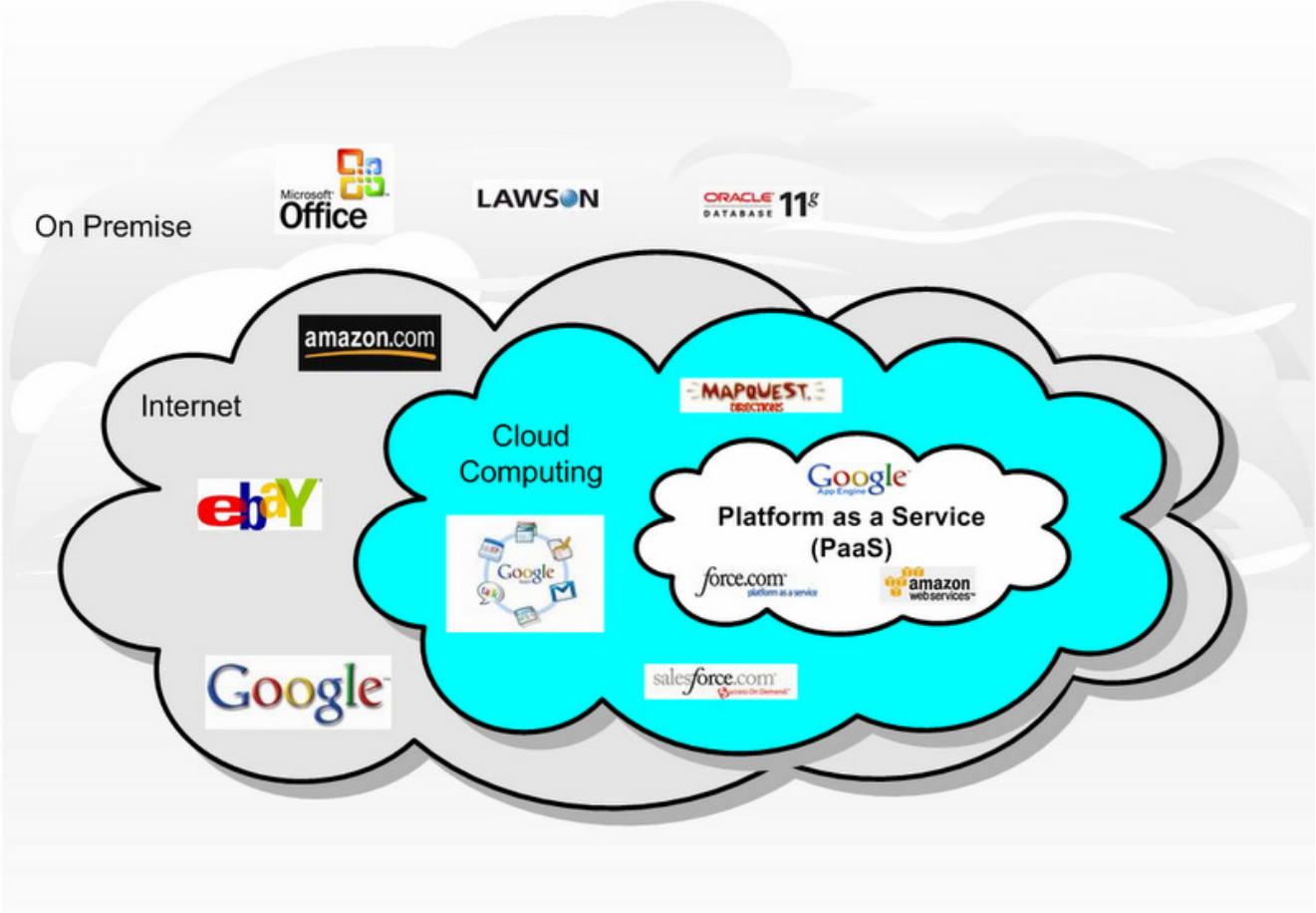
Trustworthiness and the Cloud

Neeraj Suri & James Clarke

Dept. of Computer Science
TU Darmstadt, Germany
&
Waterford Institute of Technology, Ireland

