A Framework for Computing the Privacy Scores of Users in Online Social Networks

Kun Liu

Yahoo! Labs (previously IBM Research)

September 11, 2009

The Team

IBM Almaden Research Center

- Tyrone Grandison

- Kun Liu

- Michael (Max) Maximilien

- Evimaria Terzi

IBM Silicon Valley Lab

- Sherry Guo

- Dwayne Richardson

- Tony Sun

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

Wait a minute, how come the talk is related
Credit Score?

From humble beginnings in 1956, Fair Isaac Corp.'s credit score has come to loom over consumer finance like no other statistical measure ever has.

So, how about a **Privacy Score** that indicates the privacy risk of online social-networking users?

Do you want to design a privacy score and other advanced privacy and risk management mechanisms so that 50 years (or much less) later, people will appreciate your effort?

Roadmap

- Motivation and Goal

- Privacy Score and Its Applications

- Privacy Score and Facebook/OpenSocial

- Proof of Concept: The Privacy-Aware Market Place

- Conclusions

Motivation

Millions of users share details of their personal lives with vast networks of friends, and often, strangers

Disclosure of personal info expose the users to identity theft, digital stalking, etc.

Courtesy to: http://www.contrib.andrew.cmu.edu/%7Egct/mygroup.html

Courtesy to: http://i.ehow.com/images/GlobalPhoto/Articles/4873454/identity-theft-protect-yourself-main_Full.jpg

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/
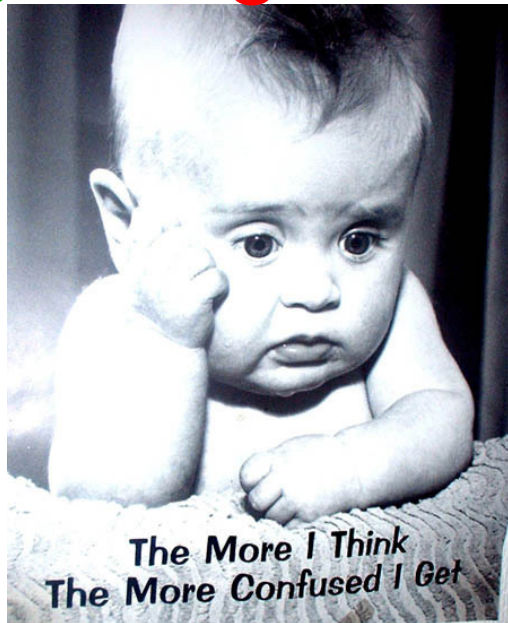
Goal

- Our goal is to develop a mechanism that is able to

  - Measure/monitor the privacy risk of social-networking users

  - Boost public awareness of privacy

  - Help users to easily manage their information sharing

- Our goal is NOT to prevent people from sharing information

- How to achieve this goal?

