Push authorization - the Whitebox model

Surf lightning talk, 22 sept 2020

Guido van ‘t Noordende

Guido van ‘t Noordende
Whitebox Systems | UvA Amsterdam

The research data management problem

Consent allows copying / sharing of data sets with multiple parties

Once obtained, parties claim / assume ownership over data(bases)

Anonymized/pseudonymous data often (easily) re-identifiable

The research data management problem

Consent allows copying / sharing of data sets with multiple parties

Once obtained, parties claim / assume ownership over datasets

Anonymized/pseudonymous data often (easily) re-identifiable

- Downstream recombination of datasets increases this problem
- Transparency: hard to track (downstream) data flows (copies)
- *The problem exacerbates, becomes less tractable – e.g., think of DNA data – ownership of families through multiple generations*

Sharing data in research – a decentralized approach

Goals:

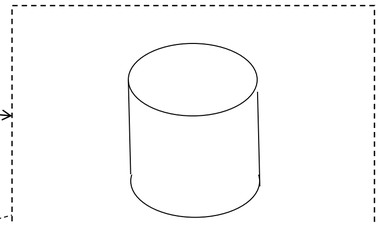
- Separation of responsibilities and concerns
- Control, tracking and tracing throughout data lifecycle
- Allow owner’s policy specification and (immediate) enforcement
- Right to withdraw access
- Up-to-date data, withdraw or change data elements immediately
- Decentralized means a network *around the patient/subject*

Approach:

- Decentralized networks: only legitimately involved parties join
- Extend or scale down network / sever links dynamically

Sharing data in research

Copy



Consumer –
classical view
e.g., works “in the cloud”

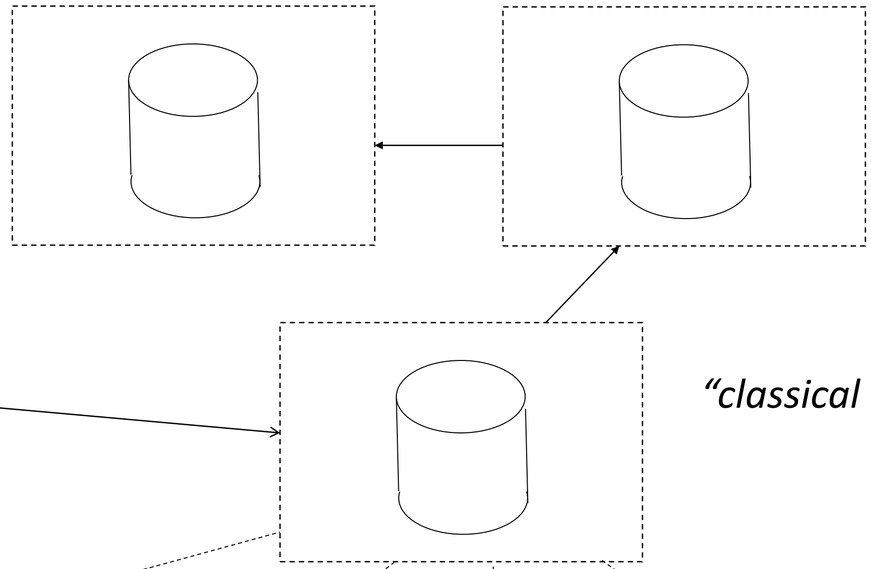
Sharing data in research

Copy

With consent, onward / Downstream copying

“classical view”

Sharing data in research



Copy

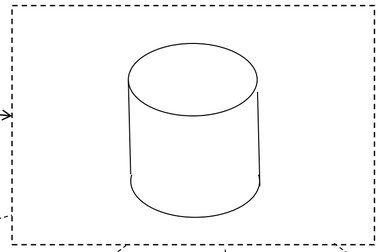
With consent, onward / Downstream copying

“classical view”

Sharing data in research

“Registration at the source”

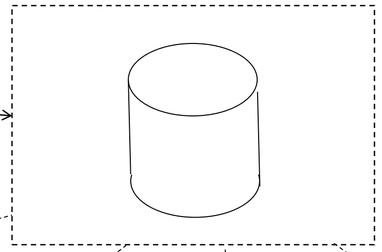
Access to current (accurate) data



Sharing data in research

“Registration at the source”

Copy



If no constraints on use - Still a data copying transparancy problem

Sharing data in research – decentralized access control

→ *New approach: implement/enforce authorization at the source*

Auth & AutZ

Access by reference

Consumer or Coordinating TTP

"sustainable view"

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Sharing data in research – how?

→ *Track (downstream) authorizations*

Auth & AutZ

Access by reference

Coordinating TTP

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Sharing data in research – how?

Consumer / Research party

Auth & AutZ

Request copy

Coordinating TTP

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Sharing data in research – how?

Consumer / Research party

Pass reference

Coordinating TTP

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Sharing data in research – how?

Consumer / Research party

Access by reference

Auth & AutZ

Coordinating TTP

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Sharing data in research – how?

white box

Consumer / Research party

Coordinating TTP

TTP coordinates the authorization process for multiple parties

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Sharing data in research – endresult

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Consumer / Researcher

Sharing data in research – result

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Consumer / Researcher

"downstream" researcher

Sharing data in research – result

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Consumer / Researcher

“downstream” researcher

Decentralized networks using authorization at the source - properties

Auth & AutZ

Policies always enforceable at the source
*All copies and access traceable at the source**
Separation of concern (responsibilities)

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Decentralized networks using authorization at the source - properties

** Long-term transparency to and control by data subjects*

Auth & AutZ

View access logs, manage authorizations

Data subject (e.g., PGO)

Auth & AutZ

Auth & AutZ

Auth & AutZ

Auth & AutZ

Decentralized **push autorisation**

Clinical use

Decentralized authorisation / networks around the patient

Dynamic and permanent authorizations

Privacy by design

- Track (audit) all data transitions in the data processing pipeline
- Control and tracking “remains” at the source
- Separate concerns / responsibilities and incentives (!)
- Ensure data subjects can always approach the original source to figure out where data (access) went
- Provides solution for data ‘owned’ by multiple parties (data not tied to one single person such as DNA data)

- *Challenge: (decentralized) identity management*

Thank you

https://whiteboxsystems.nl | guido@whiteboxsystems.nl

Whitebox foundation i/o: – separate the protocol (standard) from the product
- Intention is to bootstrap the foundation within 6 months

Relevant pointer:

https://blog.gidsopenstandaarden.nl/2020/03/Guido-van-t-Noordende-ketentransparantie-data-essentieel.html