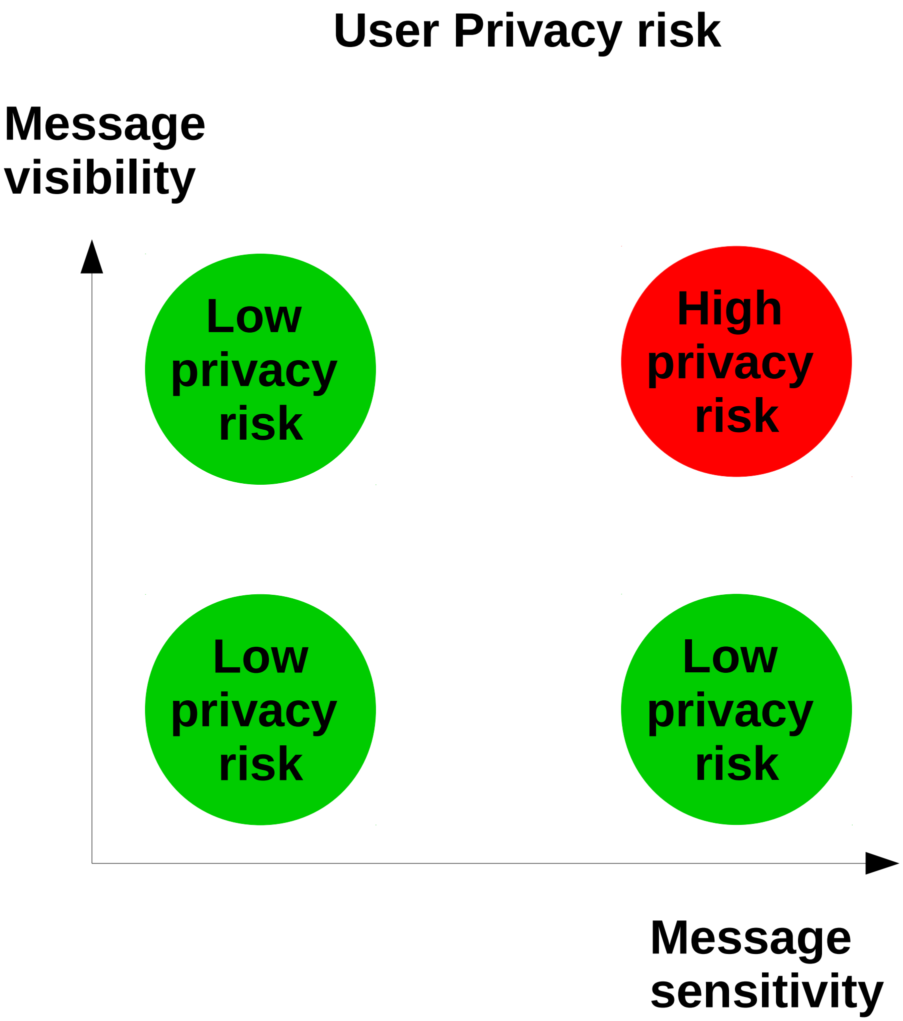
Plan of Presentation

1. Definition
2. Motivation
3. Privacy index
4. Privacy setting (computation)
   - Behavioral
     - Fuzzy c-means clustering
     - Item Response Theory
   - Social
     - Fake profiles / Spammers

1. Definition



- Privacy score is the trade-off between:
  - **Message sensitivity:**
    - Qualitative metric
  - **Message visibility:**
    - Quantitative metric

2. Motivation

Connection data	• SSL session • Device / log / Timezone • Cookies / Browsing history
Login data	• Email / Phone / Password
Mandatory data	• Name / birthday / gender
Extended profile data	• Education / hometown / languages • Political / religion / website / work
Application data	• Usage statistics / Scores • Permissions / Credit card
Interests	• Hobbies : Books / Music / Movies • Likes / Inspirational_people
Network data	• Family / Friends / Groups
Contextual data	• Taggable_friends / Tagged_places
Private communication Data	• **Private message** • Inbox / Outbox / Poke
Disclosed data	• Text post / Photo / Video • Check-in