  - Privacy-score calculation

  - Comprehensive information-sharing report

  - Privacy-settings recommendation

  - and more …

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

Life Cycle of Privacy Score
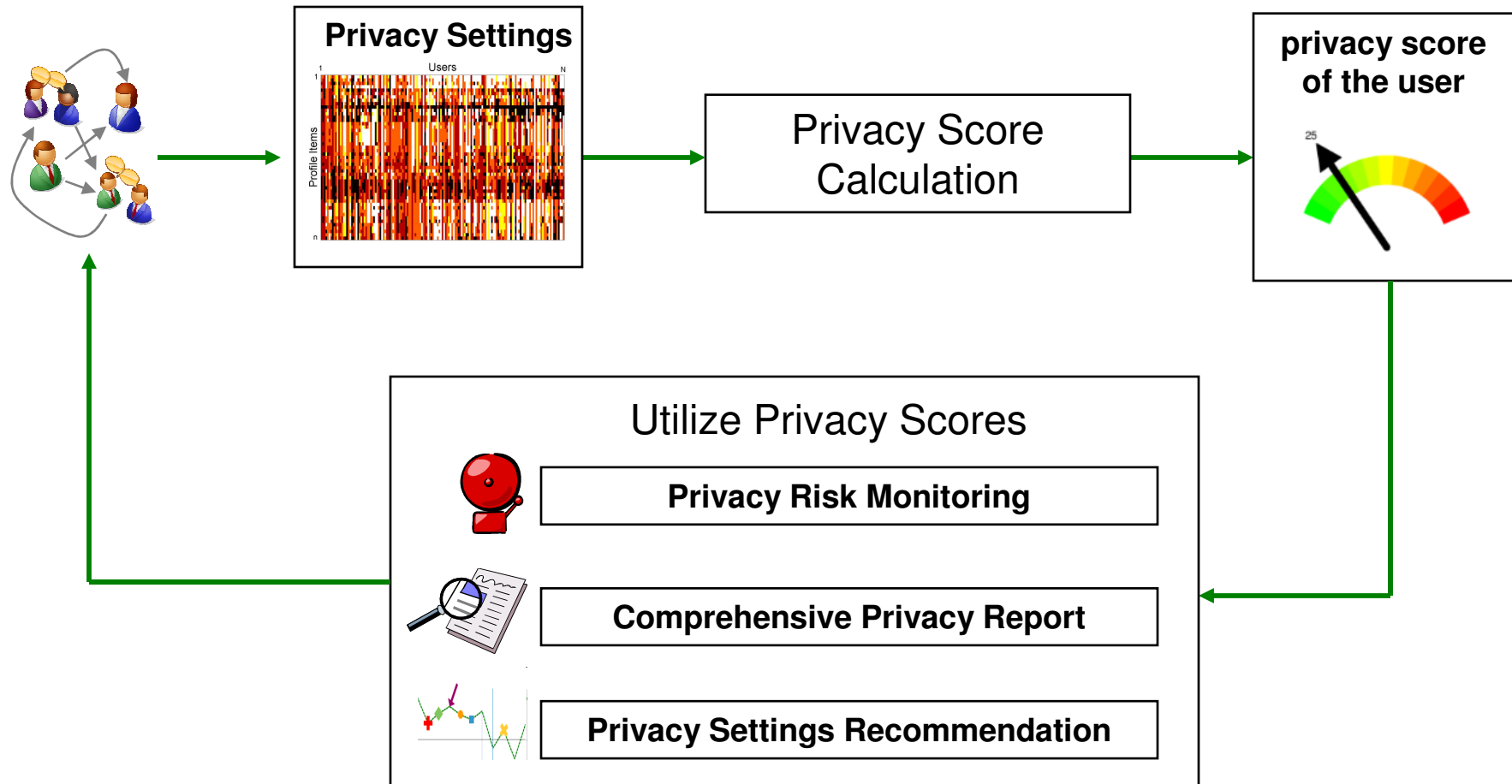
Privacy Settings

