Vertrauenswürdigkeit durch Transparenz

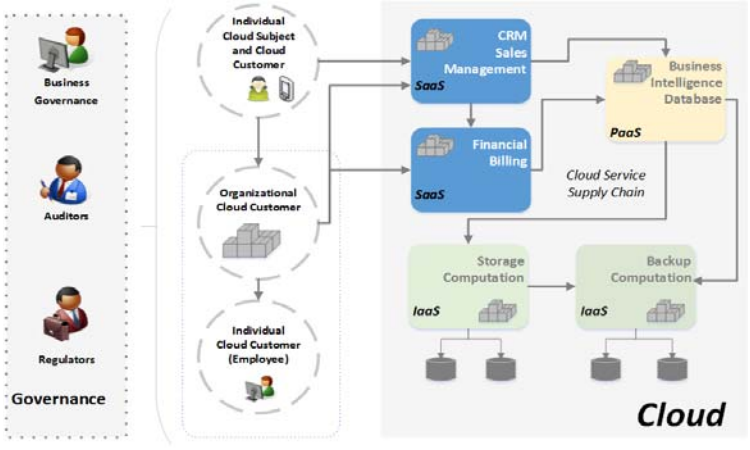
Simone Fischer-Hübner, Karlstad University

Sommerakademie, Kiel

31. August 2015

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

I. Hintergrund – Mangel an Transparenz und Kontrolle bei Cloud Computing (Art. 29-Datenschutzgruppe Stellungnahme 05/2012)



Picture: Siani Pearson, NordSec 2014, Springer LNCS.

Mangel an Transparenz in Bezug auf Cloud-Datenverarbeitung :

Kette von mehreren Auftragsverarbeitern & Unterauftragnehmern

Verschiedene geographische Standorte in der EEA

Transfer in Drittländer außerhalb der EEA

Offenlegung von Daten an fremde Strafverfolgungsbehörden

Fehlende Intervenierbarkeit:

Mangel an Tools zur Durchsetzung der Rechte Betroffener

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

Transparenz & Intervenierbarkeit

Rechtliche Datenschutz-Prinzipien

- *EU-Datenschutzrichtlinie*: Informations- und Auskunftsrechte in Bezug auf Daten und Logik der automatisierten Verarbeitung, Rechte auf Löschung, Sperrung, Korrektur

EU-DS-GVO: Informationspflicht bei Datenpannen, elektronische Rechteausübung

Schwedisches Patientendatenschutzgesetz: Zugriffsrechte auf Patienteninformationen und Log-Daten

Sozialer Vertrauensfaktor

- Erhöhtes Vertrauen, falls Prozeduren klar, transparent und reversibel sind.

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

Transparenz vs. Vertraulichkeit *Beispiele*

Log-Daten im Gesundheitsbereich – Datenschutzprobleme:

- Information über diejenigen, die [illegible] Patientendateien hatten (z. [illegible] sensitiv für Patienten
- Überwachung [illegible] Arbeit des medizini[illegible]

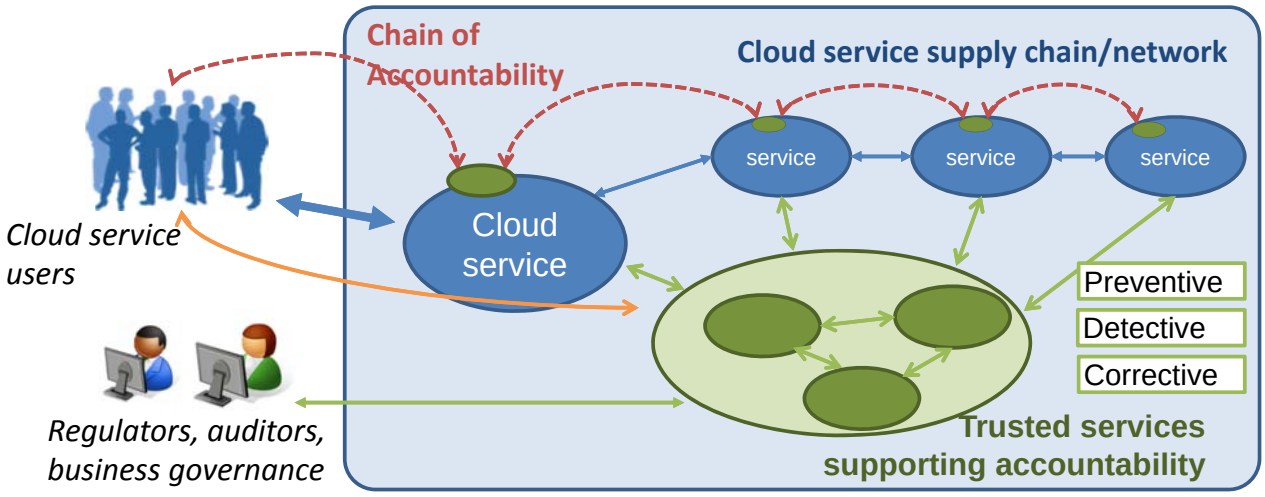
Geschäf[illegible] Bezug auf Profiling

- (vgl. Erw[illegible] und 41 Datenschutzrichtlinie)