Clouds, Clouds and Clouds



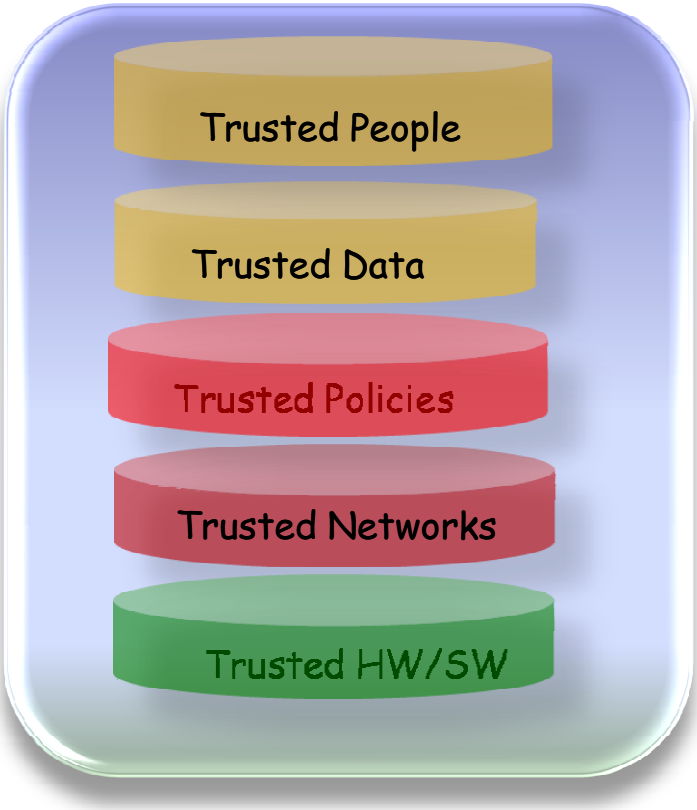
+ Transparent, Adaptable, Global – anytime, anywhere access. Immersive Computing
- BUT, your data is up "there" – security, privacy issues galore!
- Clouds also fail….Remember the Amazon Cloud disruption from 2 weeks back?

Outline

- Trustworthiness in the Cloud
  - Let's start at the beginning with the Trust Elements
  - Let's go technology agnostic for services (Cloud or whatever) – for the end to end services that drive the Cloud/Internet/+++ to develop a data level outlook
  - …and then address the Cloud issues

We use technologies (Cloud and the whole spectrum of devices, infrastructures and services) because we are willing to trust them to deliver the services we expect from them irrespective of the disruptions (design, operational or deliberate) encountered by them. This basis of trustworthiness defines their value or the lack thereof!

Trust ➔ Security + Privacy + Dependability



- Trust is an end-to-end attribute
- Trust is not a piecemeal property. Cyber attacks target the entire trust chain (the blocks, the interfaces and technology changes) for the "weakest link" vulnerabilities on the overall attack surface
- Most e-services are likely networked (in either obvious or non-obvious ways) via the internet/clouds…

…and the blocks/infrastructures/services are international!

Google reports China-based attack, says pullout possible

By **Jeanne Meserve and Mike M. Ahlers**, CNN
January 12, 2010 10:56 p.m. EST

Google reported Tuesday an alleged attack on its US corporate infrastructure last month originating in China.

STORY HIGHLIGHTS

- Google says an attack originating from China targeted its US infrastructure
- The attack occurred last month and targeted Chinese human rights activists, the company said
- Google says 20 other companies were also targeted

WASHINGTON (CNN) -- Google said Tuesday the company and at least 20 others were victims of a "highly sophisticated and targeted attack" originating in China in mid-December, evidently to gain access to the e-mail accounts of Chinese human rights activists.