Privacy Score Calculation

privacy score of the user

Utilize Privacy Scores

Privacy Risk Monitoring

Comprehensive Privacy Report

Privacy Settings Recommendation

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

Roadmap

- Motivation and Goal

- **Privacy Score and Its Applications**

- Privacy Score and Facebook/OpenSocial

- Proof of Concept: The Privacy-Aware Market Place

- Conclusions

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/
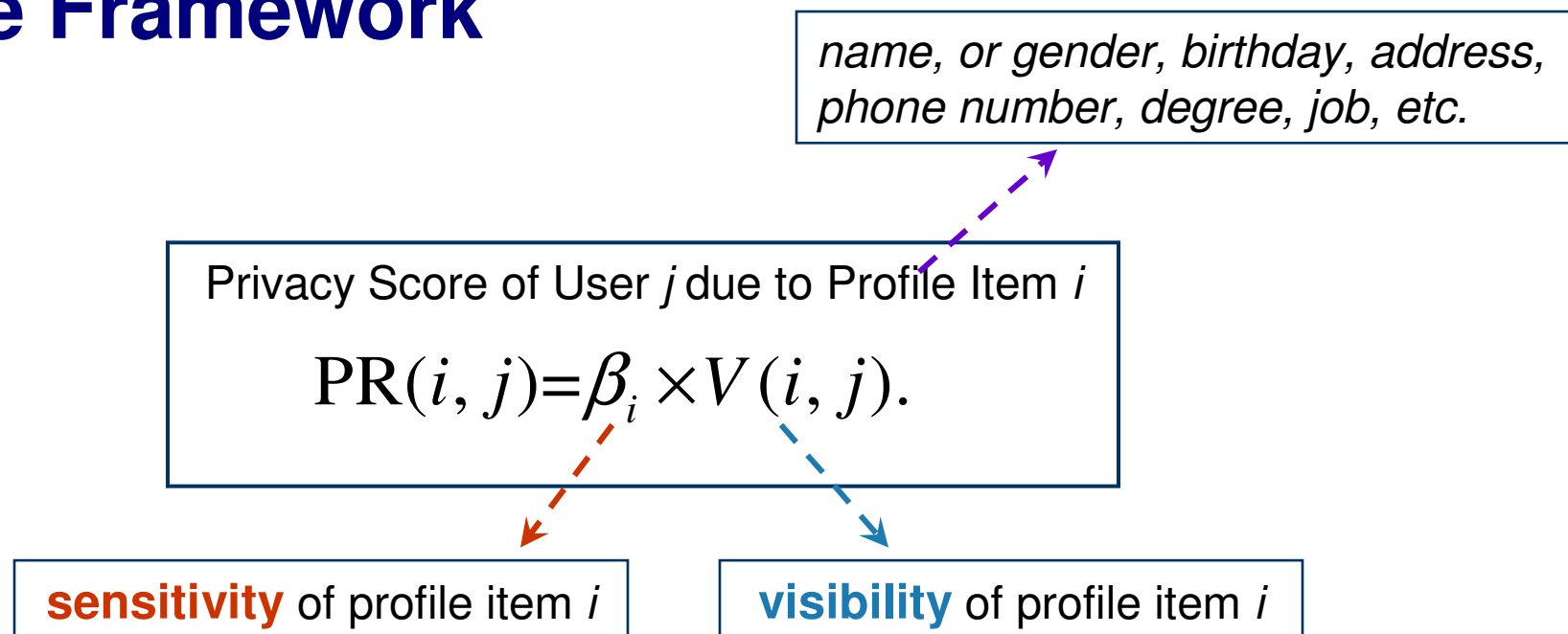
Basic Premises of Privacy Score

- **Sensitivity**: The more sensitive the information revealed by a user, the higher his privacy risk.

mother's maiden name is more sensitive than *mobile-phone number*

- **Visibility**: The wider the information about a user spreads, the higher his privacy risk.

home address known *by everyone* poses higher risks than *by friends only*

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

The Framework

name, or gender, birthday, address, phone number, degree, job, etc.

Privacy Score of User j due to Profile Item i

$$\text{PR}(i,j) = \beta_i \times V(i,j).$$

sensitivity of profile item i

visibility of profile item i

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

The Framework

name, or gender, birthday, address, phone number, degree, job, etc.

Privacy Score of User j due to Profile Item i

$$PR(i, j) = \beta_i \times V(i, j).$$

sensitivity of profile item i

visibility of profile item i

Overall Privacy Score of User j

$$PR(j) = \sum_i PR(i, j) = \sum_i \beta_i \times V(i, j).$$

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

The Naïve Approach

	User_1					User_j				User_N
Profile Item_1 (birthday)	R(*1, 1*)	R(*1, 2*)								R(*1, N*)
Profile Item_i (cell phone #)						R(*i, j*)				
Profile Item_n	R(*n, 1*)									R(*n, N*)

