

Balancing Security and Privacy in eGovernment Services

Kieran Sullivan and James Clarke

Waterford Institute of Technology

Telecommunications Software and Systems Group

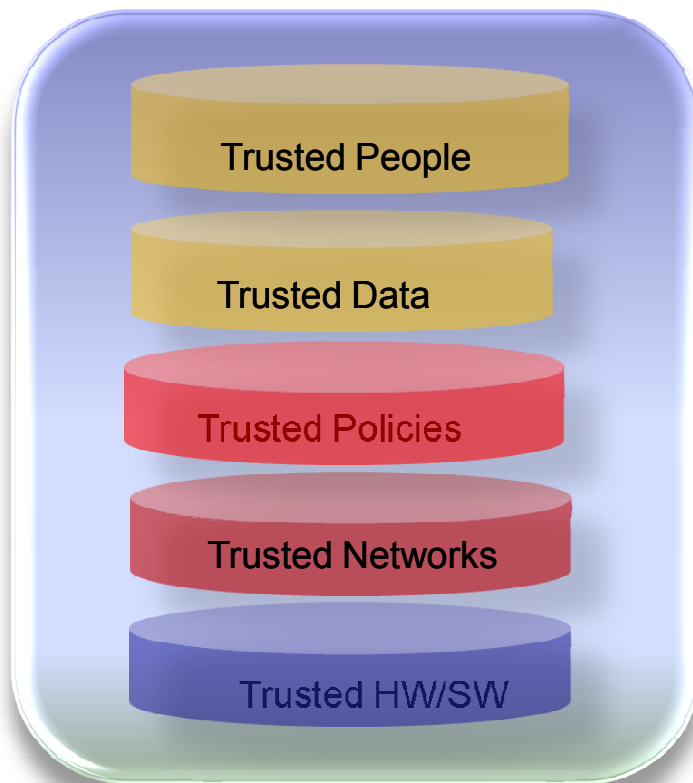
Ireland



- Connected World, Connected Exposure
- The value of digital possessions may soon exceed that of material ones - for individuals, businesses & Governments



Trust = Security + Privacy + Usability + Reliability + Governance +...



- **Trust is an end-to-end attribute**
 - **Computing**
 - **Communications**
 - **Data storage**

- **Cyberattacks target the entire trust chain (*users, blocks, interfaces & technology*) for the “weakest link” ... and the trust chain is global !**
 - **for the problems & solutions**
 - **for governance & enforcement**
 - **for co-operation!**

- Current drivers of security and privacy research in the area of eGovernment services include:
 - increasing **volume** of transactions, and even higher volume of traffic;
 - increasing **mobility** of users (physical or virtual), seeking either continuous (mobile) or intermittent (nomadic) connection and access;
 - large growth of sensors and slave-labour devices (**Internet of Things**), taking over the management of routine operations;
 - **convergence** of types: voice, visual, entertainment, social and business services. (For example, twitter.gov, and 'official' blogs);
 - increased, **heterogeneous accessibility** to converged information and services.



- Anonymity “versus” Accountability
 - *Anonymity*: absence of identifying information associated with an interaction;
 - *Accountability*: action is accountable if it can be attributed to someone (or something – such as a service provider);
 - Both characteristics must exist side-by-side in the on-line environment;
 - Neither is enough on its own; nor should any person or business have to choose only one or the other.



- To facilitate on-line accountability, two options seem promising:
 - Base the demand for traceability and accountability on global accountancy-type principles, which can encompass all networks, such that reliable and almost exhaustive incoming and outgoing accounts can be drawn up.
 - Reintroduce, on a lower network layer, a “territorialisation” of data and participating parties [1].

[1] Think-Trust EU-IST FP7 Coordination Action Project (2009) ‘Deliverable D3.1-A Recommendations Report (Interim)’.

See also **Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society** (RISEPTIS) Advisory Board Report, Oct. 2009. [available at <http://www.think-trust.eu/riseptis.html>]



- **Use cases:**

Case 1: Alice is a student who puts up an anonymous web site with allegations that the President is a disgrace to the nation because he secretly disfavours a particular nation.

Case 2: Alice is a student who puts up an anonymous web site with allegations that the President is a disgrace to the nation because he takes money for allotment of government positions.