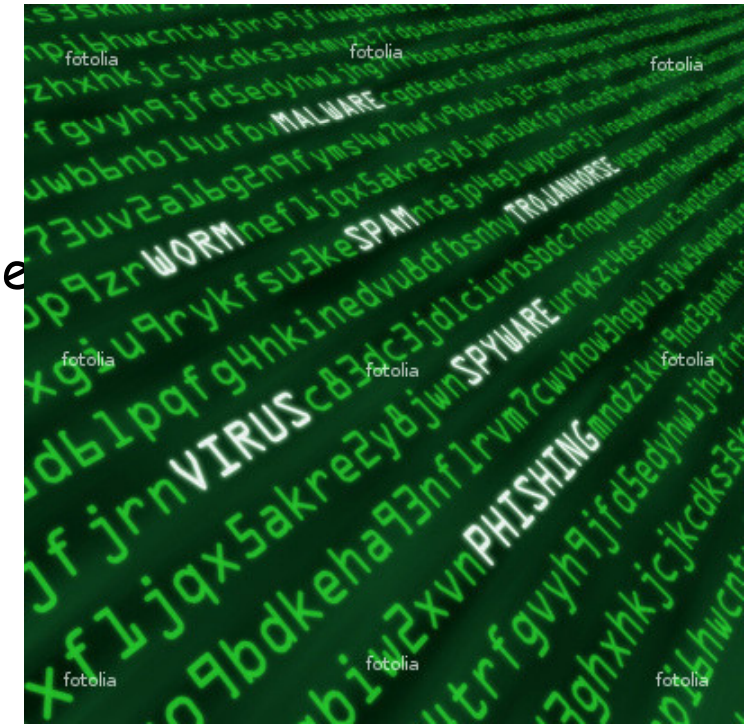
"Based on our investigation to date we believe their attack did not achieve that objective," according to a statement by David Drummond, senior vice president of corporate development and chief legal officer for Google, operator of the most popular Internet search engine.

Clouds: End-to-End Trust and the Focus on Data

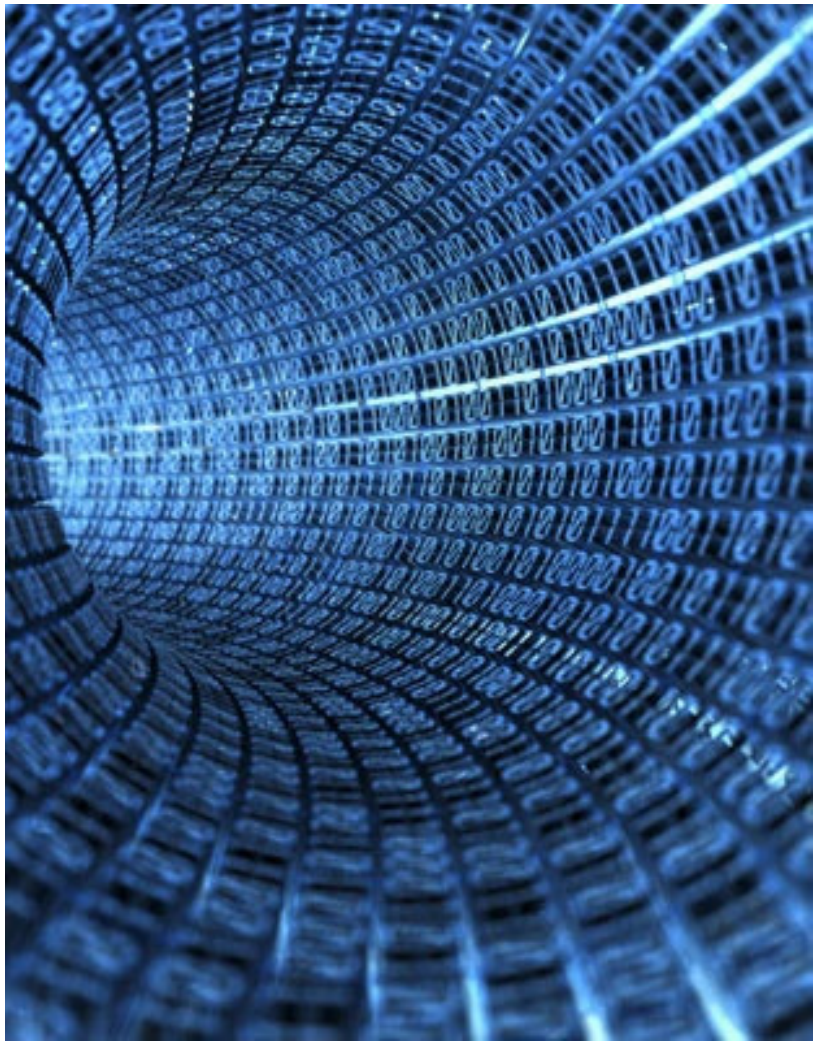
- System evolve and will and continue doing so.
  The key issue is to identify the operational "structures" such as the building blocks/interfaces to develop coherent, domain + technology invariant solutions.

- The information society runs on data!

  The "data" perspective (and related attack surfaces) for services forms the key (& invariant) abstraction behind trusted end-to-end services!