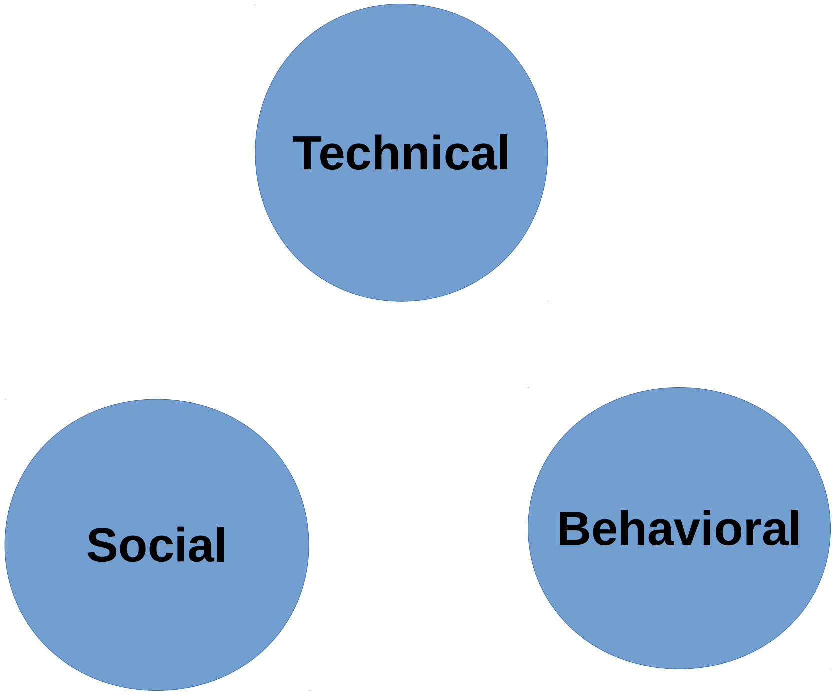
2. Motivation

Connection data	• SSL session • Device / log / Timezone • Cookies / Browsing history
Login data	• Email / Phone / Password
Mandatory data	• Name / birthday / gender
Extended profile data	• Education / hometown / languages • Political / religion / website / work
Application data	• Usage statistics / Scores • Permissions / Credit card
Interests	• Hobbies / Books / Music / Movies • Likes / Inspirational_people
Network data	• Family / Friends / Groups
Contextual data	• Taggable_friends / Tagged_places
Private communication Data	• **Private message** • Inbox / Outbox / Poke
Disclosed data	• Text post / Photo / Video • Check-in

Where are all this messages ?

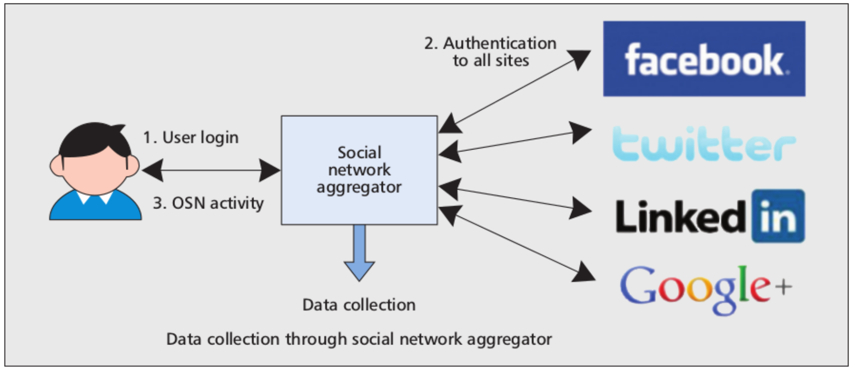
Can I measure their privacy ?

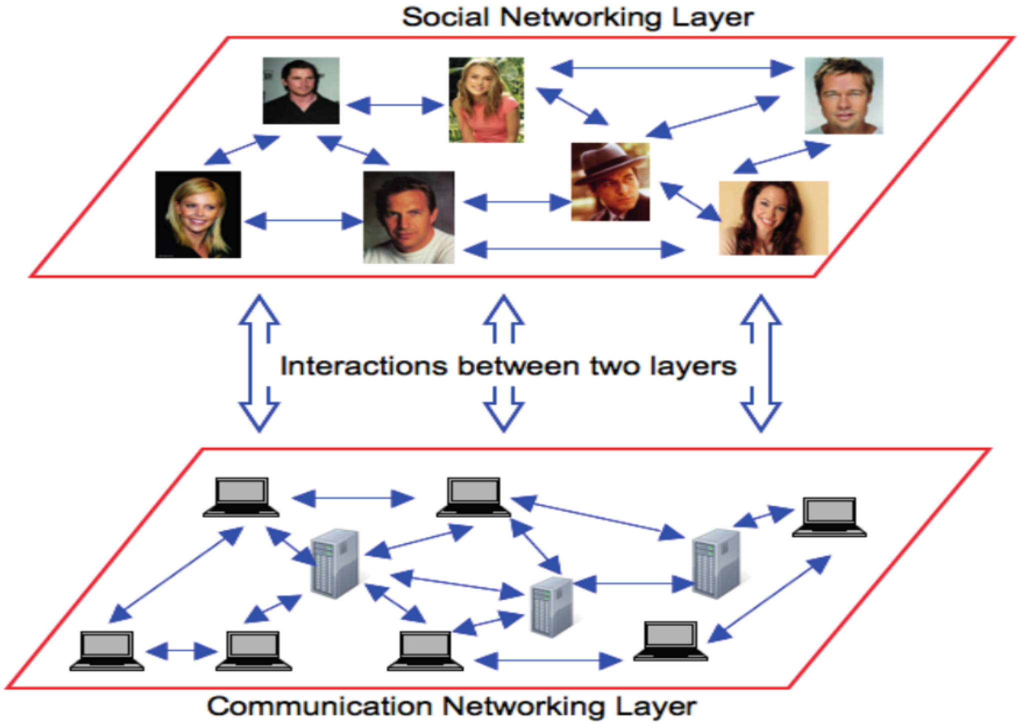
3. Privacy index



- **Behavioral**
  - Data: text, URL, Code
  - Data type: image, video
  - Nb of messages / day
- **Social**
  - Family / Friends / Groups
  - Spammers / Fake profile
- **Technical**
  - SSL session (SSL labs)
  - Device / log / Timezone
  - Cokies / Browsing history