☐ **share, R(*i, j*) = 1**

▨ **not share, R(*i, j*) = 0**

The Naïve Approach

	User_1					User_j				User_N
Profile Item_1 (birthday)	R(1, 1)	R(1, 2)								R(1, N)
Profile Item_i (cell phone #)						R(i, j)				
Profile Item_n	R(n, 1)									R(n, N)

$$|R_i| = \sum_j R(i, j)$$

☐   **share, R(i, j) = 1**

▨   **not share, R(i, j) = 0**

Sensitivity: $\beta_i = \dfrac{N - |R_i|}{N}$

The Naïve Approach

$$|R_i| = \sum_j R(i, j)$$

$$|R^j| = \sum_i R(i, j)$$

share, $R(i, j) = 1$

not share, $R(i, j) = 0$

Sensitivity: $\beta_i = \dfrac{N - |R_i|}{N}$

Visibility: $V(i, j) = \Pr\{R(i, j) = 1\} \times 1 + \Pr\{R(i, j) = 0\} \times 0$

The Naïve Approach

	User_1					User_j				User_N
Profile Item_1 (birthday)	R(1, 1)	R(1, 2)								R(1, N)
Profile Item_i (cell phone #)						R(i, j)				
Profile Item_n	R(n, 1)									R(n, N)

$$|R_i| = \sum_j R(i, j)$$

$$|R^j| = \sum_i R(i, j)$$

☐ share, R(i, j) = 1
▨ not share, R(i, j) = 0

Sensitivity: $\beta_i = \dfrac{N - |R_i|}{N}$

Visibility: $V(i, j) = \Pr\{R(i, j) = 1\} \times 1 + \Pr\{R(i, j) = 0\} \times 0$

$$\Pr\{R(i, j) = 1\} = \dfrac{|R_i|}{N} \times \dfrac{|R^j|}{n}$$

Item Response Theory (IRT)

- IRT (Lawley,1943 and Lord,1952) has its origin in psychometrics.

- It is used to analyze data from questionnaires and tests.

- It is the foundation of Computerized Adaptive Test like GRE, GMAT

Item Characteristic Curve (ICC)

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/
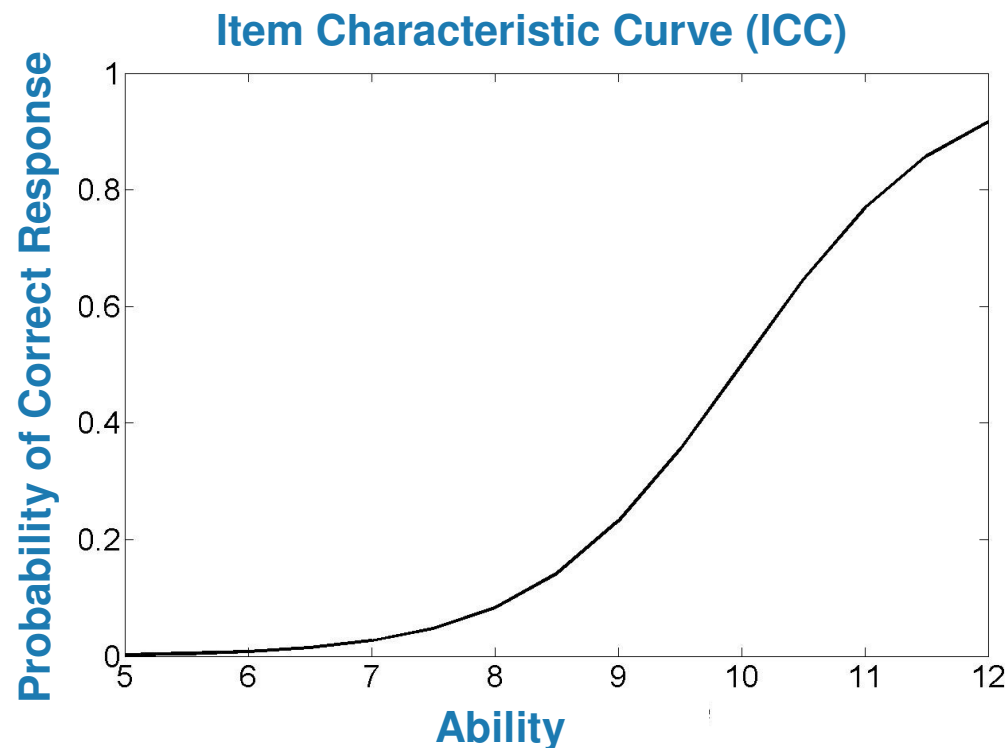
Item Characteristic Curve (ICC)