Anforderungen:
- Datenschutzfreundlich
- Faire Abwägung mit Geschäftsgeheimnissen

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

II. FP7-Projekt A4Cloud

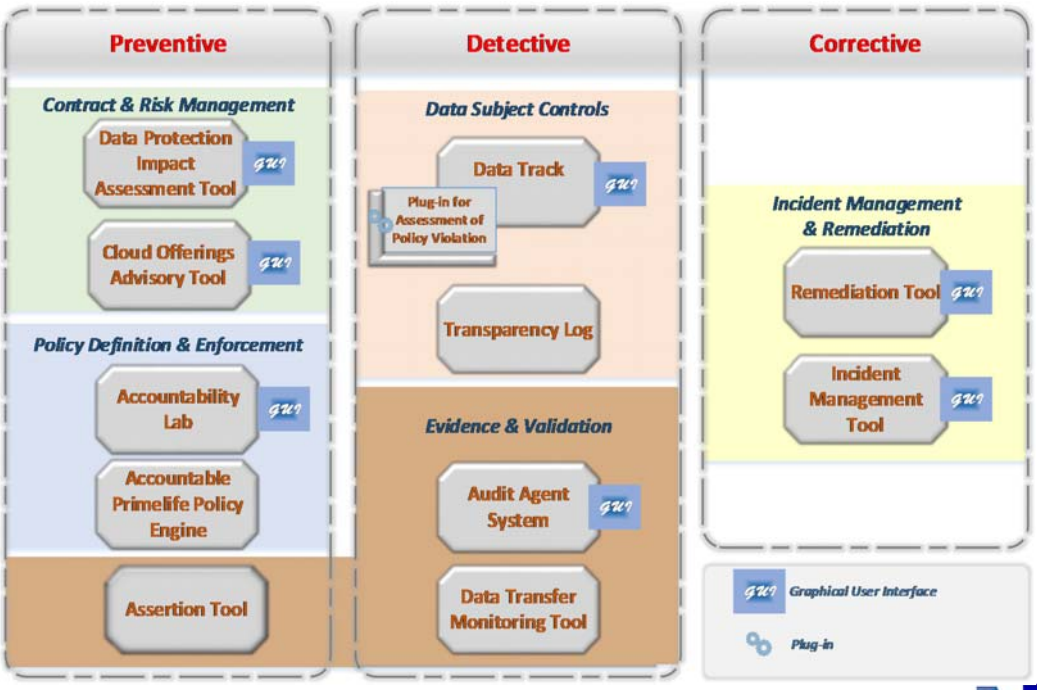


Cloud service users: Kontrolle und Transparenz der Datenbenutzung, Unterstützung in Bezug auf Entschädigung

Service providers: Techniken, um Dienste vertrauenswürdig zu machen, Datenschutz-Policies und SLAs/PLAs zu erfüllen

Regulators/auditors: Gewissheit über die Einhaltung von Policies und Vorschriften