3. Privacy index

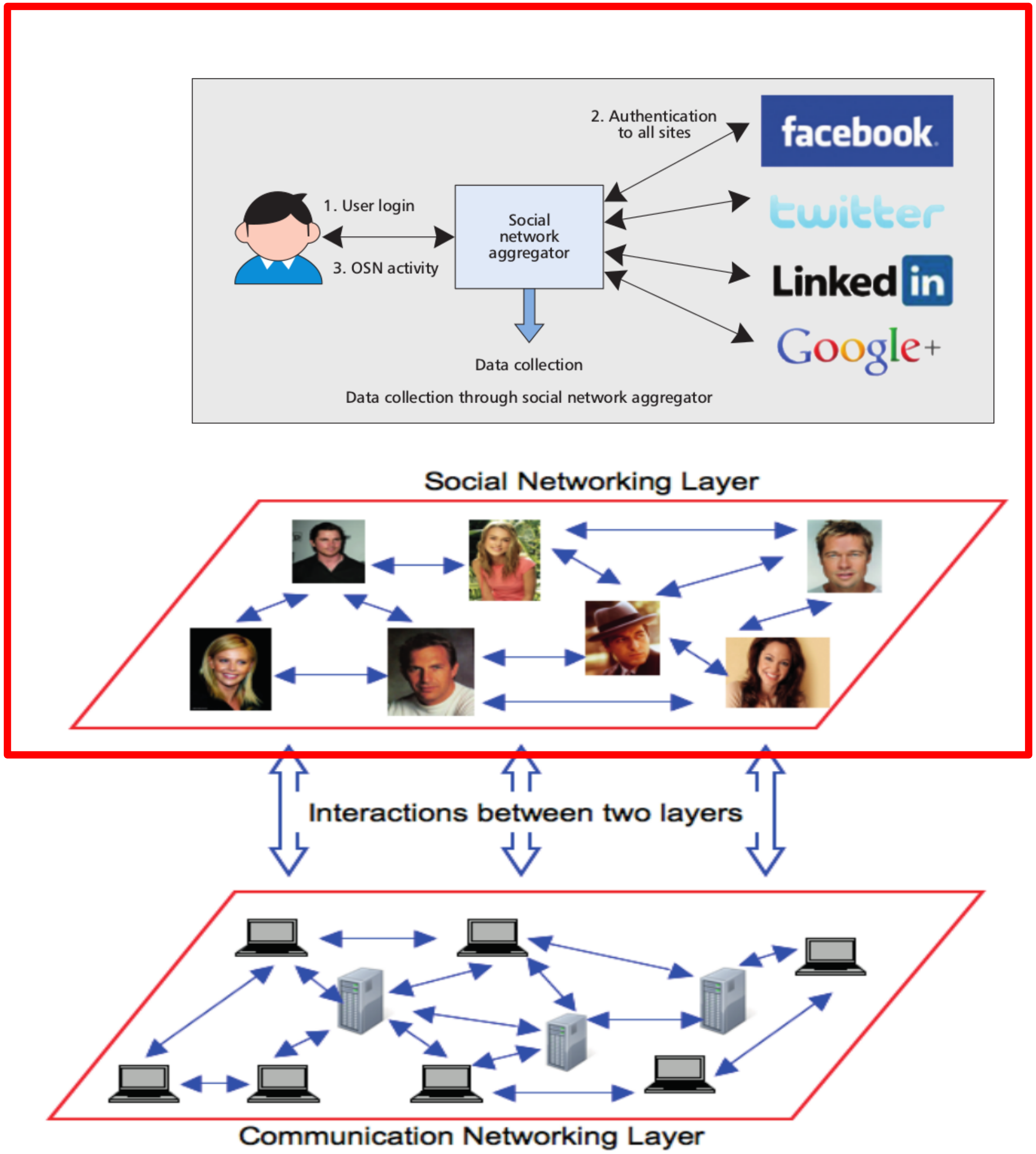

2. Authentication to all sites
facebook
twitter
LinkedIn
Google+
1. User login
3. OSN activity
Social network aggregator
Data collection
Data collection through social network aggregator


Social Networking Layer
Interactions between two layers
Communication Networking Layer

3 privacy layers → 3 privacy values

- **Behavioral**
  - Data: text, URL, Code
  - Data type: image, video
  - Nb of messages / day
- **Social**
  - Family / Friends / Groups
  - Spammers / Fake profile
- **Technical**
  - SSL session (SSL labs)
  - Device / log / Timezone
  - Cokies / Browsing history