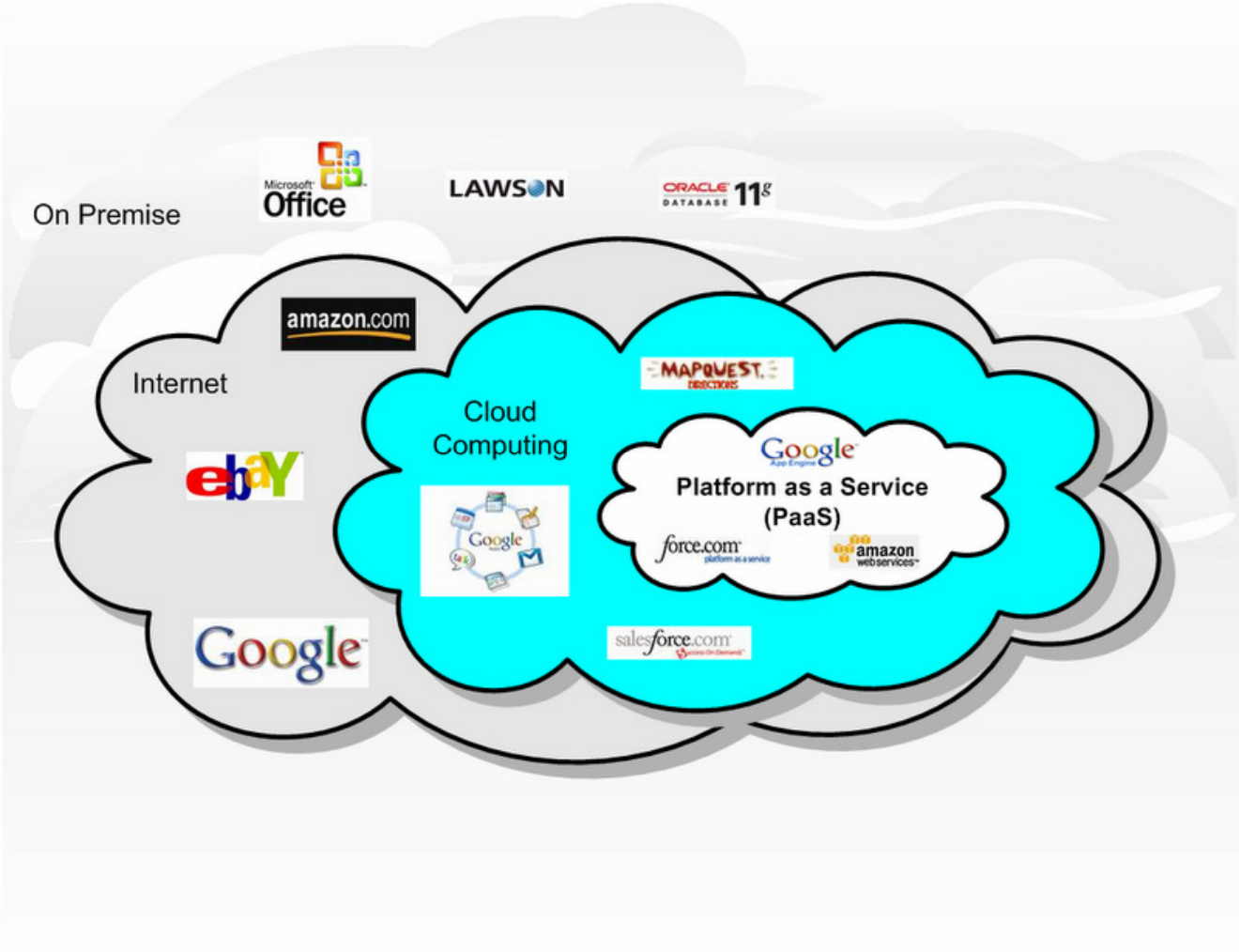


Clouds ➔Data Chain Over Global Resources



- The "Data" Elements
  - Data Acquisition
  - Data Dissemination
  - Data Storage
  - Data Management/Usage