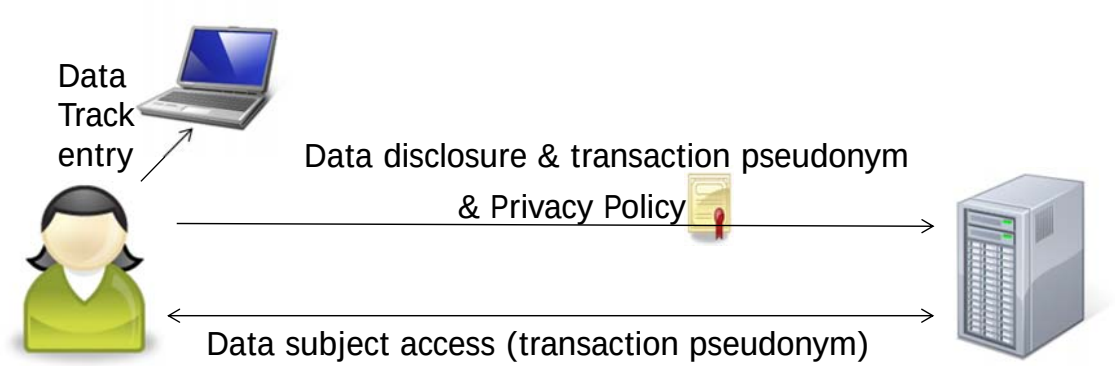
A4Cloud Toolset



This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

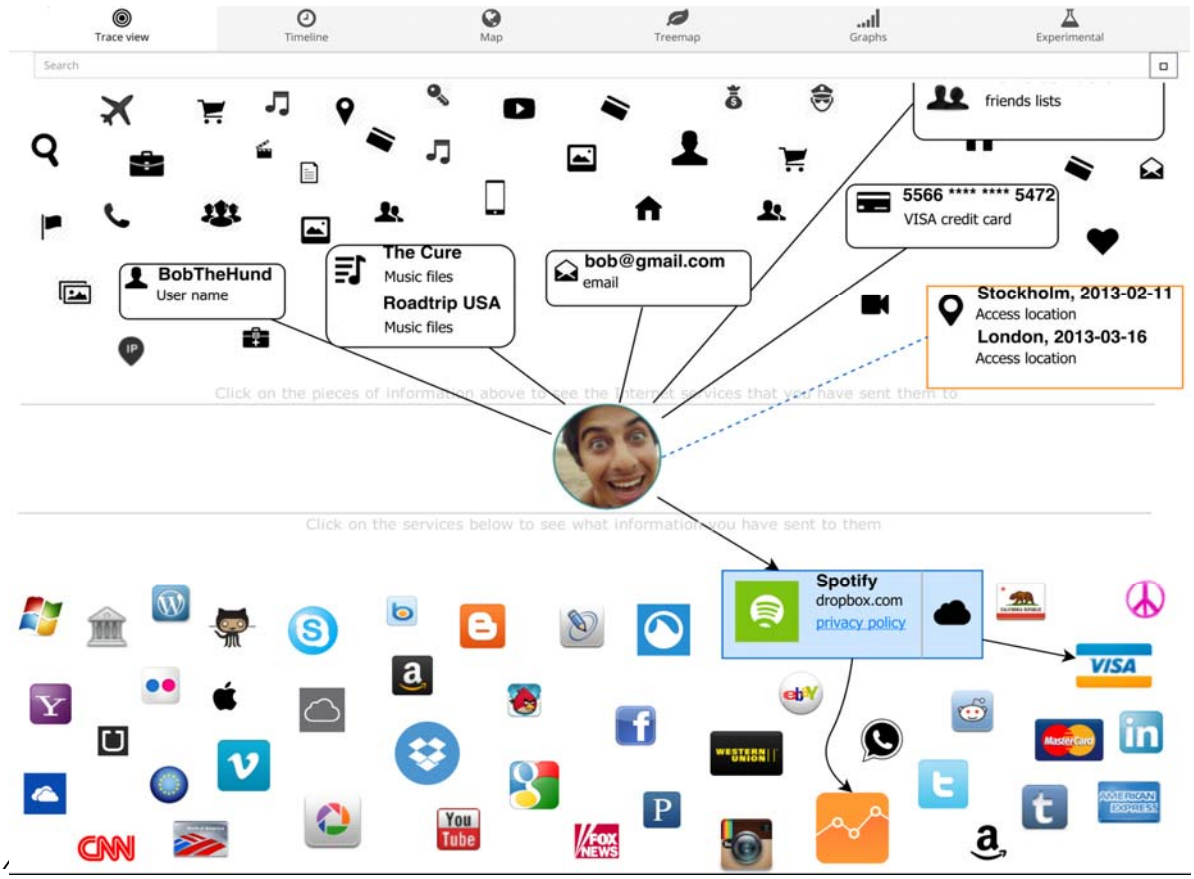
CLOUD ACCOUNTABILITY PROJECT