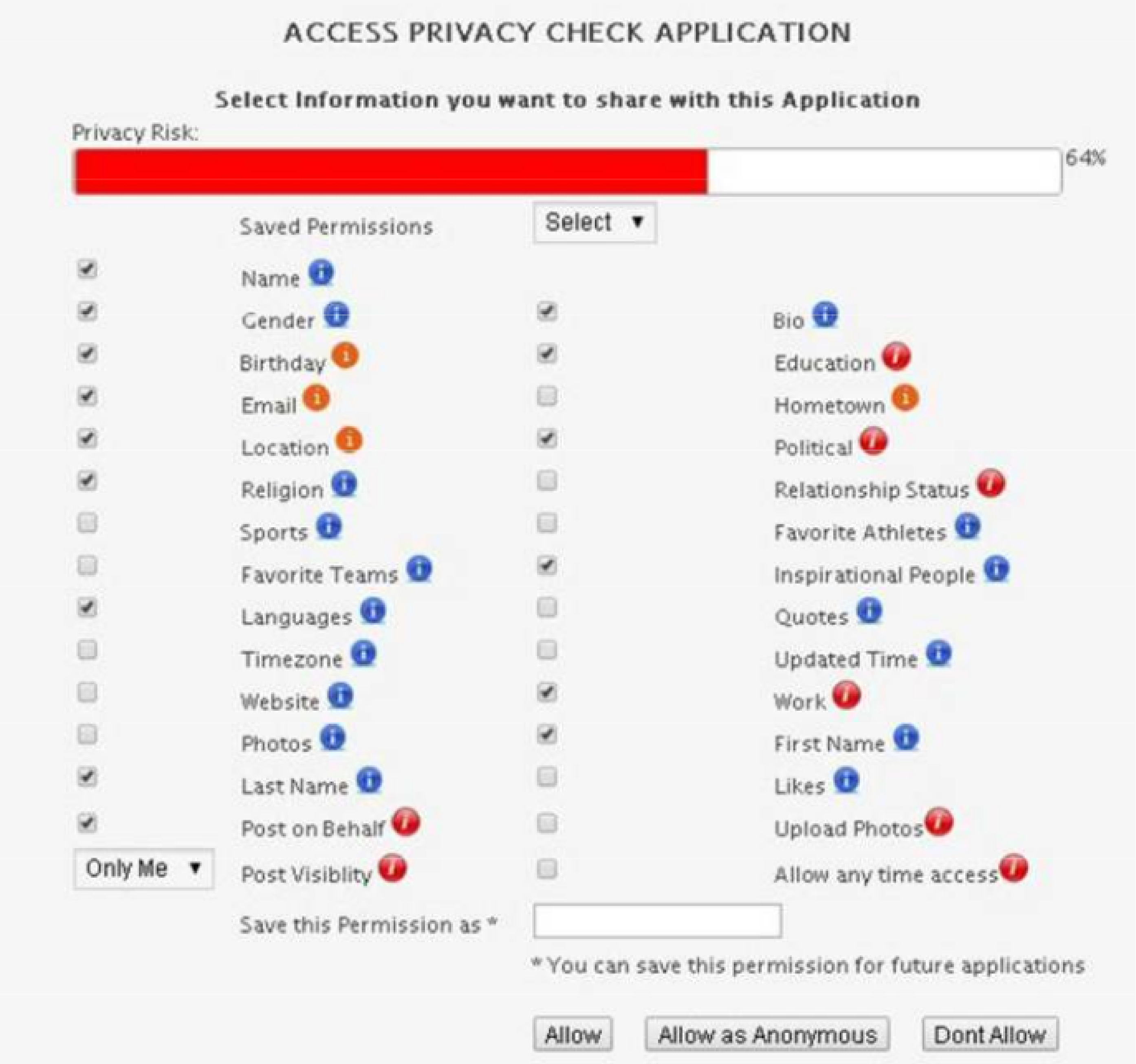
3. Privacy index


2. Authentication to all sites
facebook
twitter
LinkedIn
Google+
1. User login
3. OSN activity
Social network aggregator
Data collection
Data collection through social network aggregator
Social Networking Layer
Interactions between two layers
Communication Networking Layer

3 privacy layers → 3 privacy values

- **Behavioral**
  - Data: text, URL, Code
  - Data type: image, video
  - Nb of messages / day
- **Social**
  - Family / Friends / Groups
  - Spammers / Fake profile
- **Technical**
  - SSL session (SSL labs)
  - Device / log / Timezone
  - Cokies / Browsing history

3. Privacy index



ACCESS PRIVACY CHECK APPLICATION

Select Information you want to share with this Application

Privacy Risk: 64%

Saved Permissions: Select ▾

☑	Name		
☑	Gender	☑	Bio
☑	Birthday	☑	Education
☑	Email	□	Hometown
☑	Location	☑	Political
☑	Religion	□	Relationship Status
□	Sports	□	Favorite Athletes
□	Favorite Teams	☑	Inspirational People
☑	Languages	□	Quotes
□	Timezone	□	Updated Time
□	Website	☑	Work
□	Photos	☑	First Name
☑	Last Name	□	Likes
☑	Post on Behalf	□	Upload Photos
Only Me ▾	Post Visiblity	□	Allow any time access

Save this Permission as * ________

* You can save this permission for future applications

Controlling privacy disclosure of third party applications in online social networks (2016)

4. Privacy settings:
4.1 Behavioral privacy

Privacy settings Matrix

Sensitivity	β1	...	βn
User\Item	msg 1	...	msg n
User 1			
...		visibility	
User N			

- **Privacy score is the trade-off between:**
  - **message sensitivity**
  - **message visibility**

- data visibility and sensitivity depend on:
  - **Privacy settings matrix**

- **Behavioral privacy**
  - **Examples**
    1) **Fuzzy c-means clustering**
    2) **Item Response Theory**

4. Privacy settings:

4.1 Behavioral privacy

4.1.1 Fuzzy c-means clustering

- **Input**
  - Users: $U = \{ u_1, \dots , u_N \}$
  - Privacy settings: $S = \{ s_{(1,1)}, \dots , s_{(i,v)} \}$
    - ➔ Data type I = { MyActivity, ContactMe, MyRelations, MyTopics, PersonelInfo, VoteInfo }
    - ➔ Visibilities**:** V = { OnlyMe, Friends, FriendsOfFriends, Public }
- **Method**
  - **Fuzzy c-means clustering**
- **Output**
  - **Users behavior**

