EEXCESS or the challenge of privacy-preserving quality recommendations

Benjamin Habegger, Nadia Bennani, Elöd Egyed-Szigmond, Omar Hassan
Lyon University, CNRS, INSA-Lyon, LIRIS, UMR5205

EEXCESS - Project

Enhancing Europe's eXchange in Cultural Educational and Scientific reSources.

Started: February 2013

Duration: 4 Years

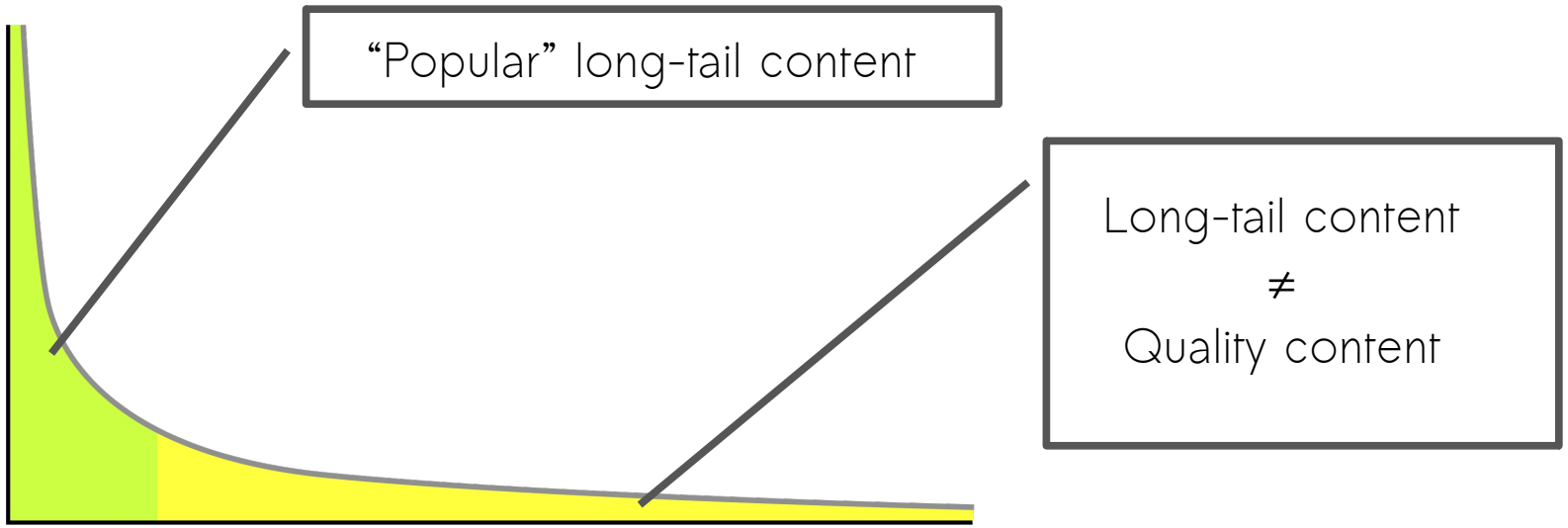
Budget: 7.05 Million EUR

http://eexcess.eu/

EEXCESS - Partners

EEXCESS - Main problem

Making existing qualilty content visible



EEXCESS - Objectives

Content enrichment

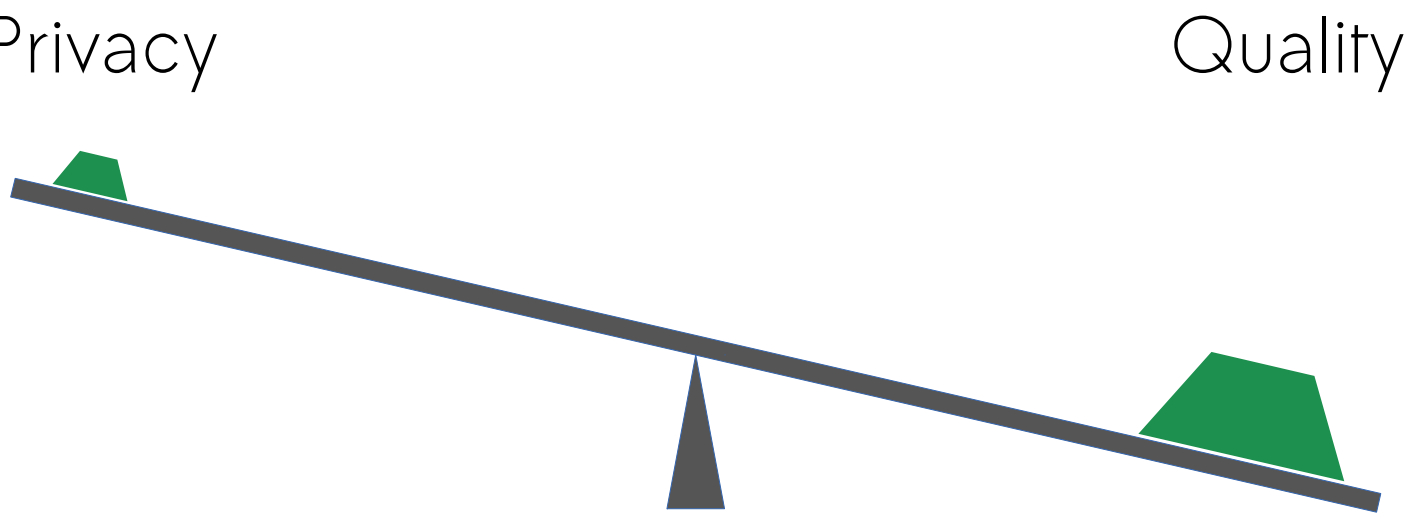
Personalized recommendation

Privacy preservation

EEXCESS - Global challenges

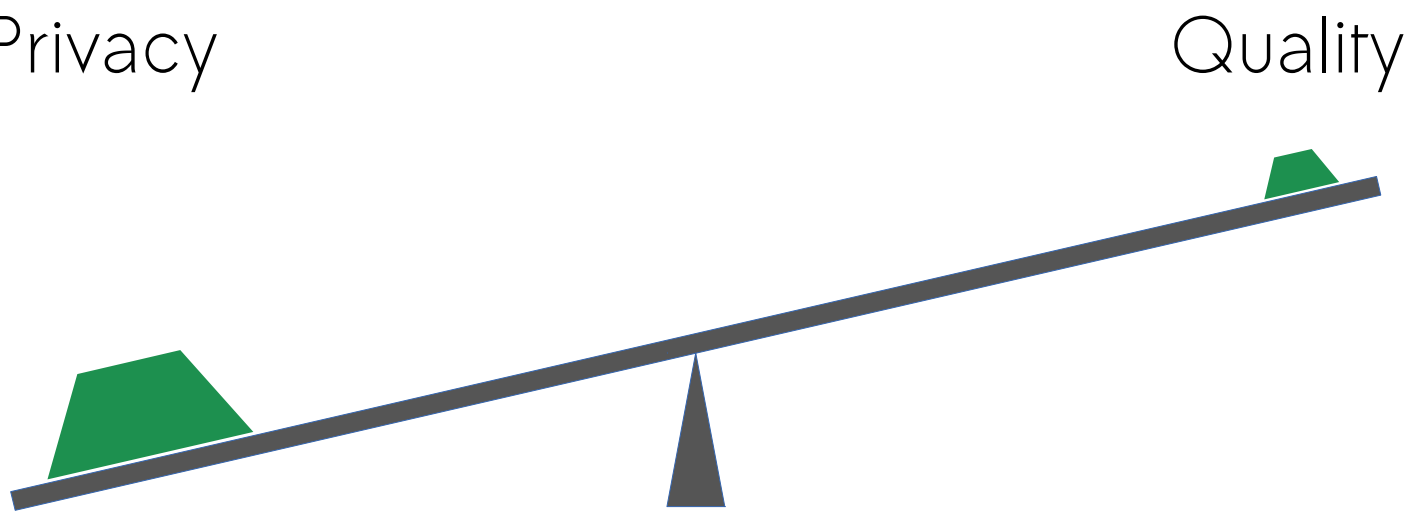
- Federated recommendation
- Integration of multiple document sources
- Mining for user profiles
- Adapting user interfaces to context
- **Preserving user privacy**

EEXCESS - Tradeoff ?



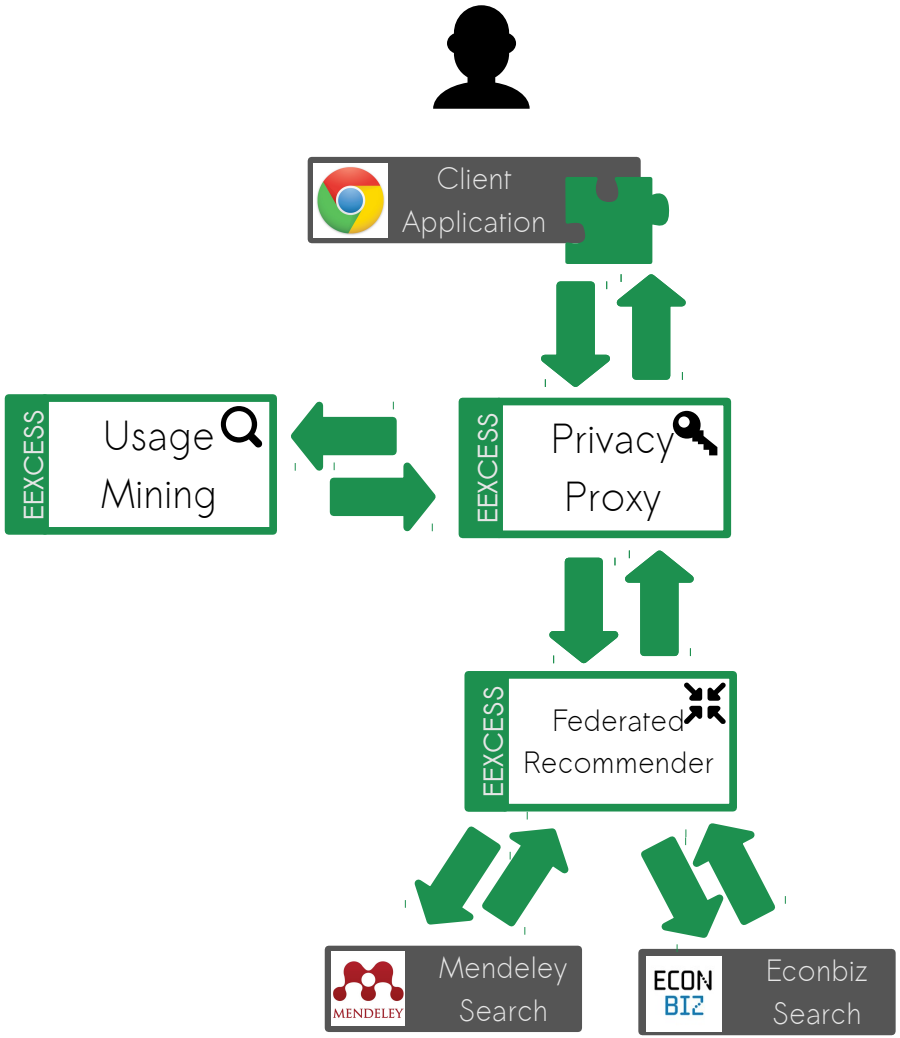
- **Unlimited disclosure**
  - User privacy is clearly at stake.
  - Does it improve quality ? How much ?

EEXCESS - Tradeoff ?



- Limited disclosure
  - Limit recommendation quality ?

EEXCESS - Simplified architecture



Usage mining

→ build detailed user profiles

EEXCESS - User context

- Activity context
  - Browsing history
  - Ongoing tasks
  - Reading history
- Environmental context
  - Temperature, Humidity, Light
  - Things, Services
- Personal context
  - Weight, Pulse, Blood pressure, Mood
- Social context
  - Friends
  - Neighbors
  - Co-workers
  - Relatives
- Spatio-temporal context