Clouds: Data Access, Dissemination, Storage & Usage

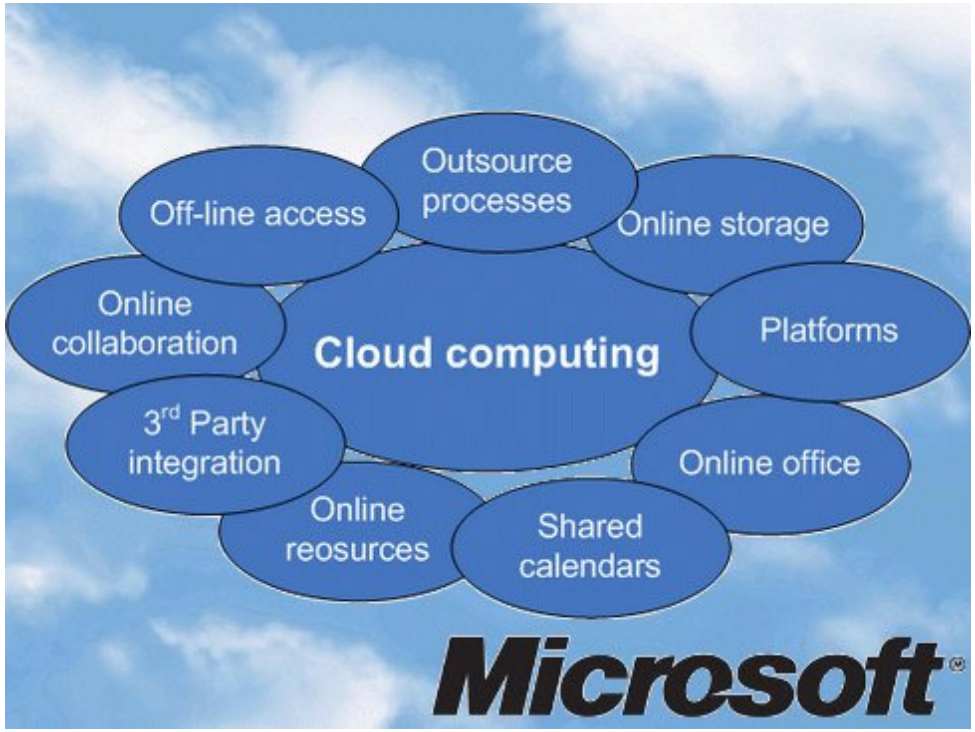


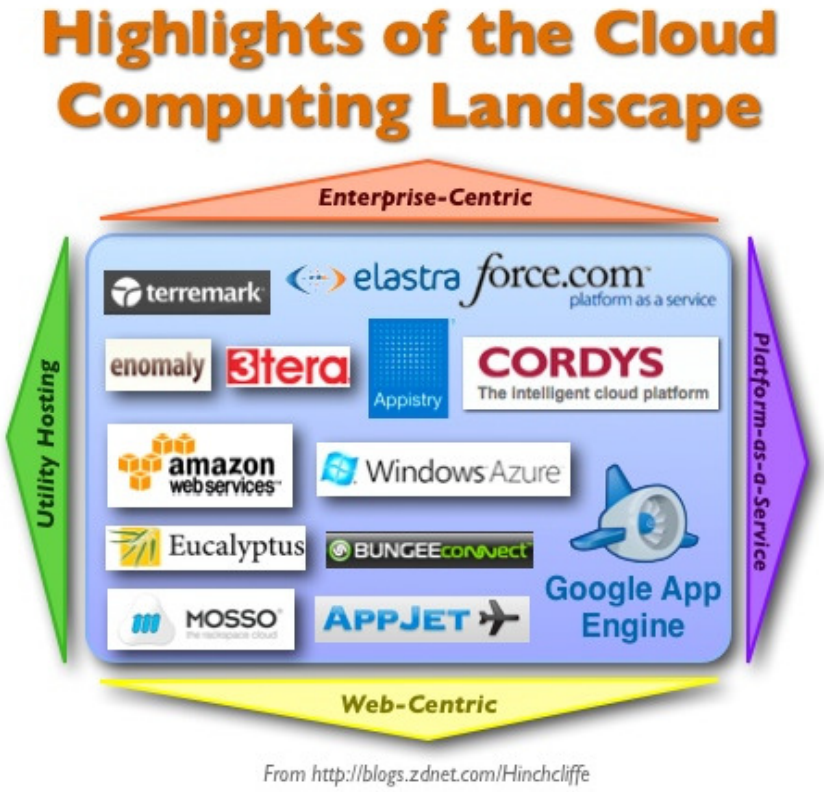
Example: Data Dissemination

- Does one know or control which network is being used?
- What are the SLA's?
  - Who is liable for a network/data breach along an intl. chain?
  - …assuming a user even has an idea what the network chain is
- What are the interfaces and access control policies across the networks, from devices (mobile) to backend etc?
- What are the monitoring policies? [country dependent?]

