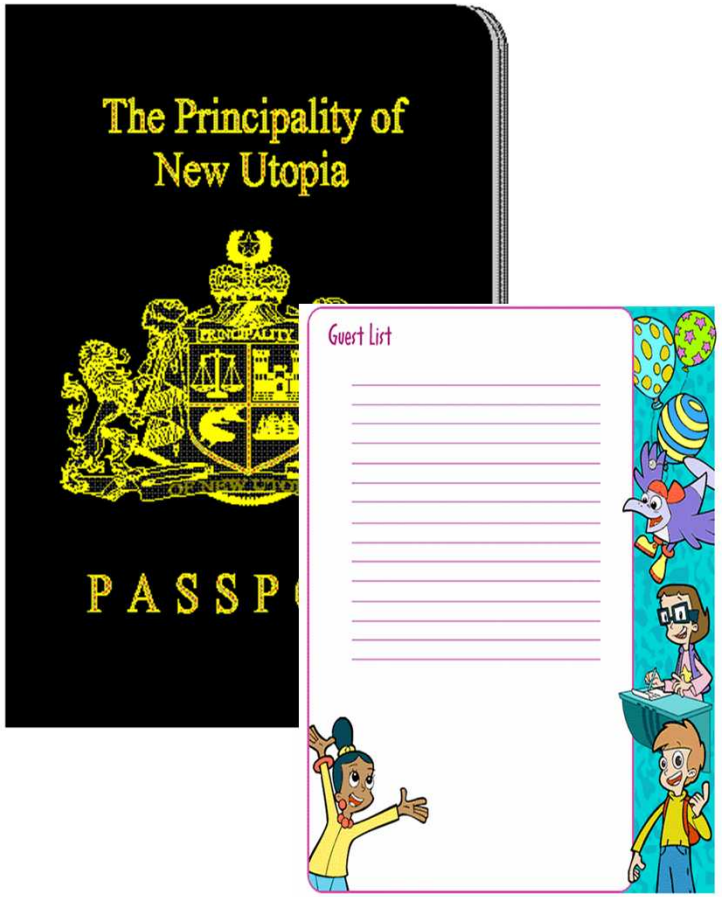
Technical and Legal Challenges of Criminal Law Enforcement in the Digital Age

Rob J Meijer & Mark Zoetekouw

Identity-based VS Authority-based access-control



VS

Authority by designation

“Today I bake, tomorrow I brew, then the Queen's child I shall stew. For nobody knows my little game, for Rumpelstiltskin is my name.”

Authority by designation

- **Rumpelstiltskin**
- **https://docs.google.com/document/d/1XQhosA3NGan2kCBdyp58wdTy9jdI9ZZBXHOCAmC2vGk**
- **https://mega.co.nz/#!RV8C3R7I! dTnm8hpBg_nUOeCmOj2ocEQur8cXsLzK-ChN7yVZ6sP**

Decomposition & Attenuation

- Trunk → Branch ✓
- Branch → Trunk ✗
- Read/write → read-only ✓
- Read-only → read/write ✗

Minor

Tree's and forests

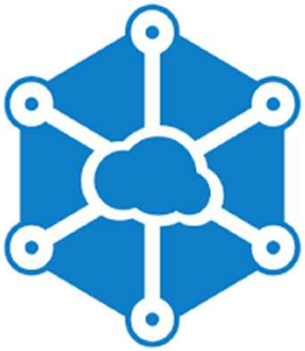
- Cloud storage customer owns a private tree
- Capabilities allow cloud storage customer to delegate a branch !
- Cloud storage provider owns the forest!

Delegation,ownership & seizure?

Separation of confidentiality & availability.

- Tahoe-LAFS: Provider independent security.
- RAIC: Redundant Array of Inexpensive Clouds
- Forest owner can no longer look up into the tree.

Tahoe-LAFS



Distributed @Home

- Blockchain = basis for P2P CSN
- Spare disk-space and bandwidth
- Meta-data in blockchain as TTP
  - Merkle-tree root
  - Erasure encoding

Convergence?

Multi-granular multi-domain provider-independent distributed least authority data storage

(Bad-ass spartan cloud security)

Public order and security

- Safer cloud.
- Lower impact cybercrime.
- Safer world.