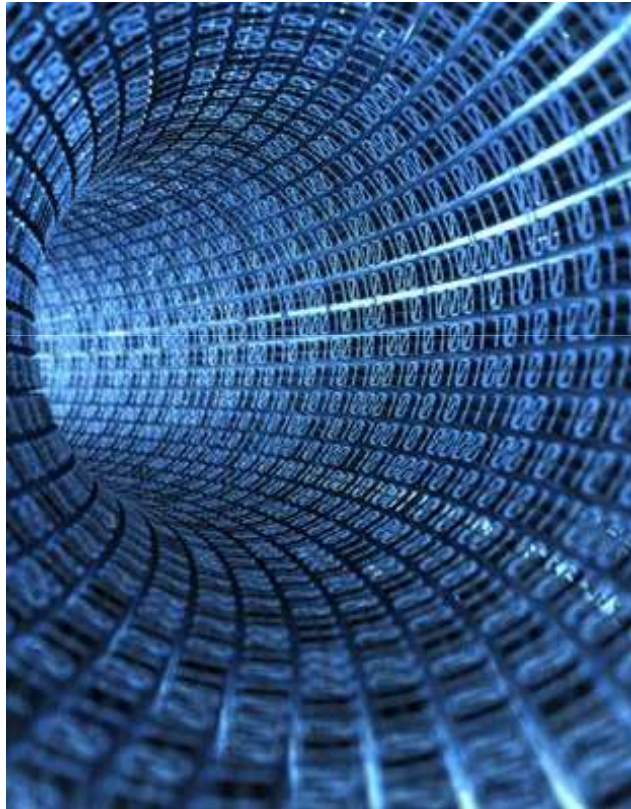
Case 1 is surely worth anonymous protection, but Case 2 adds weight to the belief that there should be increased accountability on the Internet.



- *The potential for abuse of power by traceability-seeking governments/administrators is much greater than that of an unidentified “ranting” user.*
- *Thus, the balance between anonymity and accountability should be weighted on the side of the user’s anonymity.*
- *Implies that the ability to remain anonymous in certain contexts should, therefore, be built into eGovernment services.*
- *With such a solid building block in place, the mechanisms to ensure accountability can then be pursued.*

- Assuring privacy and the protection of citizens' data must be a fabric of eGovernment services,
 - Without negatively impacting on the general public interest; the interests of involved parties; or any legal and contractual obligations.
- Protection of personal data is one of the most important aspects of privacy;
- Trustworthiness and accountability of the relevant data controllers are therefore of crucial importance, since much personal data will be under their control;
- Technology support in this process is essential, so as to provide the necessary knowledge and tools to the data subject to exercise his/her options, including the ability to act anonymously;
- ...and to ensure transparency and accountability of the data controller towards the data subject to enable assessment of trustworthiness.

- Core IT Abstraction → Data ... for services & for attacks!

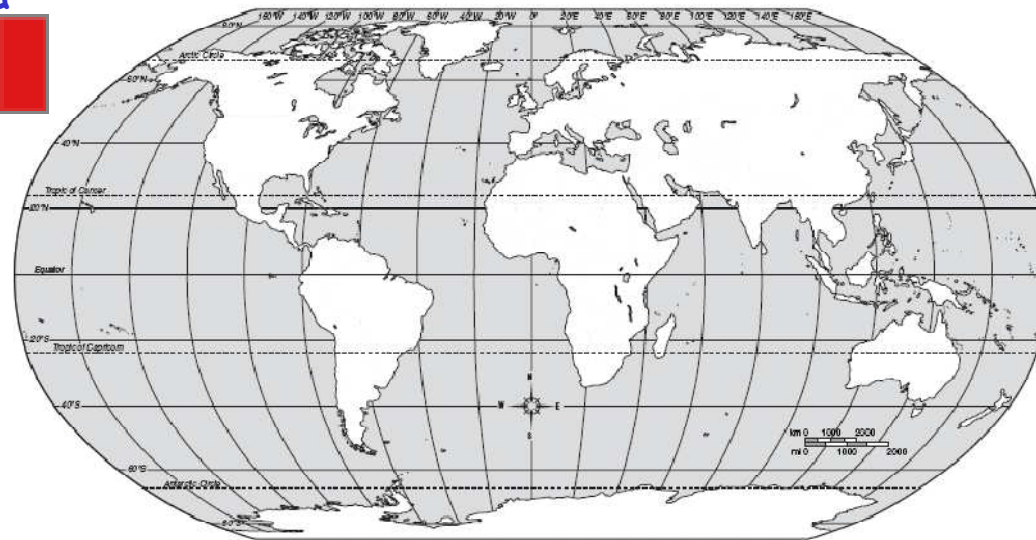
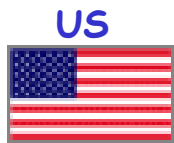