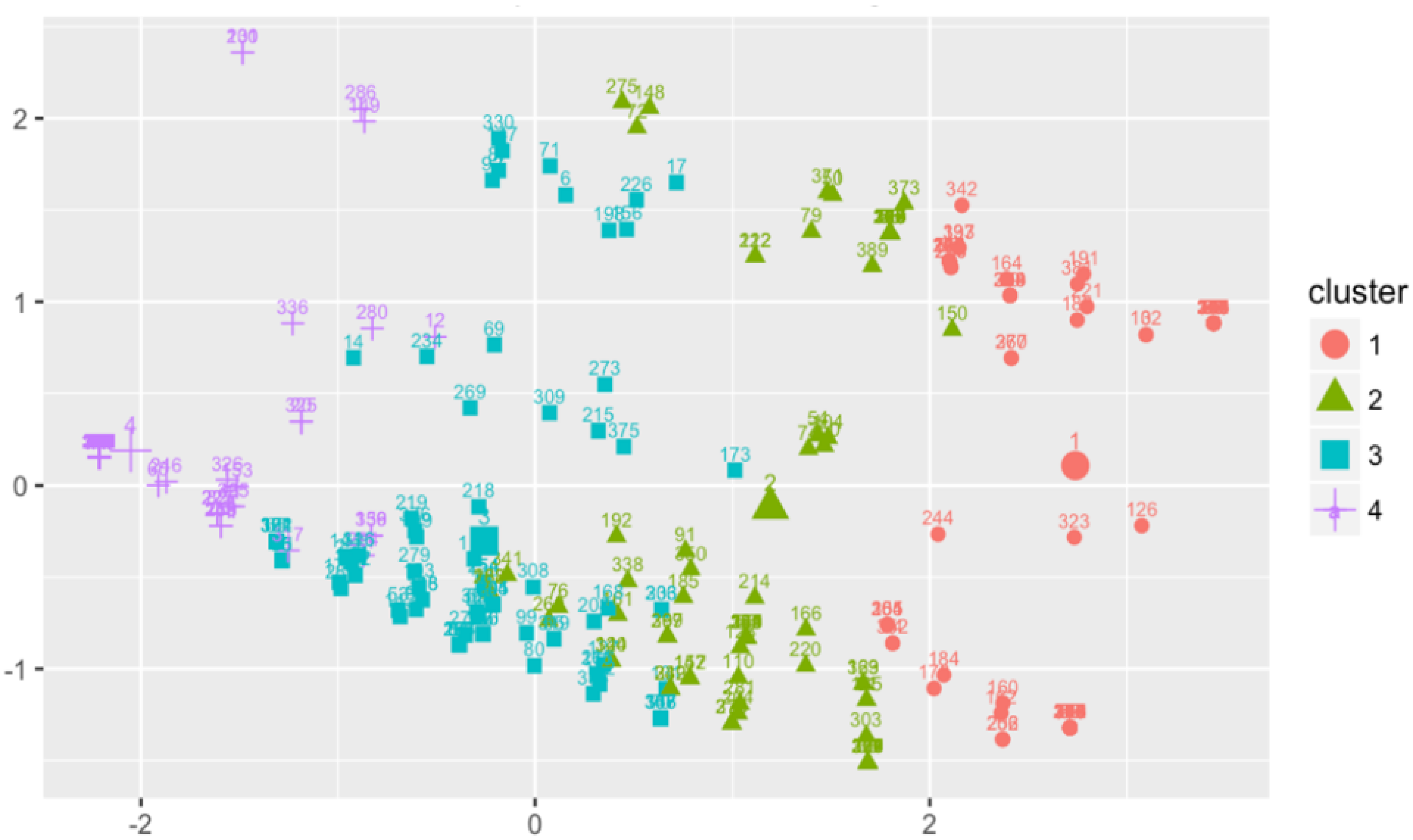
User	My Activity	Contact Me	My Relations	My Topics	Personal Info	Vote Intention
1	2	3	2	3	3	2
...	...	...	...	...	...	...
N	4	4	4	2	2	1

Privacy settings matrix

4. Privacy settings:

4.1 Behavioral privacy

4.1.1 Fuzzy c-means clustering



Fuzzy c-means clustering with 4 clusters

4. Privacy settings:

4.1 Behavioral privacy

4.1.1 Fuzzy c-means clustering

- **Input**
  - Users: $U = \{ u_1, \ldots , u_N \}$
  - Privacy settings: $S = \{ s_{(1,1)}, \ldots , s_{(i,v)} \}$
    - ➔ Data type I = { MyActivity, ContactMe, MyRelations, MyTopics, PersonelInfo, VoteInfo }
    - ➔ Visibilities**:** V = { OnlyMe, Friends, FriendsOfFriends, Public }
- **Method**
  - **Fuzzy c-means clustering**
- **Output**
  - **Users behavior**