Prosecution & Forensics

- No prosecution without proof

- No proof without (access to) data

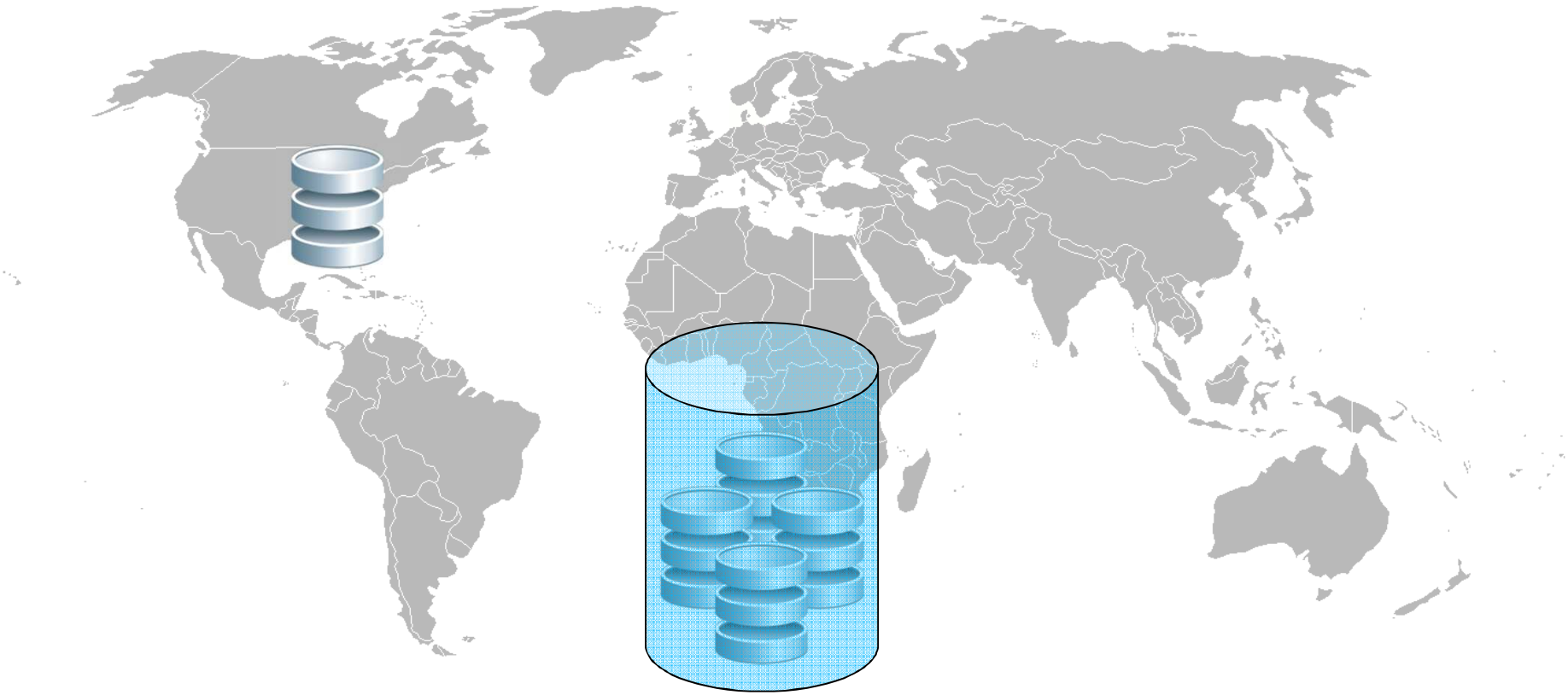
Technical to Legal Challenges

- Data ownership is ambiguous

- Cloud provider can't help (much)

- Entangled systems with multiple stakeholders.

Additional legal challenges



Its here…it's real

(and it's not waiting for us to catch up)

Never mind reading it.

Data cannot even be

located without the key.

Data is cut up in a 100 pieces

Pieces are spread over a 100 servers

In dozens of countries

Over a multitude of hosters

Solutions?

- Legal duty (based on a warrant of course) for third parties (companies) to hand over data locally in countries they offer their services in.
  Lowest sensible level: Europe

- Seizure and acquisition moves back to the client (not the hoster)

  New legal paradigm regarding the ‘location’ of data

Local Availability Duty

- If companies wish to do business inside your jurisdiction they need to be able to produce requested data bases on local warrants

  (as long as they have access to it)

- Lowest sensible level: Europe

The location of data

The traditional way of looking at the location of data.

A new way to look at the location of data.

(Cyber)Sovereignty & Jurisdiction

Cyberspace & traditional notions of Sovereignty and Jurisdiction don't mix well

Either basic Internet Architecture or several deeprooted legal notions and concepts need reconsideration

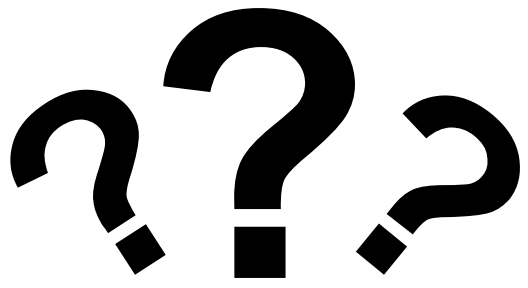
Your take home points (tech)

- Multi-granular multi-domain provider-independent distributed least authority data storage is a problem for forensic research of data **that cannot be solved with technical means.**
  - Data isn't stored locally
  - The 3rd party traditionally approached can't help you any more
  - Data attribution to persons is hard or impossible
  - Data (bits) are shared between many parties
  - (Don't be sloppy with your security tokens – even when you think you are alone or in a safe environment)

Your take home points (legal)

- Technological developments in data storage and cloud computing are exacerbating already existing legal challenges with regards to (location of) data.
- We have to consider making law that if you want to do business (in europe) you are obliged to produce data locally, without need of international legal assistance.
- Instead of looking at “where data lives” we have to consider “where data is accessed” as a legal hook.
- We need to start reconsidering the (standard explanations of) Jurisdiction, Sovereignty and Non-Intervention in the face of Global Cyberspace & Cybercrime

Questions? / About us



mr. M. Zoetekouw
Ph.D. Researcher - Internet and Jurisdiction (UNIJURIS) @ Utrecht University
m.zoetekouw@uu.nl
&
Legal Advisor Cybercrime & Digital Technology @ Dutch National Police
mark.zoetekouw@politie.nl

R.J. Meijer
ICT Specialist Information Security & Digital Forensics @ Dutch National Police
rob@dnpa.nl