III. Datenschutzfreundliche Transparenz-Tools – Ex post TETs: Data Track



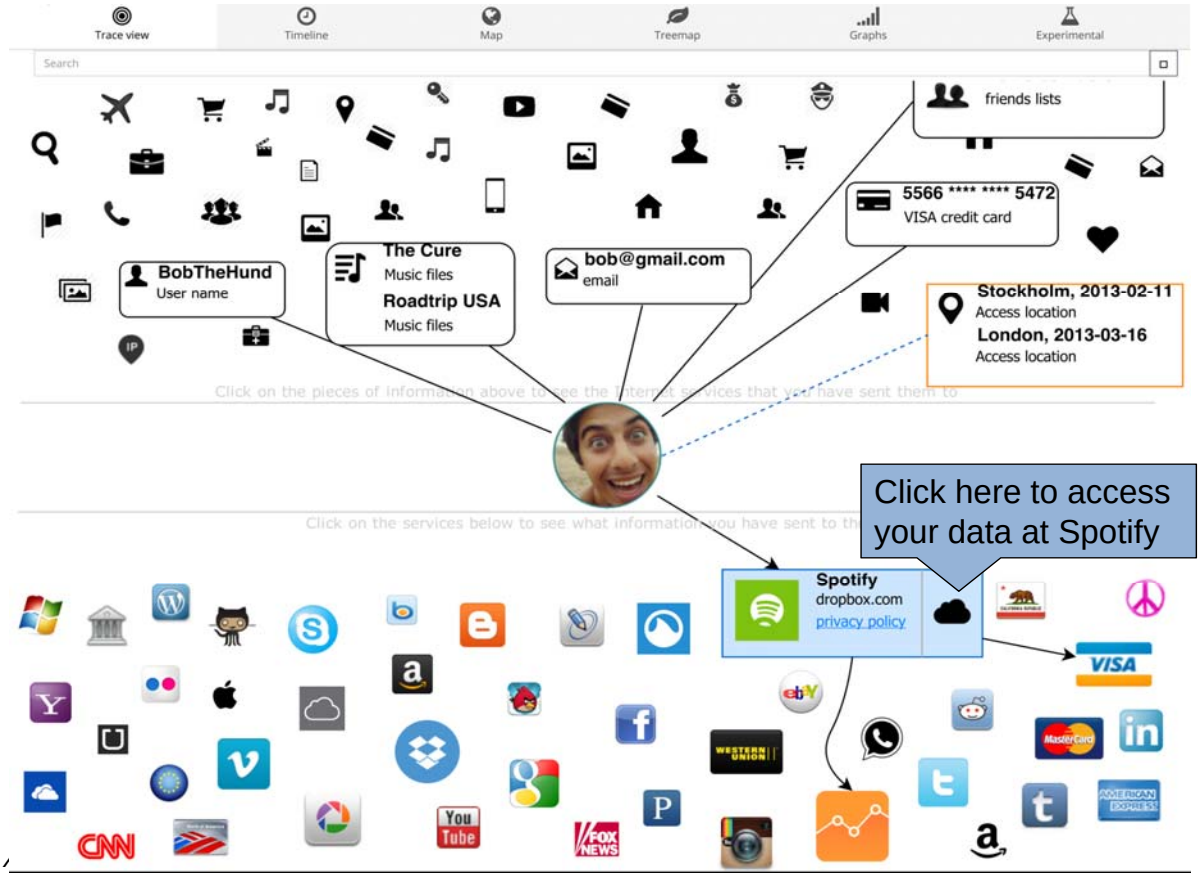
This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

A4Cloud Data Track (3. Iteration)