❖ Networks might be diverse & changing though the common monitoring/control elements related to account/pricing tracking often form the weak point!

Spectrum of Cloud Functionality is the Worrisome Part!





Data Servers, Storage & The Human Element

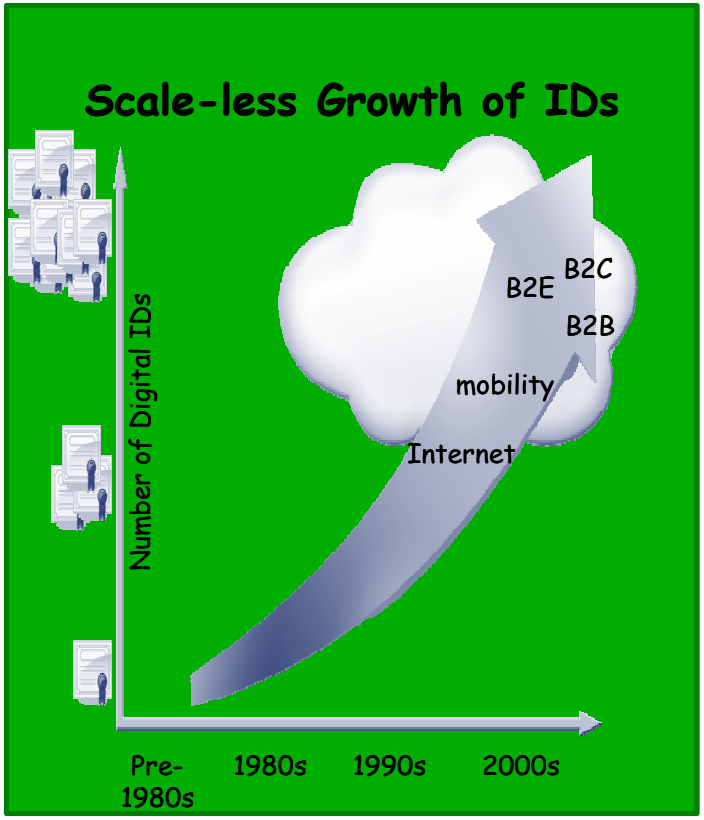
- Services and servers are no longer monolithic or local … global, collaborative computing, P2P, Cloud…
- Data Servers are located worldwide - Google Data Centers
  - For a security breach on the data, who is liable? The data center locale? The owner of the data center? The network?
  - Bangalore Case: Secure Data Servers but data sold by employee

The Big "Data" Issue in Clouds: Accountability?

- At what level & by what "trusted" authority ?
- For networks? For services/apps?
- Data – ownership, digital rights
  - Traceability?
  - Browsing data?
  - Account data patterns for trend analysis?
  - Data longevity?
  - Legal ownership & rights?
  - Liability? Governance? Compliance?

- Data Acquisition
- Data Dissemination
- Data Storage
- Data Access

Data ➔ Identity: Provision & Management



- **Physical/Real ID, Virtual ID, Service-Device-Session ID …**
- **ID: Scope & Rights**
  - Individual/Collective/Business
  - Unique? Link to Physical ID?
  - Acquired, transferred…
  - Regulated
  - Authenticated
  - Hierarchical
  - Permanence
  - Scalable?

- Who manages the mgmt, & mgmt of what ID? Policies?
- How?
- What are the controls (and their accountability)?
- Is there any globally conformal and attributable identity?

The Privacy & Security Interplay

- Multi-cultural/national nuances! The role of technology in trust is also often cultural – what to monitor, how to monitor, who monitors, and issues of data retention…

- **Localized Approaches**: Smart spaces - ID's & authentication? Zero knowledge proofs?