- The information society runs on data!
- .. and data doesn't really come with borders

- The “Data” Elements
 - Data Acquisition
 - Data Dissemination
 - Data Storage
 - Data Management/Usage

	FP6	FP7
Biometrics		
Privacy, identity		
Network		
Services		
Secure Implementation		
Trusted Computing		
Coordination Action		

INCO-TRUST: Intl Co-operation in Trustworthy, Secure & Dependable Infrastructures



Brazil



India



S. Africa

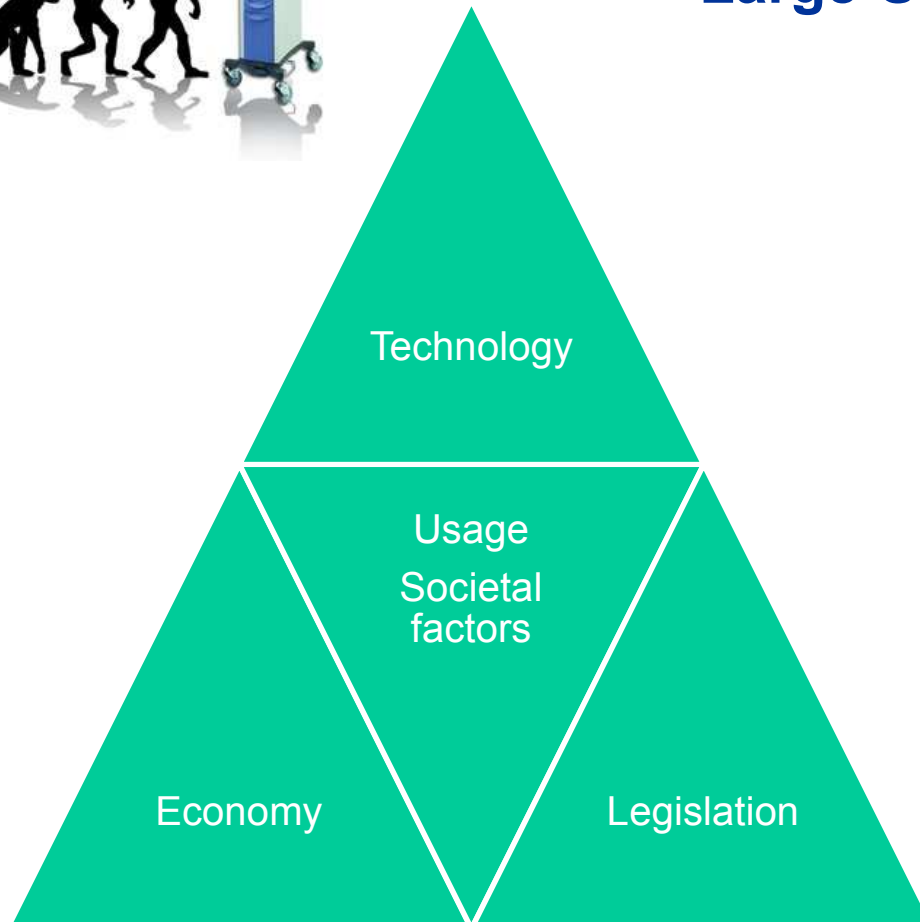
INCO-TRUST

www.inco-trust.eu





WG1: Dependability and Security of Future Large-Scale Networked systems



- ❑ **FOUNDATIONS** – Key enabling technologies, new computation/communication models, crypto models, trust architectures, ...
- ❑ **NETWORKS/SERVICES INFRASTRUCTURE ISSUES** – TSD relevant network/services issues in the Future Internet.
- ❑ **CONTENT** – TSD challenges in data acquisition, dissemination, access and storage.