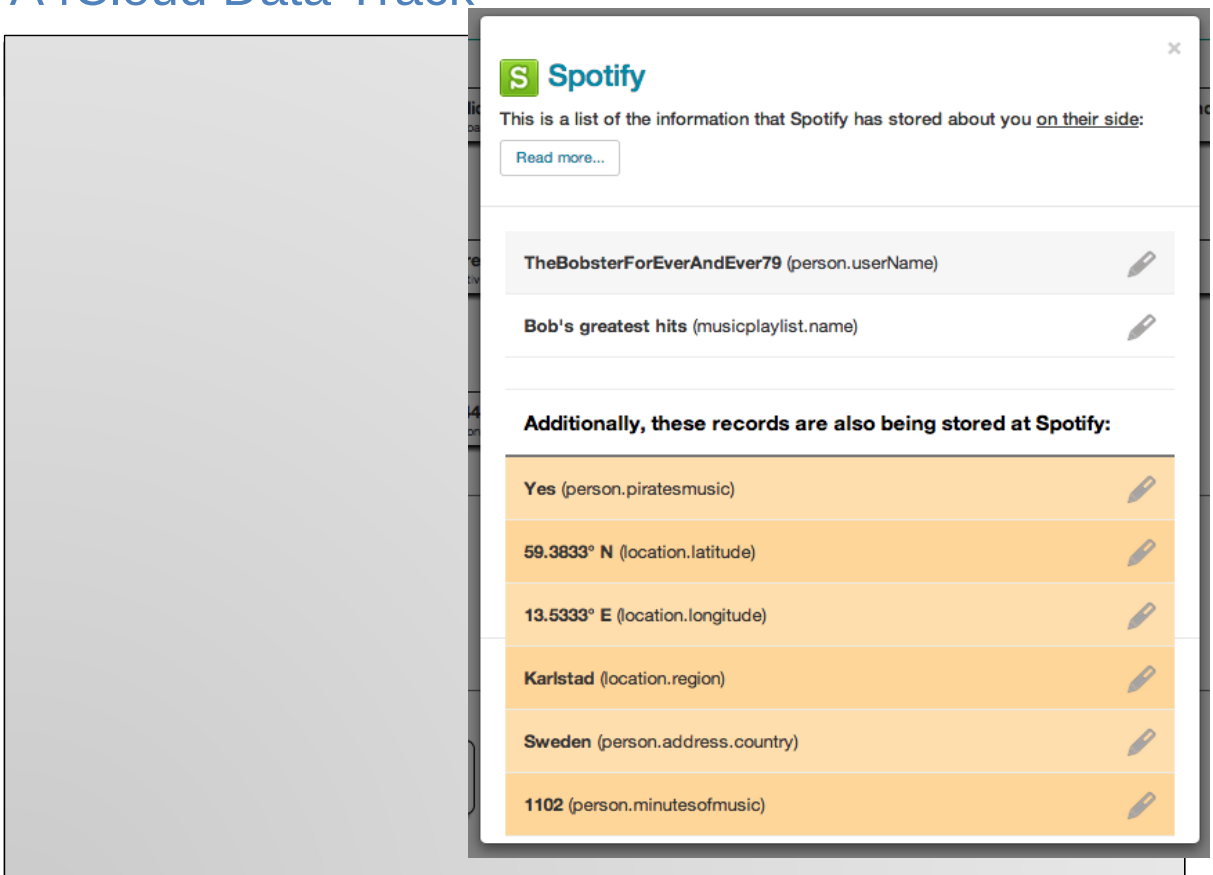
Source: /

A4Cloud Data Track



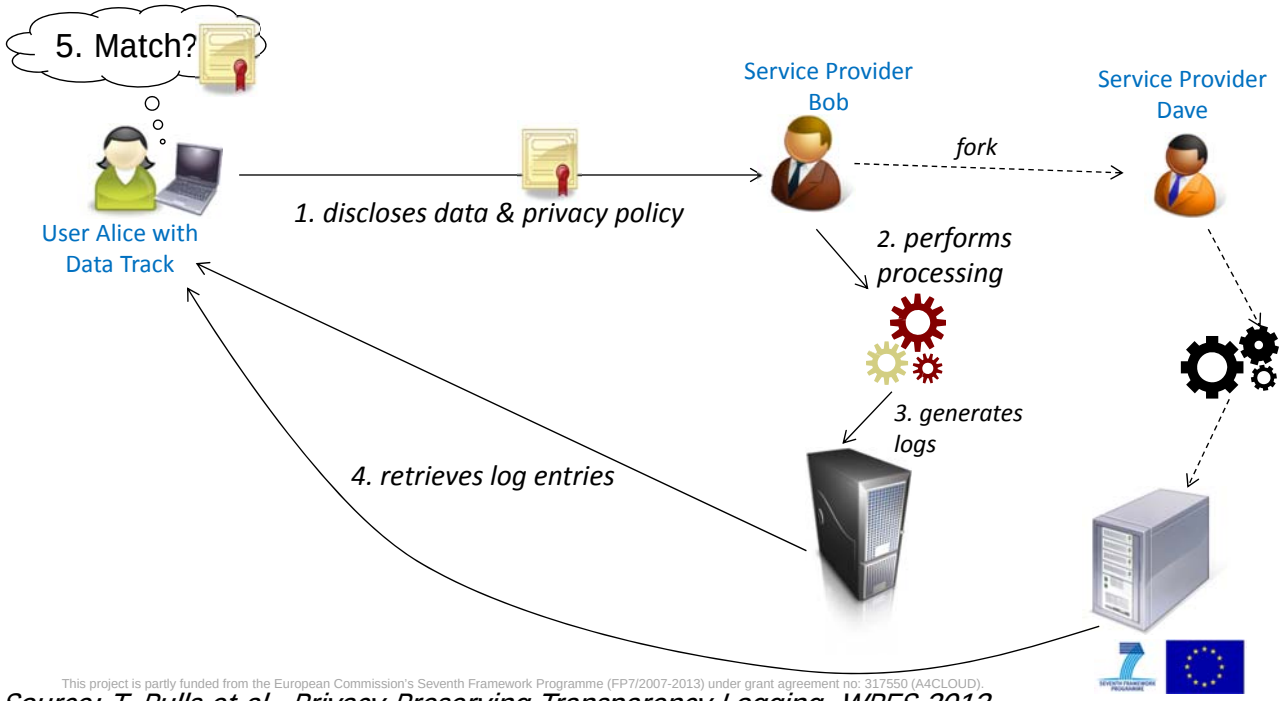
Source: A

A4Cloud Data Track



Source: A

Transparency Logging



This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

Source: T. Pulls et al., Privacy-Preserving Transparency Logging, WPES 2013

Verteiltes datenschutzfreundliches Transparency Logging – *Sicherheitseigenschaften*

Integrität: Keine nicht-entdeckbaren Modifikationen von protokollierten Daten (gespeichert vor einer Komprimittierung)

Vertraulichkeit: Nur Betroffene (oder Auditoren) können die Daten lesen, die für sie protokoliert wurden

Unverkettbarkeit von Log-Einträgen und Benutzer-Identitäten zwischen verschiedenen Datenverarbeitern

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

Benutzer-Evaluation vom Data Track

Finden Benutzer die „Trace View“ des Data Tracks intuitiv und verständlich?

Schätzen Benutzer die Funktionalität des Data Track?

Verstehen die Benutzer die zwei verschiedenen Ansichten der Datensätze (1. lokal beim Benutzer, 2. remote beim Diensteanbieter gespeichert)?