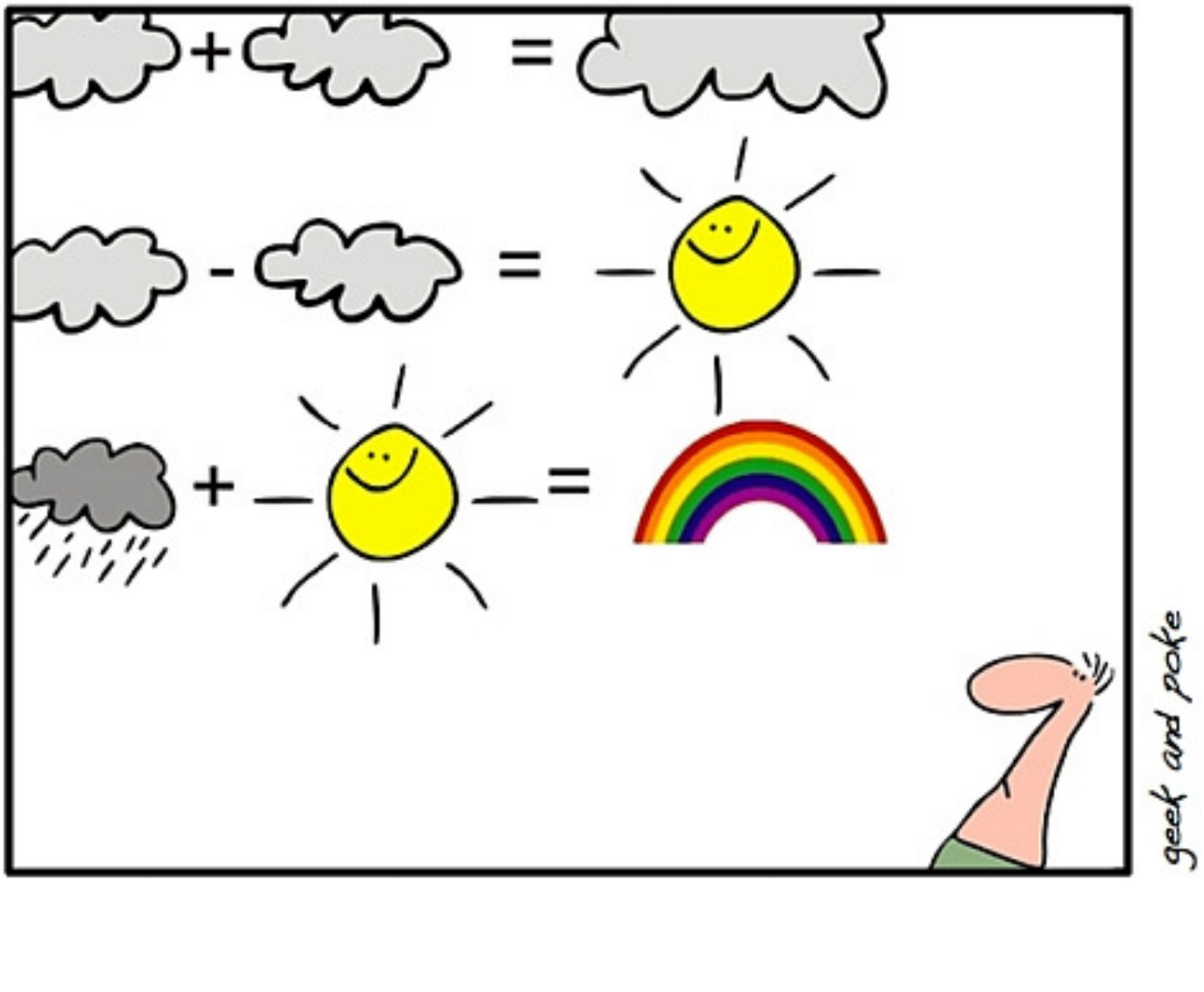
- **E2E Trust-Privacy-Security Envelope:** Measures of privacy? Quantification of Trust-Privacy-Security? Tradeoffs?
  ** Liability and Governance on an international scale?

Social Requirements | **Economic Basis** | **Policies/Political**

The Data Perspective: Common Focus Areas

- While one can come up with many (many many) innovative technological solutions *"your favorite cloud-y approach here"*, do we have a handle on:
  - What constitutes (globally conformal) data ownership and data accountability – individual and institutional?
    - What to monitor, at what level and where – & by who in the intl. chain?
  - What constitutes globally conformal identity?
  - Do we know how to specify and assess trust for liability? quantitatively, reproducibly?
  - What are the quantifiers/metrics of trust (Security & Privacy) based on which one can develop solutions – that are technologically and internationally viable!
    - … and are also invariant to technology changes

So which one is the future?



- www.deeds.informatik.tu-darmstadt.de
- suri@cs.tu-darmstadt.de; jclarke@tssg.org