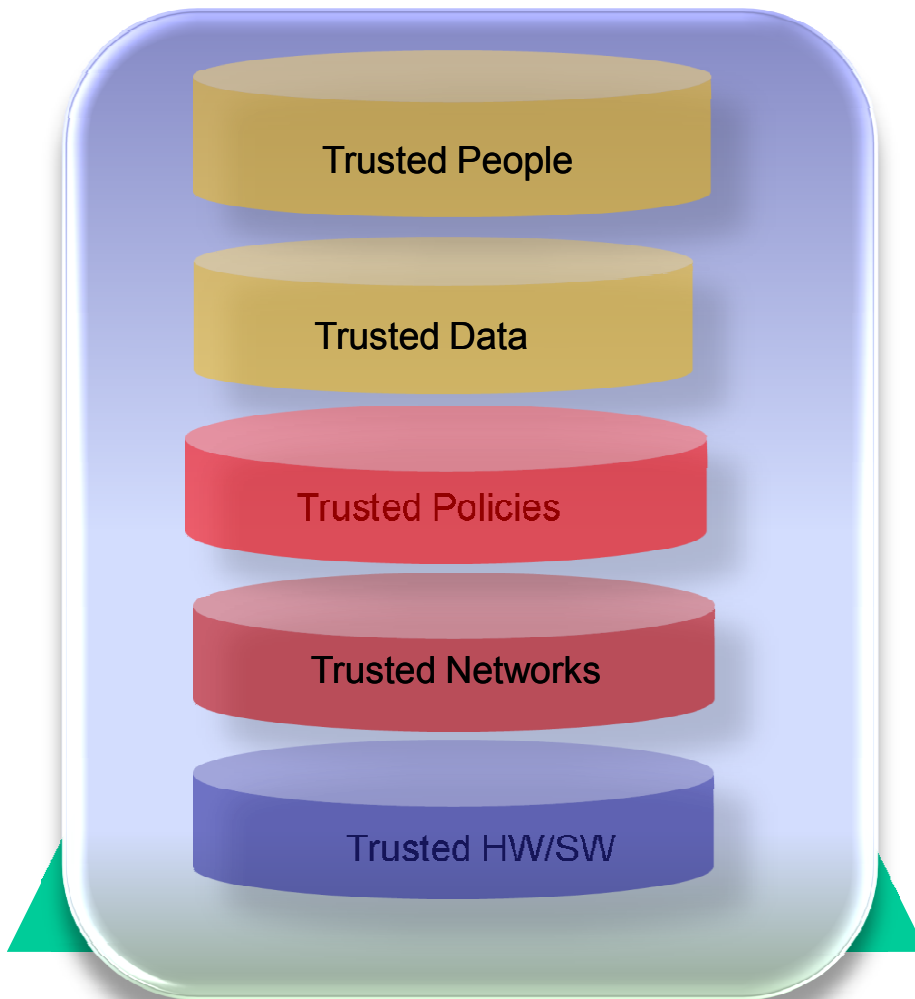


WG2: Privacy and Trust in the Information Society

- ❑ **IDENTITY PROVISION & MGMT**
Physical, virtual, service, session, device ID's; ID mgmt issues: who/what/where/when/how?

- ❑ **INTERPLAY OF SECURITY & PRIVACY** - E2E Trust-Privacy-Security Envelope, Quantification of Trust-Privacy-Security? Tradeoffs?

- ❑ **INFO ACCOUNTABILITY** Appropriate Use, Access Control, Traceability, Governance, Liability, Compliance...



- Please visit
 - <http://www.think-trust.eu>
 - <http://www.inco-trust.eu>
- Public deliverables available
 - <http://www.think-trust.eu/public-documentation/think-trust-documents.html>
 - <http://www.inco-trust.eu/incotrust/general/project-impact.html>
- For Think-Trust, contact Kieran Sullivan <ksullivan@tssg.org>
- For INCO-TRUST, contact James Clarke <jclarke@tssg.org>
- Projects funded by the European Commission, Unit "Trust and Security" (F5) [http://cordis.europa.eu/fp7/ict/security/home_en.html]