  - Time
  - Location
  - Direction of movement

EEXCESS - User profile

- Demographic information
  - Age
  - Gender
  - Relationship status
  - Address
  - ...
- Interests
  - Professional interests
  - Personal interests
  - Interest in commercial products
- Knowledge, background, skills
  - Knoweldge within a domain (e.g. acquired by a student)
  - Professional expertise and skills
- Goals
  - Short term goal (current task)
  - Long term goal
- Behavior
  - Repetitive behaviors
  - History of user actions

Recommendation

→ find recommendations adapted to the user profiles

EEXCESS - Recommendation

- Content-based
- Collaborative filtering
- Demographic filtering
- …

Privacy preserving recommendation

→ compromise between private information disclosure and quality

EEXCESS - Privacy questions

- What profile information is useful ?
  - For usage mining ?
  - For quality recommendations ?
- How much and how detailed should this information be disclosed ?
  - To preserve privacy ?
  - To ensure recommendation quality ?
- What control and feedback can we provide ?
  - To „measure“ the impacts of disclosure

EEXCESS - Privacy wish-list

- Guarantees
  - Deterministic ?
    - Guarantee that a particular piece of information doesn't leak
  - Risk of disclosure (including inference)
    - Measuring risks and impacts of privacy breaches
- Flexibility
  - User-dependant policy
    - Alice and Bob may have different requirements
  - Context-dependant policy
    - Alice may have different requirements at home and at work