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

Benutzertest-Resultate

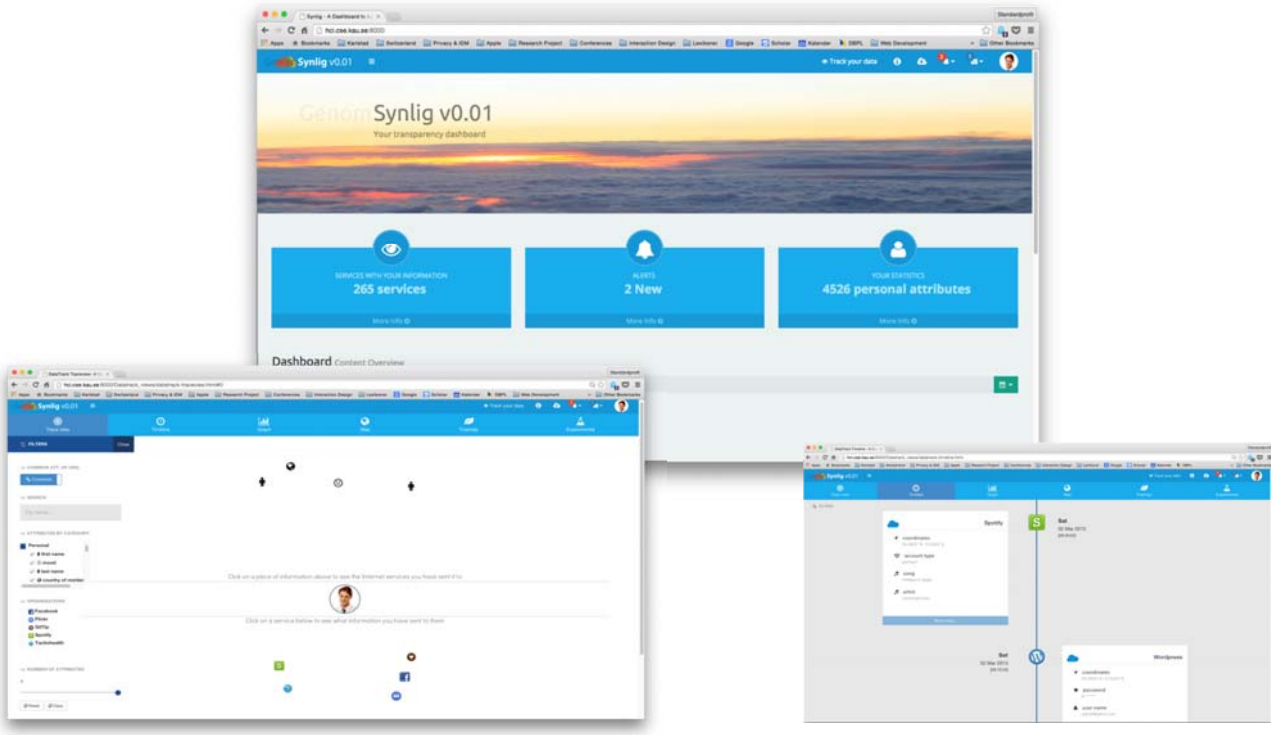
Where are the Data Track records stored?	Frequency	Percent
On the DataTrack program (on a cloud/Internet storage)	9	52.9
On the DataTrack program (locally in computer)	4	23.5
On the Internet somewhere	1	5.9
On the services that I have given information to	3	17.6

How often do you think you would have the program turned on so that it tracks the information you give to Internet services?	
Never tracking (-0% of the time)	2
Rarely tracking (25% of the time)	3
Often tracking (75% of the time)	5
Always tracking (100% of the time)	7

How often do you believe you would use the DataTrack program?	
Very rarely (almost never or never)	1
Rarely (a few times per year)	1
Sometimes (a few times per month)	7
Often (around two to four times per week)	4
Very often (almost always)	4