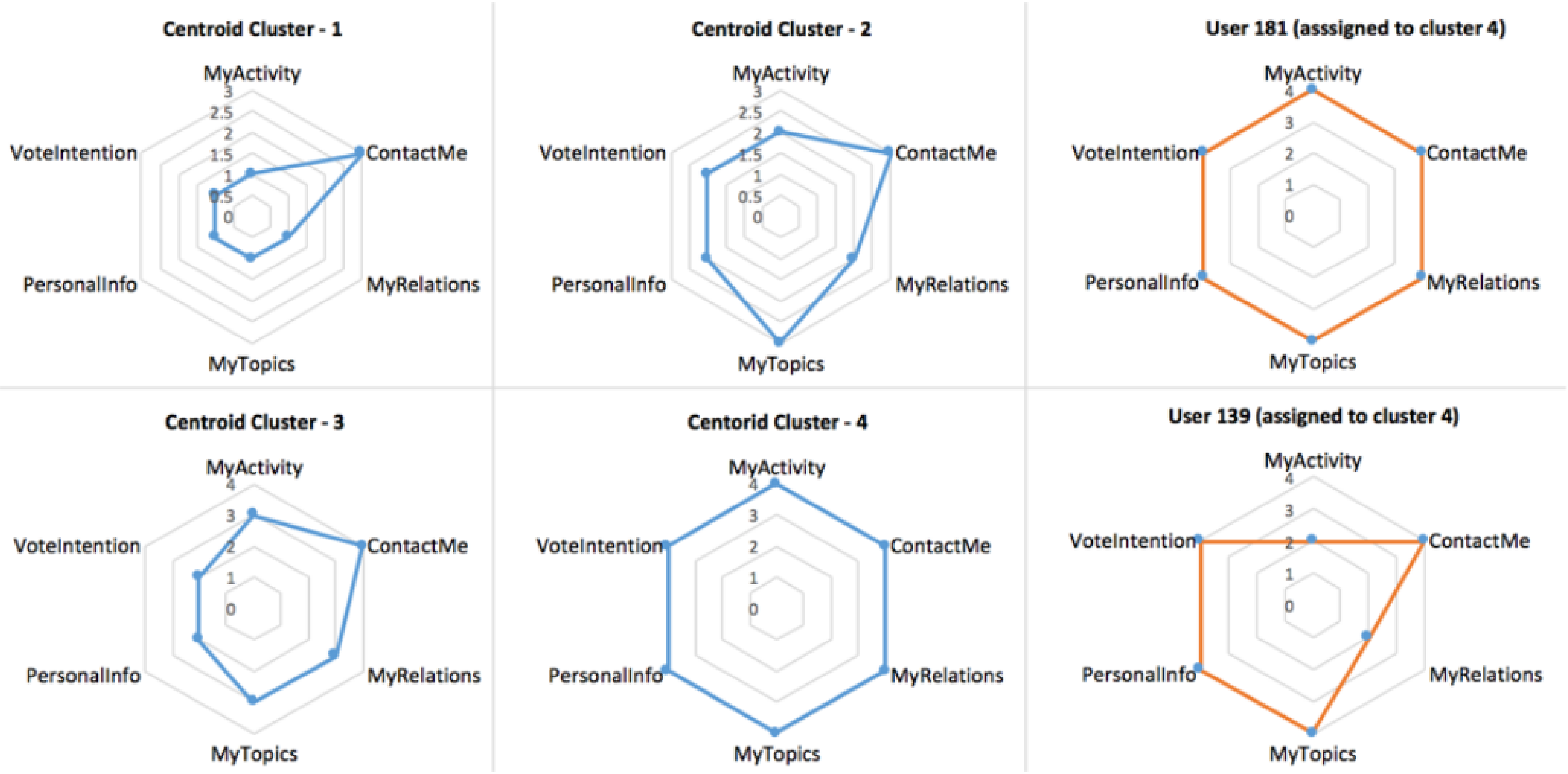
User	My Activity	Contact Me	My Relations	My Topics	Personal Info	Vote Intention
1	2	3	2	3	3	2
...	...	...	...	...	...	...
N	4	4	4	2	2	1