EEXCESS - Privacy techniques

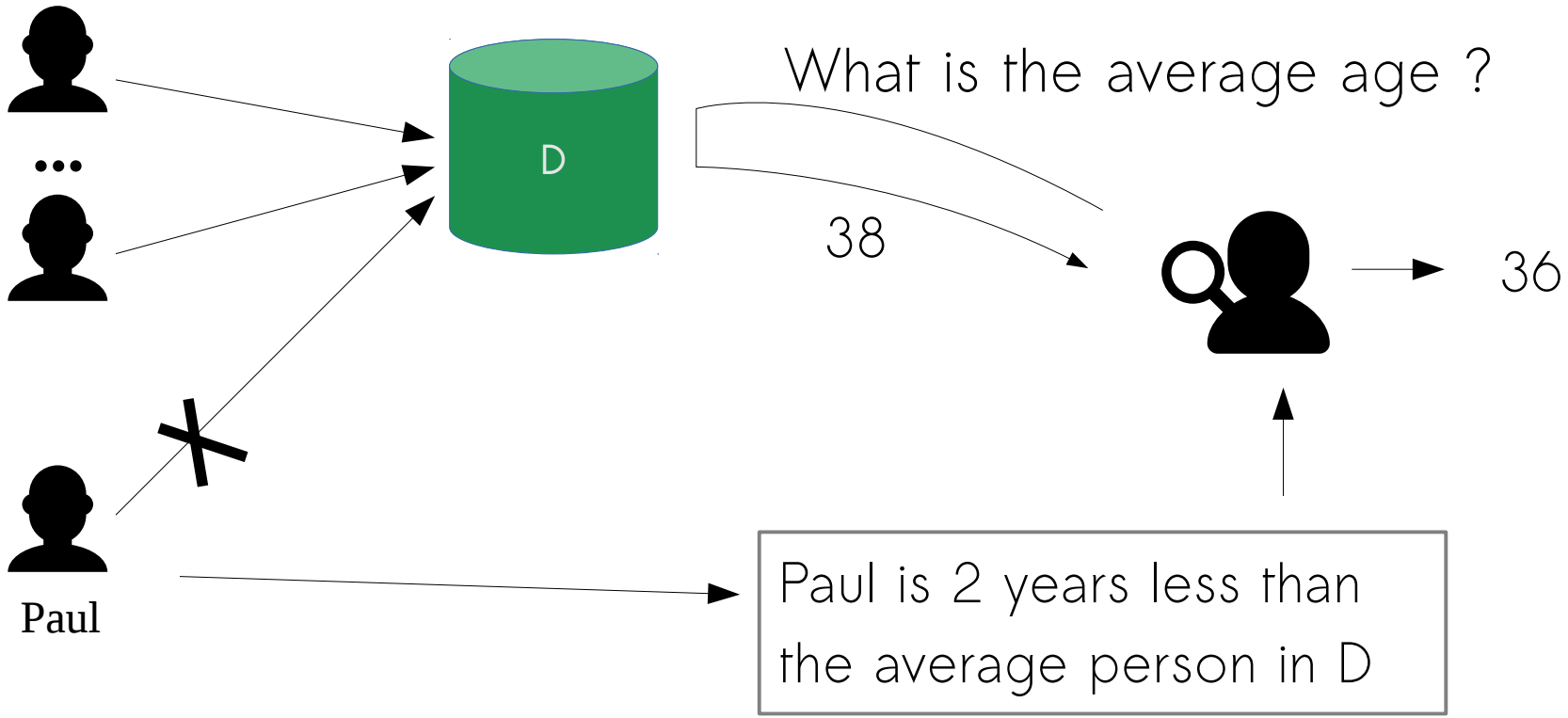
- Anonymization
  - K-anonymity [Sweeney2002]
- Differential Privacy [Dwork2006]
- Hiding in the crowd
- Distributed recommendation
- ...

EEXCESS - Privacy challenges

- Data mining, Big data analytics
- External knowledge
  - De-anonymization [Narayanan2008]
  - Breaches w.o. participation [Dwork2006]

EEXCESS - Privacy challenges

Privacy breach w.o. participation [Dwork2006]