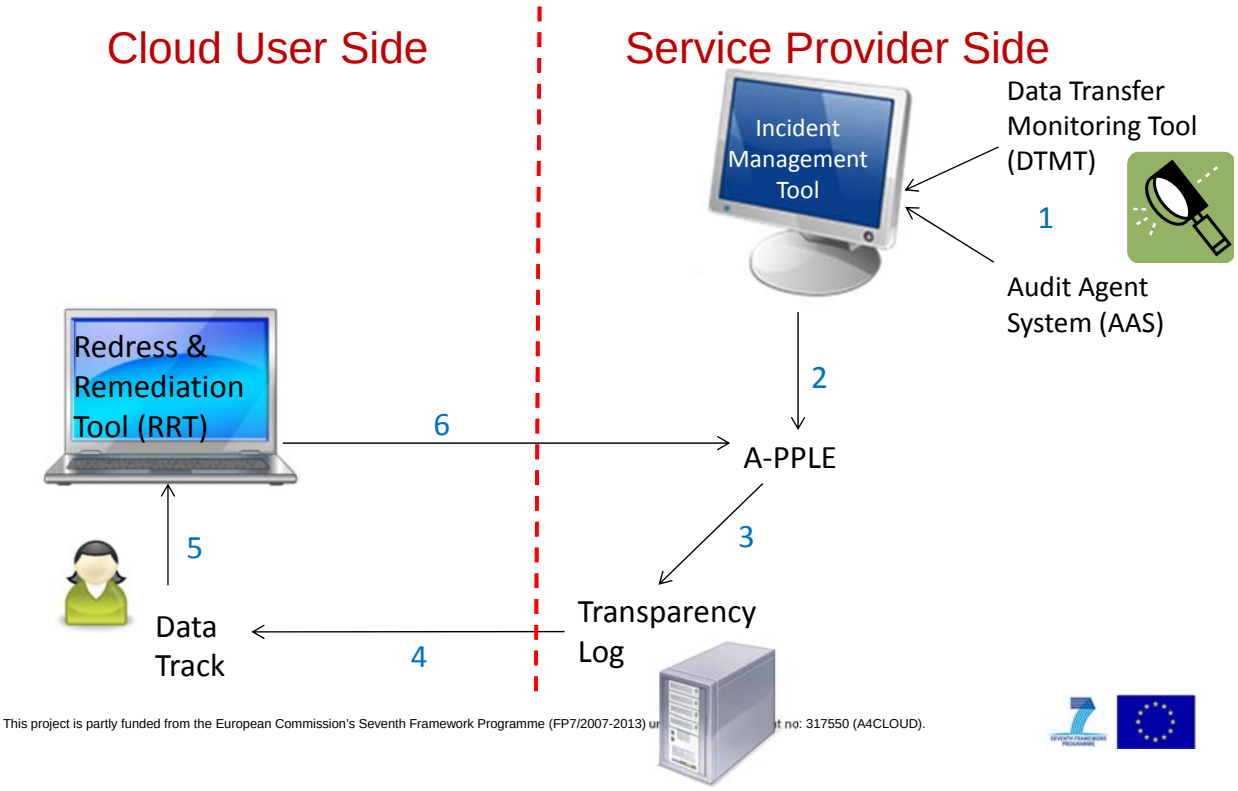
This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

4. Iteration – Data Track



CLOUD ACCOUNTABILITY PROJECT

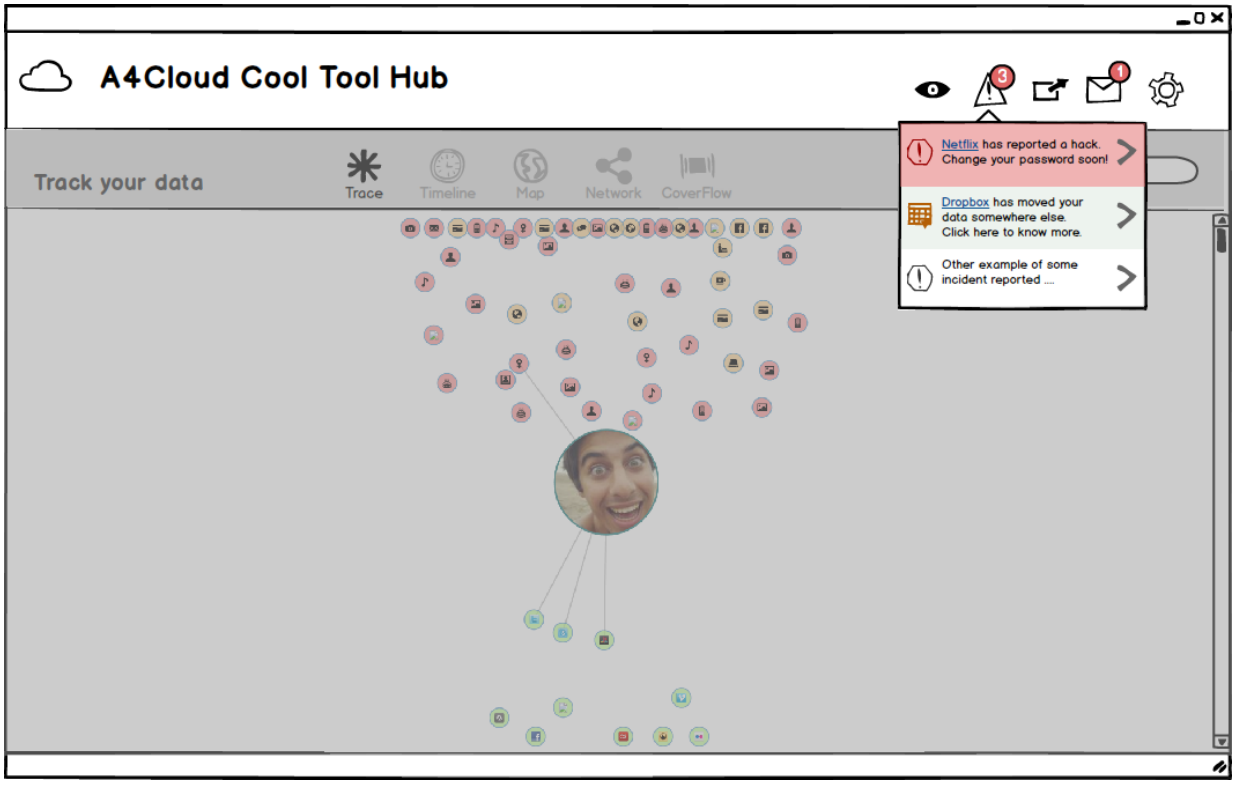
Zusammenspiel der A4Cloud-Tools



This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) ur t no: 317550 (A4CLOUD).

