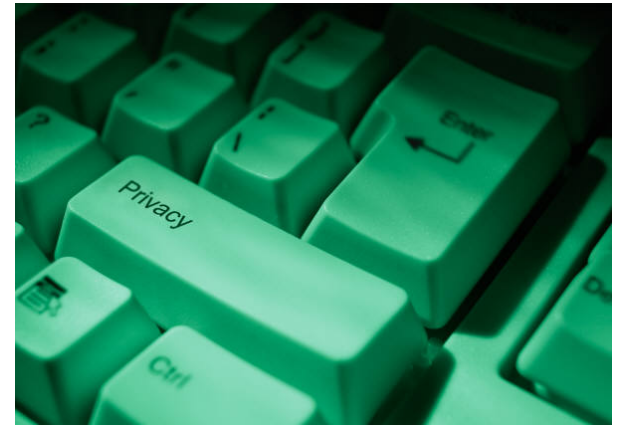
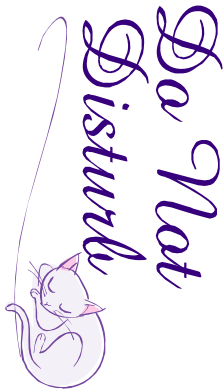


# Privacy

- *“A free man will let the Rain, the Wind and the Sun freely in his house. But the King of England must ask permission to enter.”* (from an old English poem)
- *“Privacy is about what is not covered by other civil liberties”* (Paul de Hert)

**Privacy is on keeping power in society in check.  
The Citizen/Consumer vs  
the State and the Multi-national Enterprise**

- *“Privacy cannot and should not be precisely defined – definition would kill it”* (Seda Guerses)



# Privacy

**Allen** considers:

- physical privacy (seclusion, solitude);
- informational privacy (confidentiality, secrecy, data protection and control over PI)
- proprietary privacy (control over names, likeliness and repositories of PI)

Three dimensions: spatial, informational and relational.

Approach: (1) Secrecy/anonymity; (2) Control/ID mgt; (3) Practices;

**Nissenbaum:** A framework for privacy as “Contextual Integrity of Information”, emphasising the essential contextual and normative character of privacy.

**Q:** How to consider context and norm/cultural dependency in technical privacy systems?

# Privacy – Social issues

- Strongly culturally linked (normative)
- Enabled by security and trust
- Benefits individual's freedom
- Benefits society: freedom of speech, democracy, creativity, innovation, economic prosperity
- Reflects the social power (im)balance

- Paradox of freedom:  
*more security -> less freedom/privacy or v.v.*

Wrong in general  
see Solove, *Nothing to Hide*



# Privacy – a Model

Nissenbaum, *Contextual Integrity of Information*

- Emphasises the contextual and normative character (hence the complexity of the concept)
- Three dimensions:
  - Actor: government and private
  - Realm: public space, private space (privatised space – see O’Hara & Shadbolt, *The spy in the coffee machine*)
  - Information: public and personal

Context-relative informational norms characterised by:

Context, actor, attribute and transmission principles

Any IS that is designed must be analysed on these parameters.

**Privacy can not simply be achieved by general rigid legal rules on processing and protection of “personal data”.**

# Privacy – Legal approach

Legal perspective of privacy is for a large part focused on regulating the way personal data can be processed, its enforceability and practical applicability.

The Data Protection Framework (Dir 2002/58/EC), e-Privacy Regulation (EC 45/2001) and Council Decision for police and judicial cooperation (2008/977/JHA) gives the EU a strong legal framework.

But it is currently under high pressure.

# Revision of EU Framework – Why?

- Adaptation to Internet and Web world with:
  - Social networks
  - Profiling and targeted advertising
  - Changing view on what is the public space
- Need for better EU-wide harmonisation of MS law
- Impact of Lisbon Treaty
  - EU charter of Fundamental Rights binding in EU, incl. right to protection of personal data (Art. 8); right to respect for private life (Art 7); and Art 16 giving a general legal basis for DP.
- Data protection very relevant for other policy fields (Digital Agenda, eHealth, eGov, eCommerce, trust between MS in exchange sensitive data)

# Revision of EU Framework – How?

- Comprehensive approach (all policy fields: justice and human rights, e-Services, police and judicial cooperation, internal EC rules)
- No reinvention, but more effectiveness of:
  - implementation
  - enforcement of DP principles
  - delivery of data subject's rights,
- Simplification and Harmonisation
- Strengthening the three main roles:
  - Data subject (consent, access, right to “be forgotten” and “data portability)
  - Controller (mandated and being able to demonstrate that the necessary has been done - Accountability, Privacy by Design)
  - Supervisory authority (resources, power and independence)