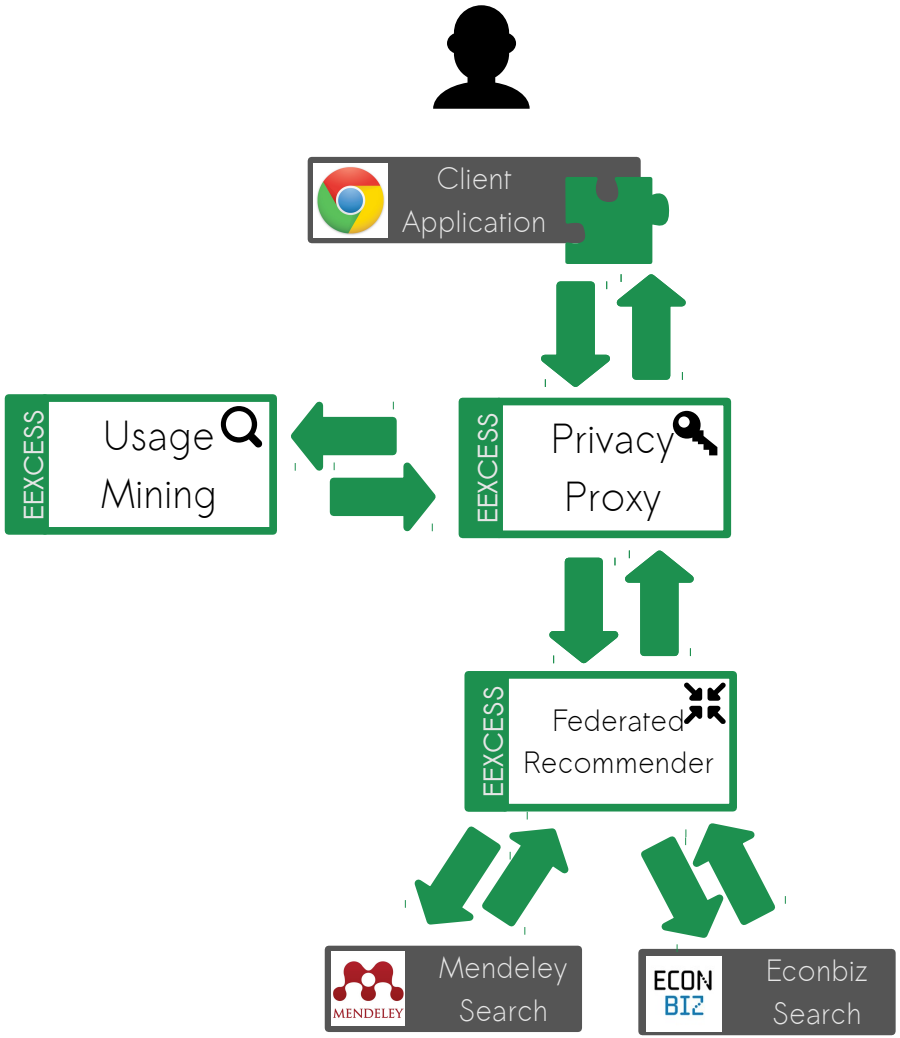


Ongoing work

EEXCESS - Current focus

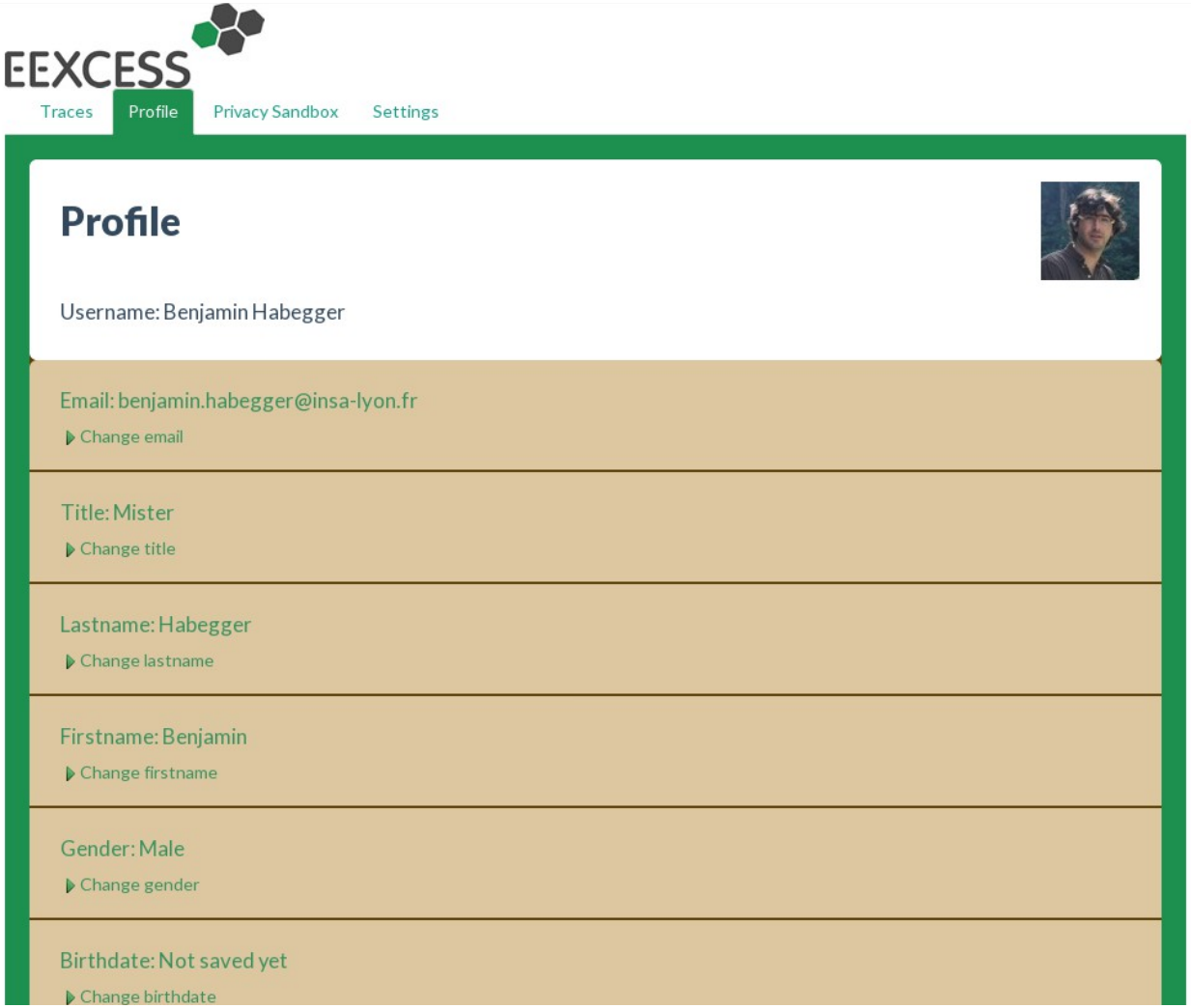
- Setup a test-framework
  - User interface
  - API's
  - Evaluation tools
- Involve the user
  - Transparency
    - What is going on ?
    - What does the system know ?
  - Control
    - Let users define their own policy
  - Feedback
    - Show the impacts of user's policy