Privacy settings matrix

4. Privacy settings:

4.1 Behavioral privacy

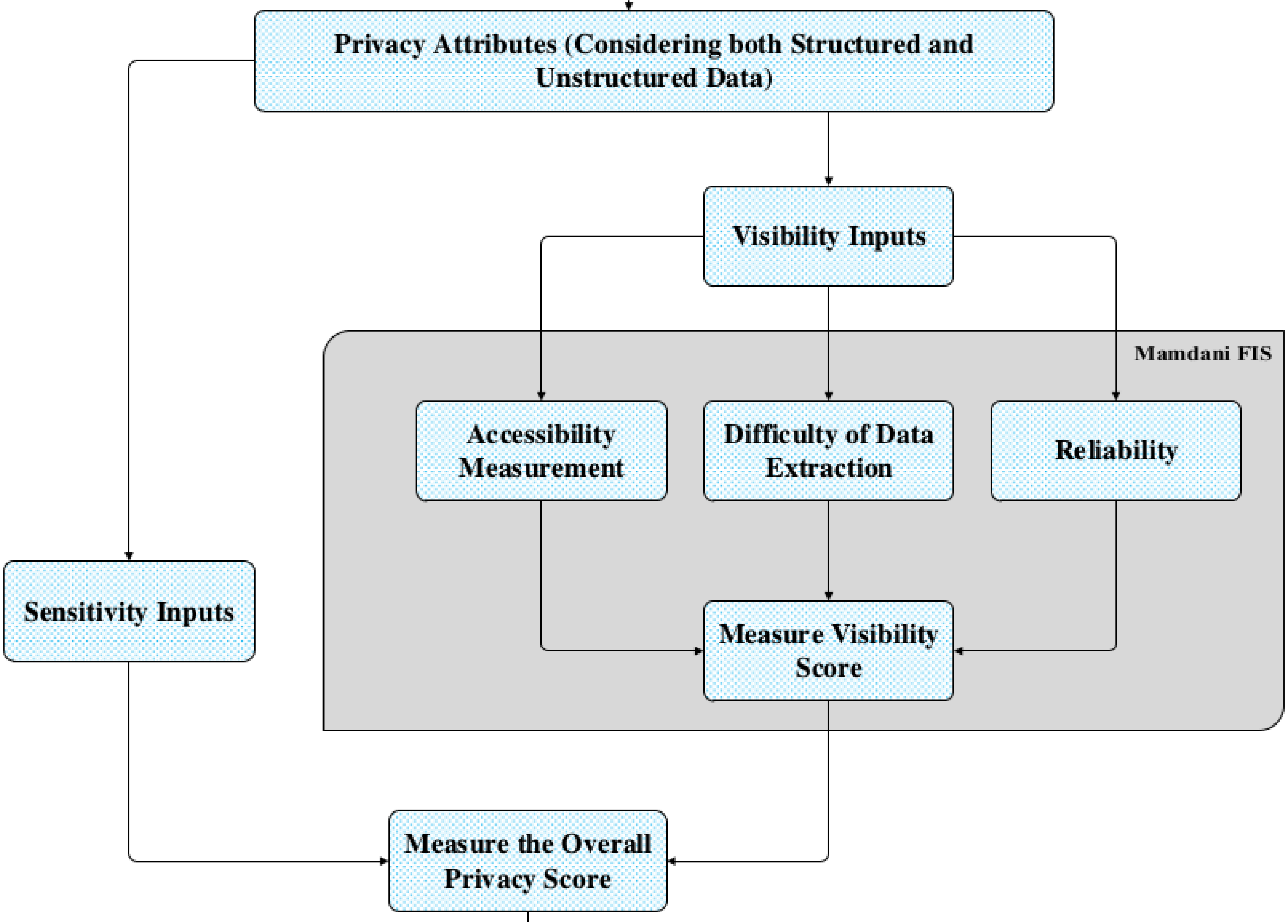
4.1.1 Fuzzy c-means clustering



4. Privacy settings:

4.1 Behavioral privacy

4.1.1 Fuzzy c-means clustering


Privacy Attributes (Considering both Structured and Unstructured Data)
Visibility Inputs
Mamdani FIS
Accessibility Measurement
Difficulty of Data Extraction
Reliability
Sensitivity Inputs
Measure Visibility Score
Measure the Overall Privacy Score

Scoring Users’ Privacy Disclosure Across Multiple Online Social Networks (2017)

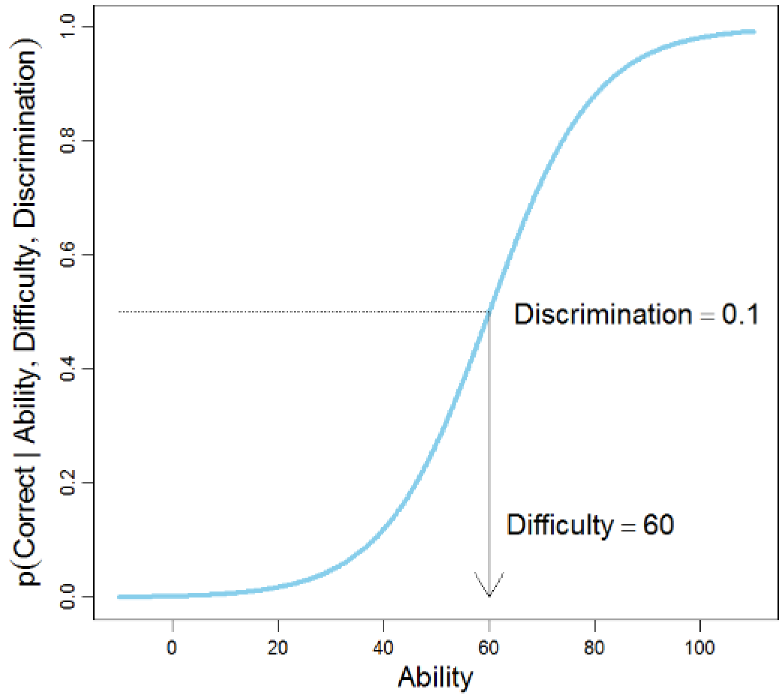
4. Privacy settings:

4.1 Behavioral privacy

4.1.2 Item Response Theory (IRT)

Privacy settings Matrix

	Sensitivity	β1	...	βn
Attitude	**User\Item**	**msg 1**	**...**	**msg n**
θ1	**User 1**			
	...		R(i,j)	
θN	**User N**			



- Privacy score is the trade-off between:
  - **message sensitivity**
  - **message visibility**

- data visibility and sensitivity depend on:
  - **Privacy settings matrix**

- **data visibility depends on:**
  - Response Matrix

    $$P_{ij} = Prob\{R(i,j)=k\}$$

    - **Item Response Theory (IRT)**

    $$P_{ij} = \frac{1}{1+e^{\alpha_i(\theta_j-\beta_i)}}$$

4. Privacy settings:
4.1 Behavioral privacy
4.1.2 Item Response Theory (IRT)

		Sensitivity	β1	...	βn
Privacy	Attitude	**User\Item**	**msg 1**	**...**	**msg n**
P_1	θ_1	**User 1**			
		...		R(i,j)	
P_N	θ_N	**User N**			