New framework for dealing with technological change and globalisation, with impact assessment, transparency and accountability, a-priori certification, hence more results-based

**But will this enable representation of the contextual, normative character?**

# Privacy by Design

Developed first by Ann Cavoukian (Privacy Commissioner Ontario, CA)

Based on seven foundational principles:

- Data minimisation
- Individual participation
- Security
- Accountability
- Pro-activity and prevention
- Embedded in design of systems and products
- Full functionality and application of “Fair Information Practices”

There are three methods to improve Privacy by regulation

- Specifying requirements a-priori for system design and life cycle (Technology approach)
- Ex-post evaluation of outcomes rather than process (Consumer protection)
- Mandating State-of-the-Art technology and Compliance (Supplier liability)

All three have problems, all three are needed

# Identity

## Davis: 3 concepts

- Metaphysical identity: what are the essential qualities of a person that makes him unique
- Physical identity: the carrier in flesh and blood of all the roles and qualities
- Epistemological identity: created by relations to institutions; or existing because of various practices connected to our culture, language, ...
- We can also talk about multiple (partial) identities, if we consider every creation of a relation or existence of practice. Together they form the epistemological identity.
- An ID in a certain context is a particular set of credentials (attributes or claims), called a partial ID

## FIDIS distinguishes:

- the structural perspective (ID as set of attributes)
- process perspective (ID as set of processes of disclosure and usage of ID data; **authentication**)



# Identity and Authentication

## Ongoing work

Kim Cameron (Identityblog) gives his “7 Laws of Identity”

1. User Control and consent
2. Minimal disclosure for constrained use
3. Justifiable Parties
4. Directed Identity
5. Pluralism of Operators and Technologies
6. Human integration
7. Consistent Experience across Contexts

Cameron, Posch & Rannenber g gave a Proposal for a Common Identity Framework: A user-Centric Metasystem (Identityblog), based on these laws , published on Identityblog and in FIDIS book.

An EU funded IP: ABC4TRUST works since last year on bringing two minimal disclosure technologies (U-Prove-MS and IDEMIX-IBM) together in one open platform

STORK, and other EU projects in the Competitiveness Programme, work on interoperability between Member State ID cards, digital signatures, exchange of documents, etc.

# Literature (1)

- Antoniou, Reeves & Stenning – *The Networked Society* (2000)
- Cameron, Posch, and Rannenbergh - *Proposal for a Common Identity Framework: A user-centric Identity Metasystem* - [www.identityblog.com](http://www.identityblog.com) (2009)
- FIDIS project: <http://www.fidis.net> (2009)
- Frank – *25 Jahre Fachgebiet Mess and Regelungstechnik, Mercator Un. Duisburg* (2001)
- Fukuyama – *Trust: The social virtues and the creation of prosperity* (1995)
- Hardin - *Trust and trustworthiness*; Russell Sage Foundation, NY(2002)
- Langton – *Computation at the edge of chaos*, Physica D (1990)
- Luhmann - *Trust: A mechanism for the reduction of Social Complexity* – in: TRUST and Power (1979)
- Nissenbaum - *Securing Trust Online: Wisdom or oxymoron?* (2001)
  - *Privacy in Context – Technology, Policy and the Integrity of Social Life*, Stanford (2010)
- O'Hara, K. (2004) *Trust: From Socrates to Spin*, Icon Books, Cambridge
  - *A general definition of Trust*, Working Paper (2009)
- Prigogine - *The end of Certainty*, Free Press (1996)
  - *The Networked Society*, Jo World Systems Res (2000)
  - *Norbert Wiener and the idea of contingency*, Kybernetes (2000)
  - *Is Future given*, NTUA (2001)
- Prigogine and Antoniou – *Science, Evolution and Complexity* (2001)
- Putnam - *Making democracy work: Civic traditions in modern Italy* (1993)

# Literature (2)

- Shadbolt & O'Hara – *The spy in the coffee machine*, One World (2008)
- Solove – *Nothing to hide*, Yale (2011)
- Tetlow – *The Webs Awake*, IEEE Press (2007)
- Toure & PMP InfoSec WFS – *The Quest for Cyber Peace*, ITU (2011)
- Trust Guide - <http://www.trustguide.org.uk/>