EEXCESS - Simplified architecture

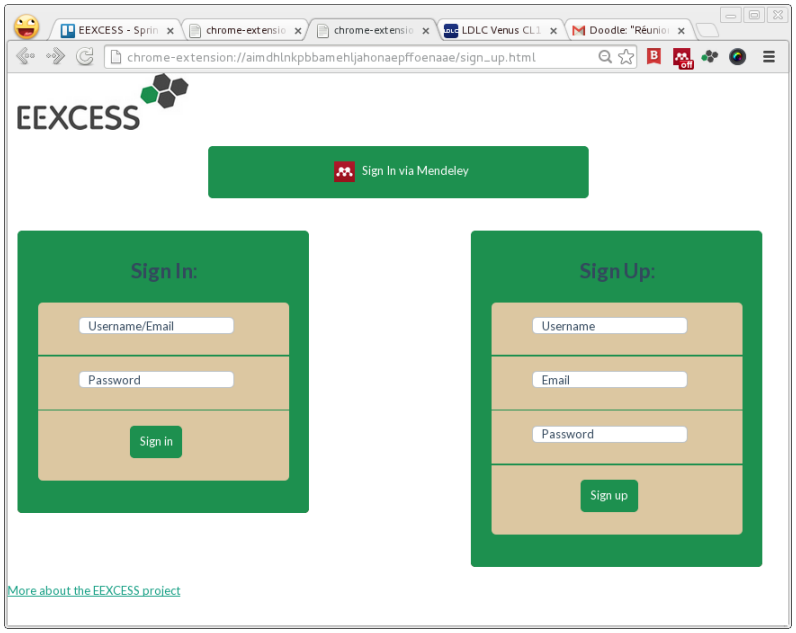


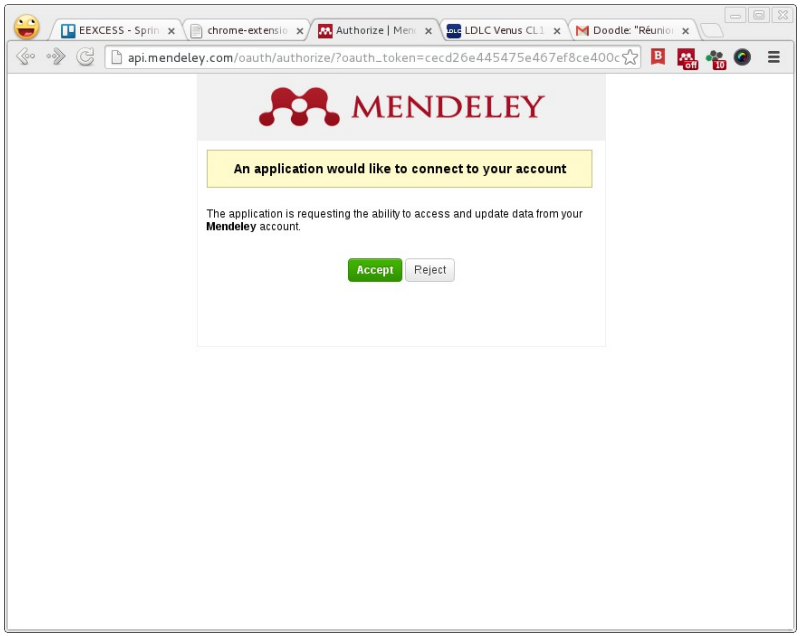
Privacy Plugin - Recommendations

Privacy Plugin - Profile edition



Privacy Plugin - Profile data collection

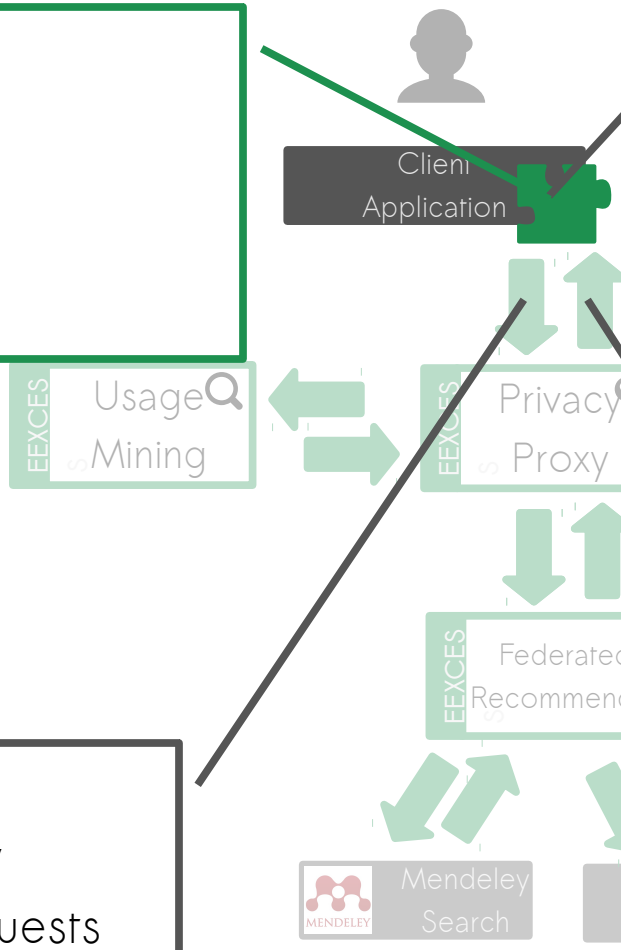




- Mendely auth + profile import

Privacy Plugin

- Recommendations
- Privacy settings
- Profile editing
- Privacy sandbox

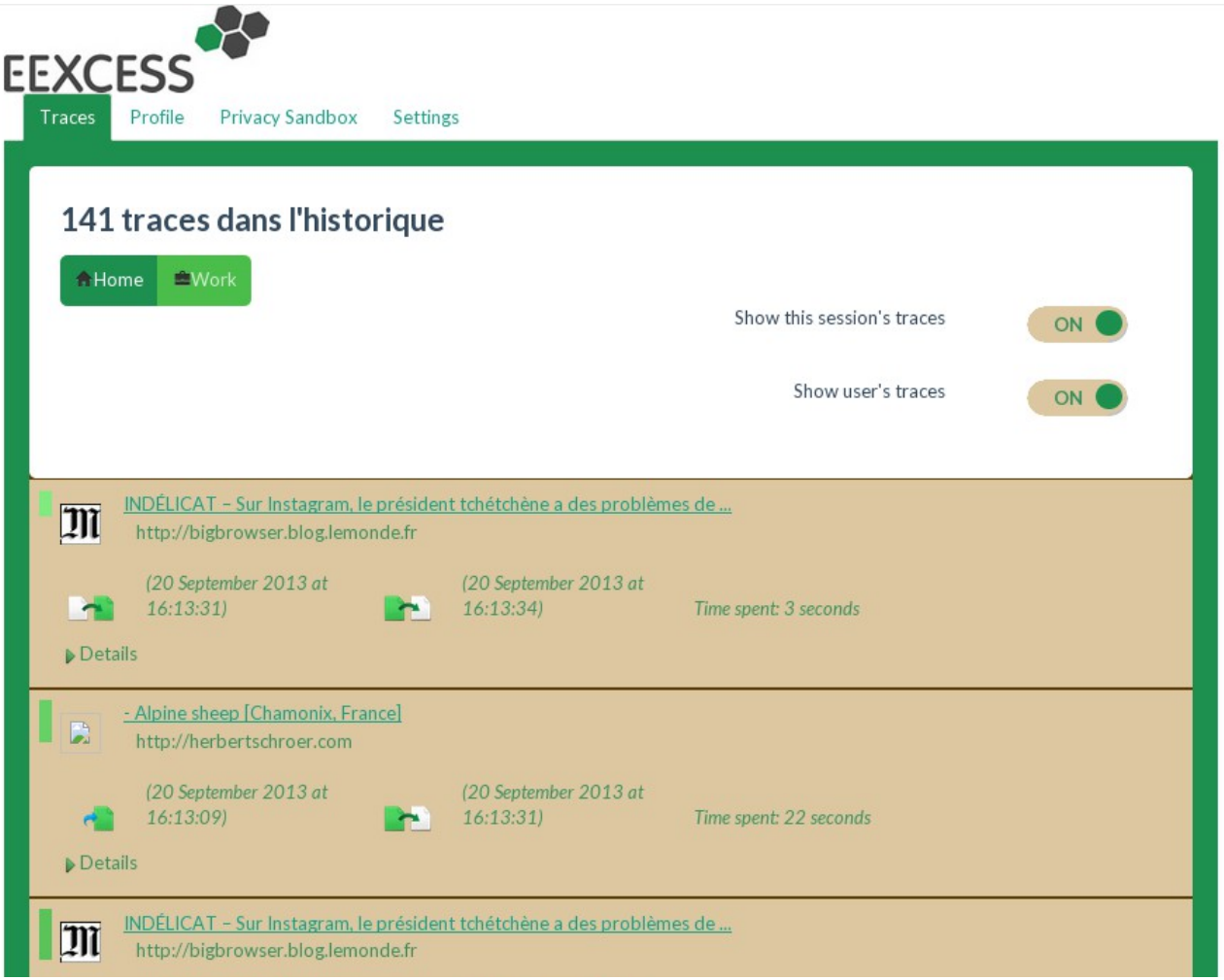