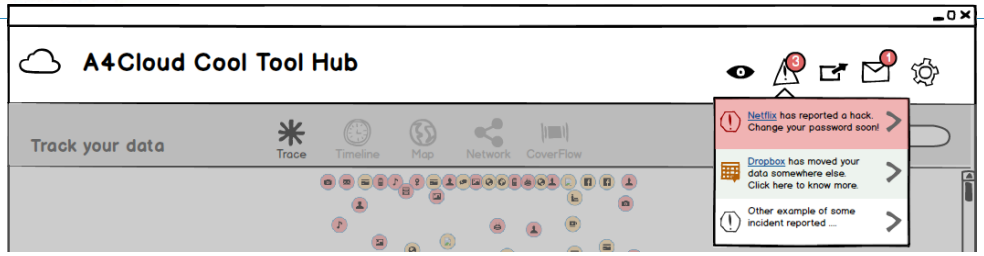
CLOUD ACCOUNTABILITY PROJECT

Data Track & RRT



CLOUD ACCOUNTABILITY PROJECT

Benutzer-Workshops zu Notifizierungen



I would like this tool to notify me	Avg
when my data has been shared with other companies or people	3.63
when a hacker has obtain my data from the service that has it	**4.78**
when my data has been moved to a different country (which might have different laws to handle my data)	2.89
when a service that has my data has used my data for purposes that I do not agree with (e.g. for sending me advertisement, or for tracking my activities, etc.)	4.21
when a service that has my data has been attacked by a hacker	**4.53**
if a service that has my data was recently mentioned in the news or if a scandal is reported about this service	3.47

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 317550 (A4CLOUD).

Schlussfolgerungen von Evaluierungen– HCI-Anforderungen

(see also: Angulo, Fischer-Hübner, et.al., CHI 2015 – Proceedings, Work in Progress Session, ACM).

- Mache den Unterschied von lokal und remote gespeicherten Daten offensichtlich;
- Biete Transparenz auch für implizite Daten;
- Priorisiere Notifikationen von Vorfällen, für die Korrektur und Entschädigung angeboten werden können;
- Biete den Nutzern Hilfe (z.B. über Tooltips oder einführende Tutorials) dazu, wie Kontrollfunktionen aktiviert werden können.

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

IV. Schlussbemerkungen

- Transparenz-Tools können
  - Technisch Datenschutz-Prinzipien & Benutzerrechte durchsetzen
  - Vertrauen von Benutzern und anderen Stakeholdern in Infrastrukturen erhöhen
  - Verantwortung (accountability) erhöhen.
- Kooperation mit Diensteanbietern nötig für die volle Funktionalität;
- "Stand alone"-Data Track kann visuell Transparenz über die preisgegebenen Daten bieten (auch via Visualisierung von Daten-Exports).

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

CLOUD ACCOUNTABILITY PROJECT

Referenzen

Julio Angulo, Simone Fischer-Hübner, John Sören Pettersson, Jessica Edbom , Mia Toresson, Henrik Andersson. D:C-7.3 Report on end-user perceptions of privacy enhancing transparency and accountability, A4Cloud Deliverable D37.3, September 2014.

Julio Angulo, Simone Fischer-Hübner, John Sören Pettersson, Erik Wästlund, and Leonardo Martucci. D:C-7.1 General HCI principles and guidelines for accountability and transparency in the cloud. Project deliverable D:C-7.1, A4Cloud Project, September 2013.

Julio Angulo, Simone Fischer-Hübner, Tobias Pulls, Erik Wästlund: Usable Transparency with the Data Track: A Tool for Visualizing Data Disclosures. CHI Extended Abstracts 2015. ACM 2015.

Simone Fischer-Hübner, John Sören Pettersson, Julio Angulo: HCI Requirements for Transparency and Accountability Tools for Cloud Service Chains. A4Cloud 2014, Springer 2014.

Simone Fischer-Hübner, Julio Angulo, Tobias Pulls: How can Cloud Users be Supported in Deciding on, Tracking and Controlling How their Data are Used? Privacy and Identity Management 2013, Springer 2014

Tobias Pulls, Roel Peeters: Balloon: A Forward-Secure Append-Only Persistent Authenticated Data Structure. ESORICS 2015.

Tobias Pulls, Roel Peeters, Karel Wouters: Distributed privacy-preserving transparency logging. WPES 2013.

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

CLOUD ACCOUNTABILITY PROJECT

Fragen?

www.A4Cloud.eu

simofihu@kau.se

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).