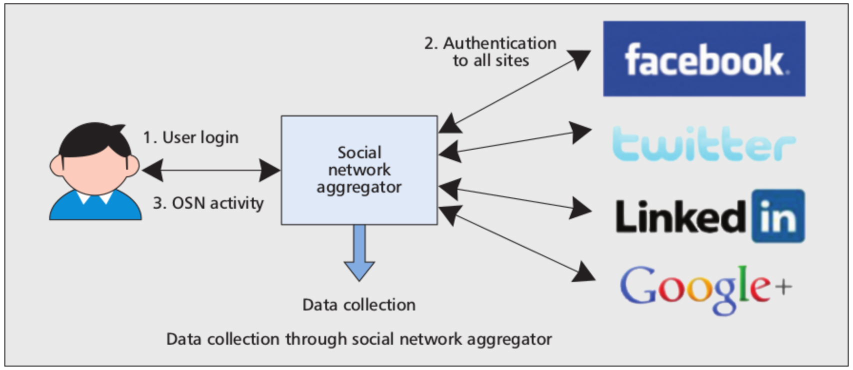
- $P_j = \sum_{i=1}^{n} \beta_i . V_{ij}$
- $V_{ij} = P_{ij}$
- $P_{ij} = \frac{1}{1+e^{\alpha_i(\theta_j - \beta_i)}}$
- $P_{ij} = Prob\{R(i,j)=k\}$

4. Privacy settings:

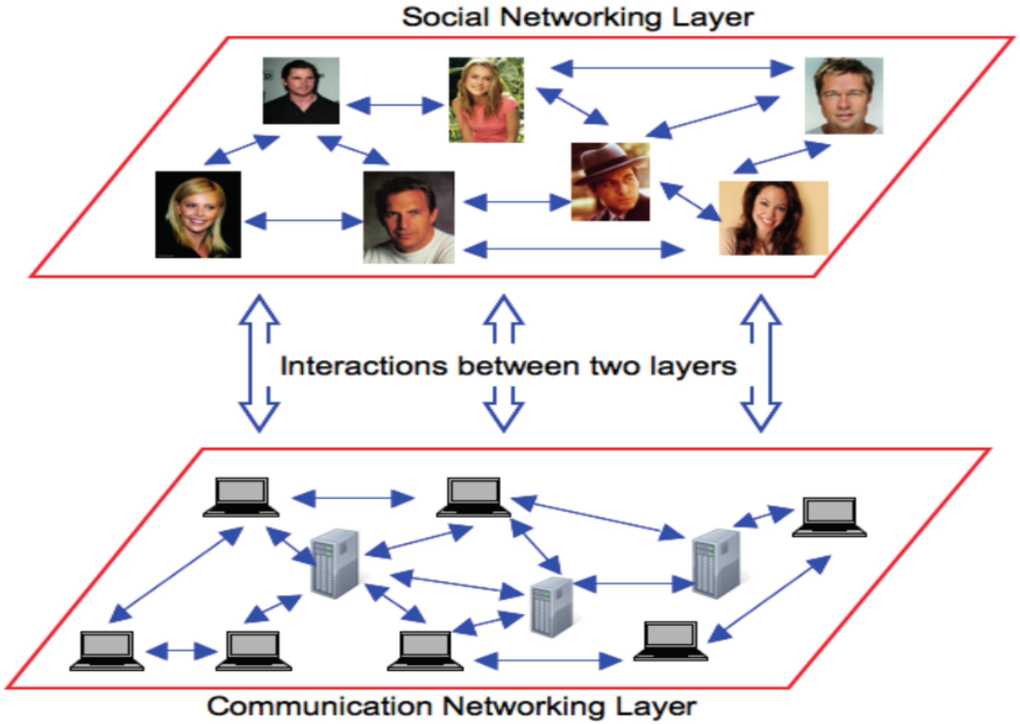
4.2 Social privacy

Authors	Features/Attributes	Type of features	Purpose
Zheng et al (2012): Sockpuppet detection in online discussion forums	- Nb of replies - Registration dates	Behavioral	Sock-puppet Detection
Zheng et al (2015): Detecting spammers on social networks	- Nb of reposts / Nb of Comments - Nb of Likes / Nb of Mentions - Nb of URL in the post - Nb of Hash-tags	Behavioral	Spammer Detection
Sarode et al (2015) : An experimental approach to detect fake profile in online social network	- Education and work - Relationship status / Gender - Nb of wall posts by the person - Nb of photos of person tagged - Nb of photos that has uploaded - Nb of tags in the uploaded photos	Non-Behavioral	Detection of Fake profiles
Zhou et al (2012): Feature analysis of spammers in social networks with active honeypots	- Micro-blogs - Followers / Followings - Friend Number - Nb of micro-blogs to get a fan	Non-Behavioral	Analysis of Spammers

Conclusion & challenges



Data collection through social network aggregator


Social Networking Layer
Interactions between two layers
Communication Networking Layer

- Privacy index requires:
  - Qualitative measurement
    - Message sensitivity
  - Quantitative measurement
    - Message visibility
- Behavioral privacy index :
  - Cluster model
  - Stochastic model
- Social privacy index:
  - Detect Spammer
  - Detect fake profile
- Technical privacy index:
  - (see SSL labs)

Thank you for your attention