- Oauth interactions with Mendeley

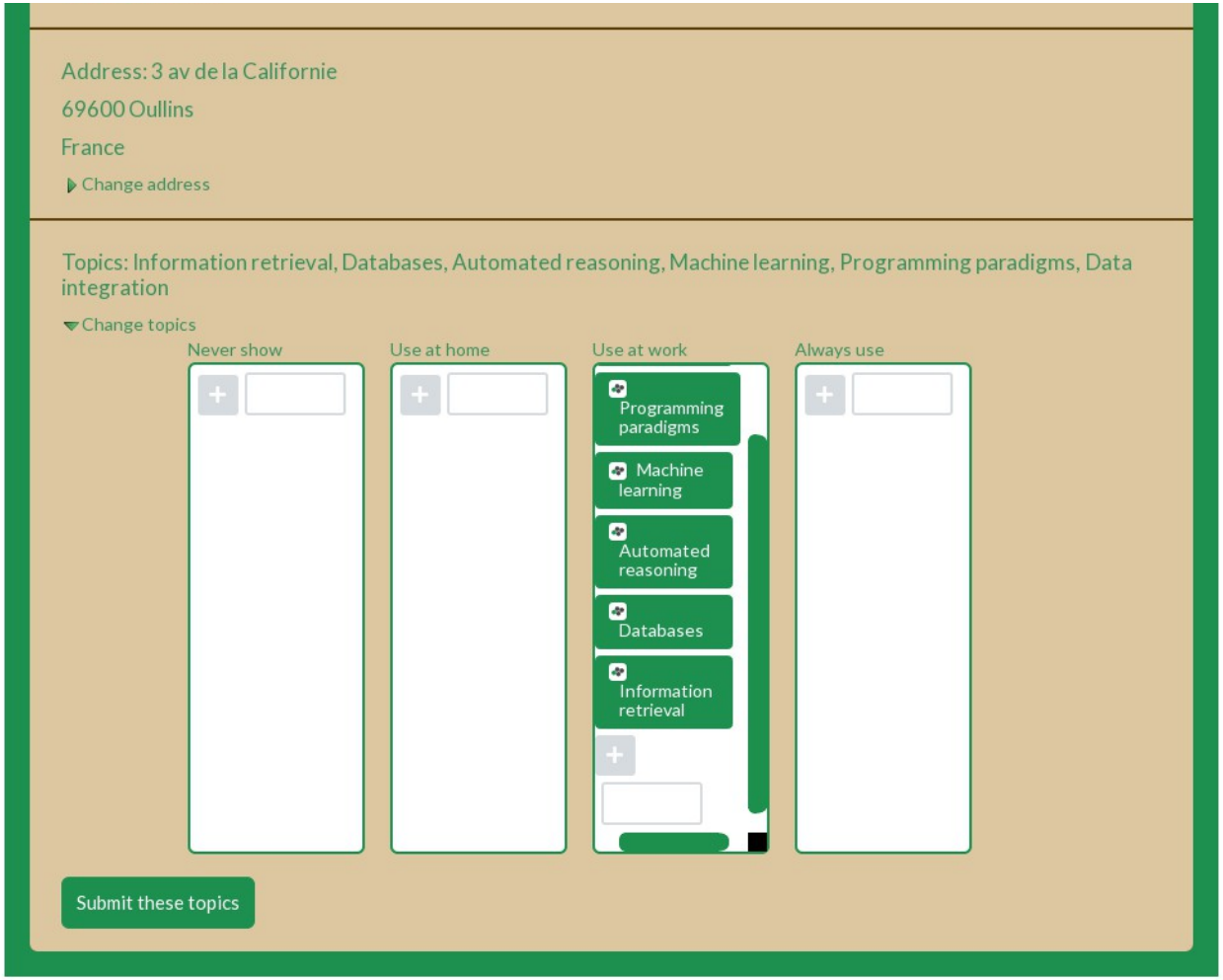
- Receives recommendations

- User profile edits
- User browsing activity
- Recommendation requests

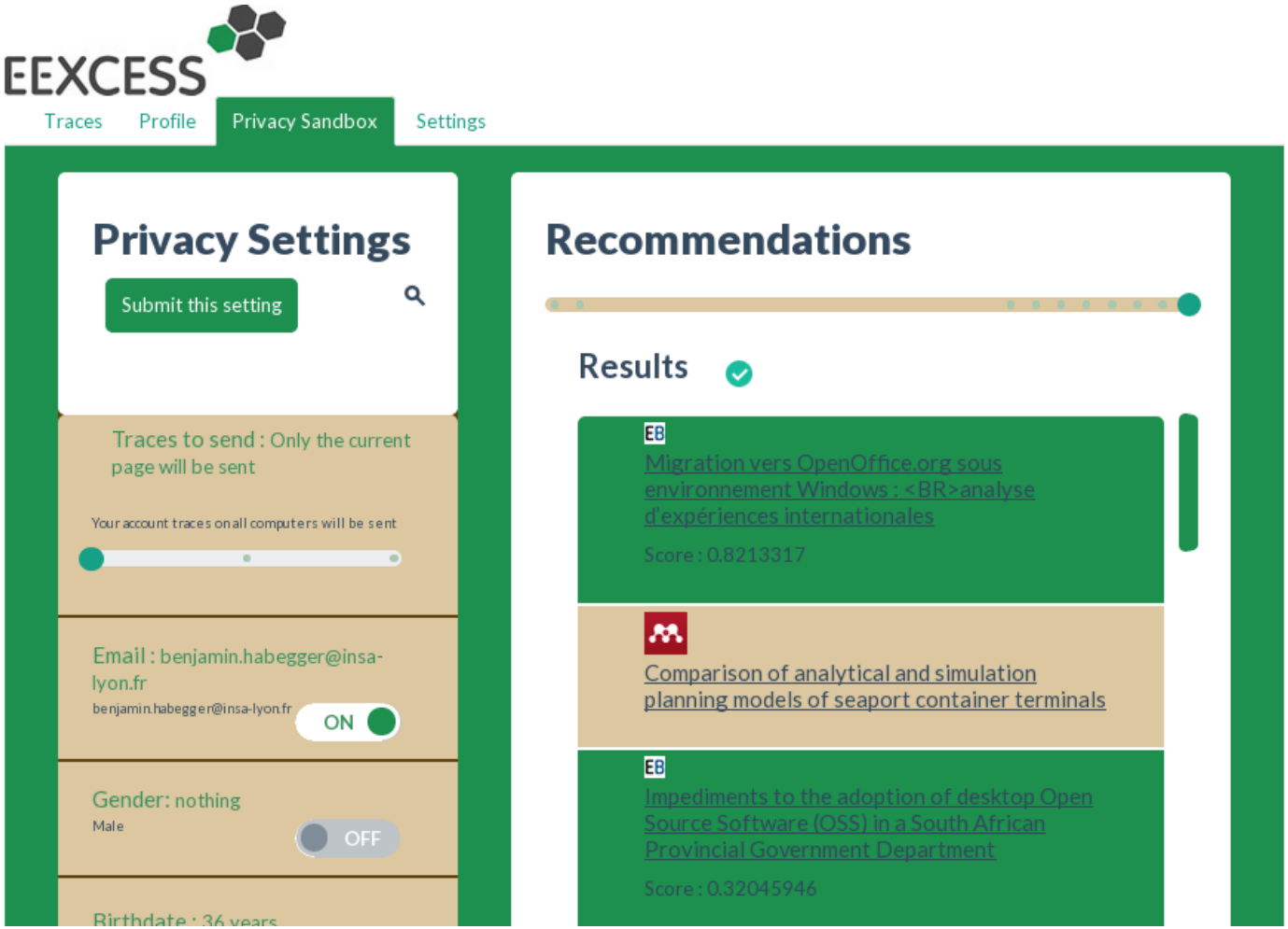
Privacy Plugin - Transparency



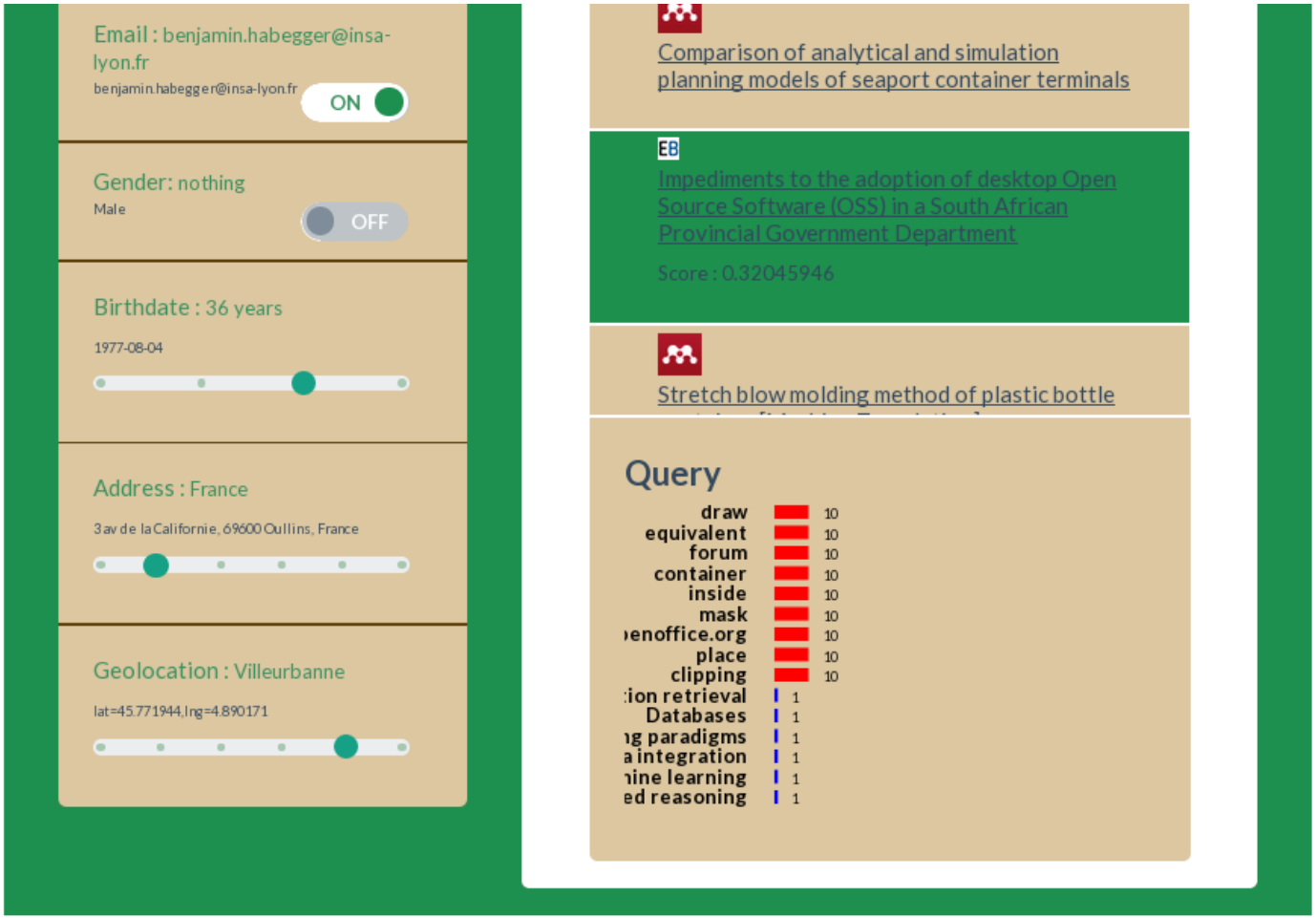
Privacy Plugin - Trancparency



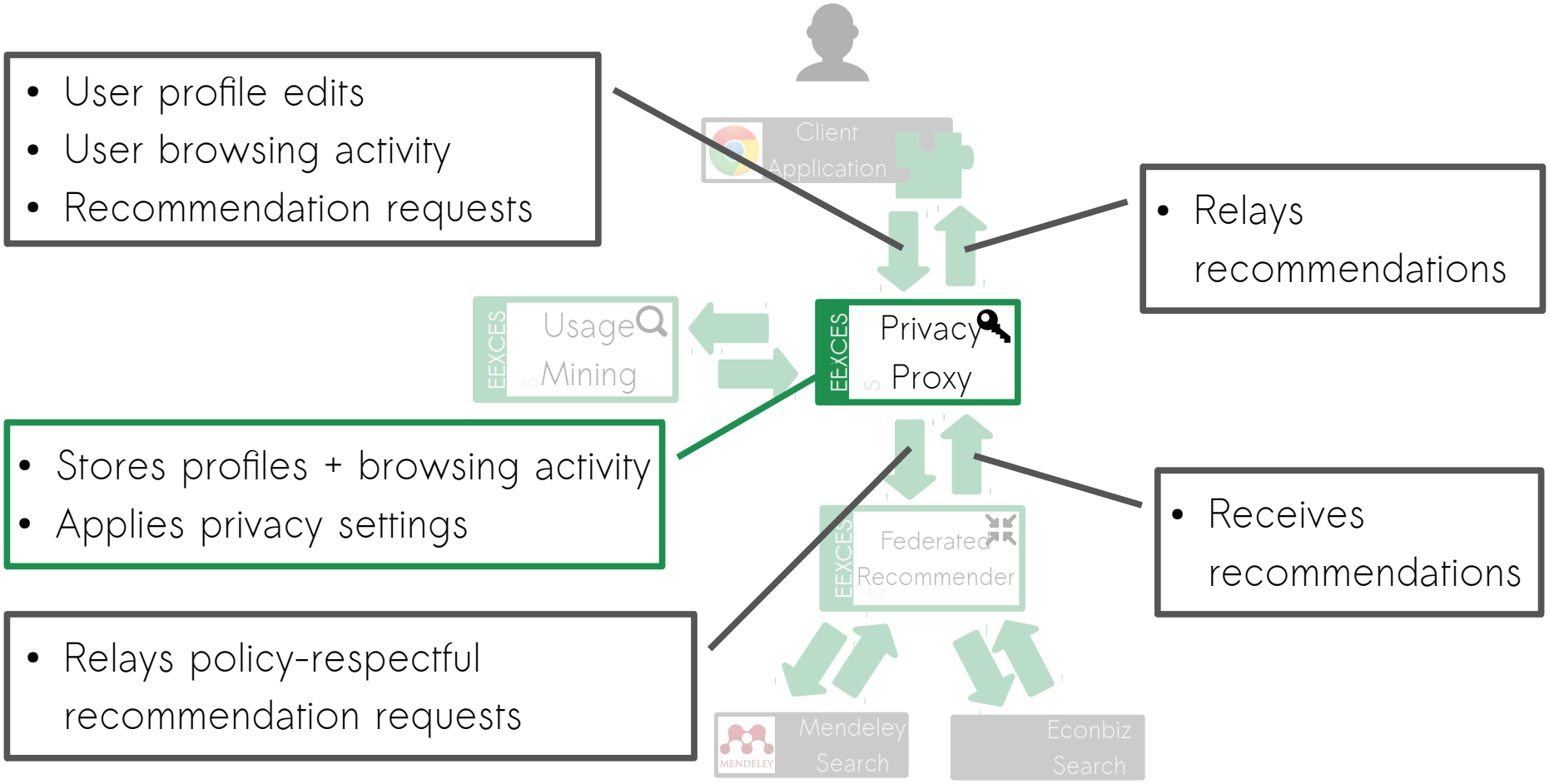
Privacy Plugin - Control & Feedback



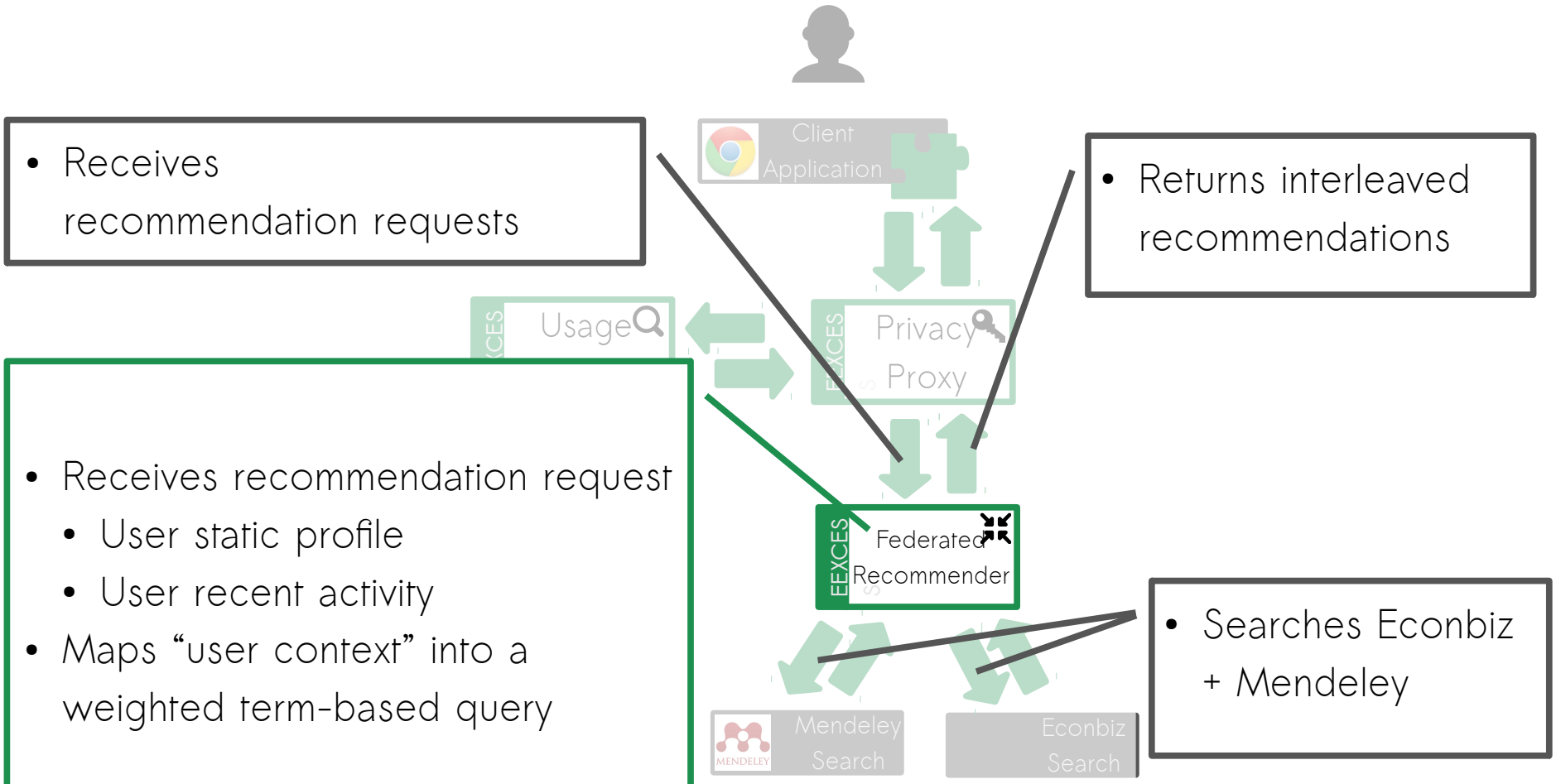
Privacy Plugin - Control & Feedback



Privacy Proxy - Protection



Basic Federated Recommender



- Receives recommendation requests
- Returns interleaved recommendations
- Receives recommendation request
  - User static profile
  - User recent activity
- Maps "user context" into a weighted term-based query
- Searches Econbiz + Mendeley

EEXCESS - Summary

- Quality
  - Recommendations adapted to the user
- Preserving privacy
  - Guaranteeing respect of privacy policy
- Scalability
  - Ensuring the whole system scales

- Quantifiable measures

EEXCESS - Future work

- Privacy-preserving search
- Measuring
  - recommendation quality
  - privacy impacts of disclosure
- Impacts of trustworthiness in peers

Contact

benjamin.habegger@insa-lyon.fr
http://www.linkedin.com/in/benjaminhabegger
@b_habegger

UNIVERSITÉ DE LYON

INSA LYON

LIRIS

EEXCESS