$$\Pr\{R(i,j)=1\} = \frac{1}{1+e^{-\alpha_i(\theta_j-\beta_i)}}$$

Question i's discrimination

Student j's ability

Question i's difficulty

Item Characteristic Curve

Probability of Correct Response

- $\beta_1 = 10.5$, $\alpha_1 = 1.0$
- $\beta_2 = 11.5$, $\alpha_2 = 1.0$

Question 1

Question 2

ability θ_i

β_1 β_2
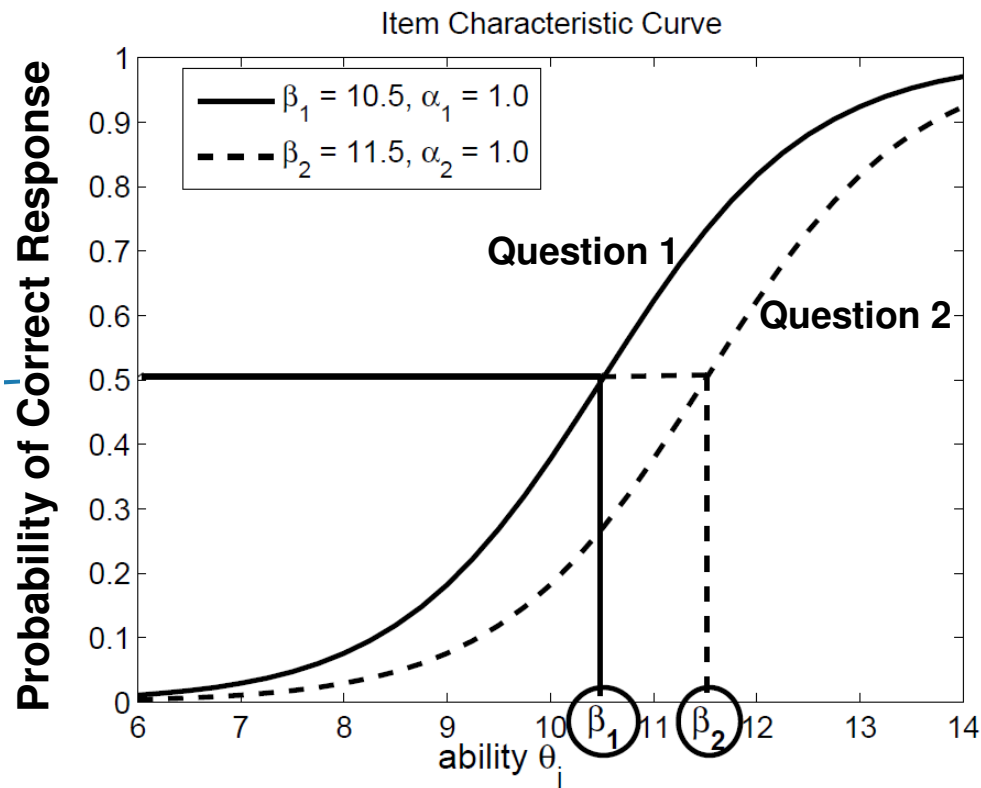
The Item Response Theory (IRT) Approach

$$P_{ij} = \Pr\{R(i, j) = 1\} = \frac{1}{1 + e^{-\alpha_i(\theta_j - \beta_i)}}$$

Profile item's discrimination

User's attitude, e.g., conservative or extrovert

Profile item's sensitivity

Profile item i's true visibility

Calculating Privacy Score using IRT

Overall Privacy Score of User j

$$\mathrm{PR}(j) = \sum_i \beta_i \times V(i, j)$$

Sensitivity: β_i

Visibility: $V(i, j) = \mathrm{Pr}\{R(i, j) = 1\}$

$$P_{ij} = \mathrm{Pr}\{R(i, j) = 1\} = \frac{1}{1 + e^{-\alpha_i(\theta_j - \beta_i)}}$$

byproducts: profile item's discrimination and user's attitude
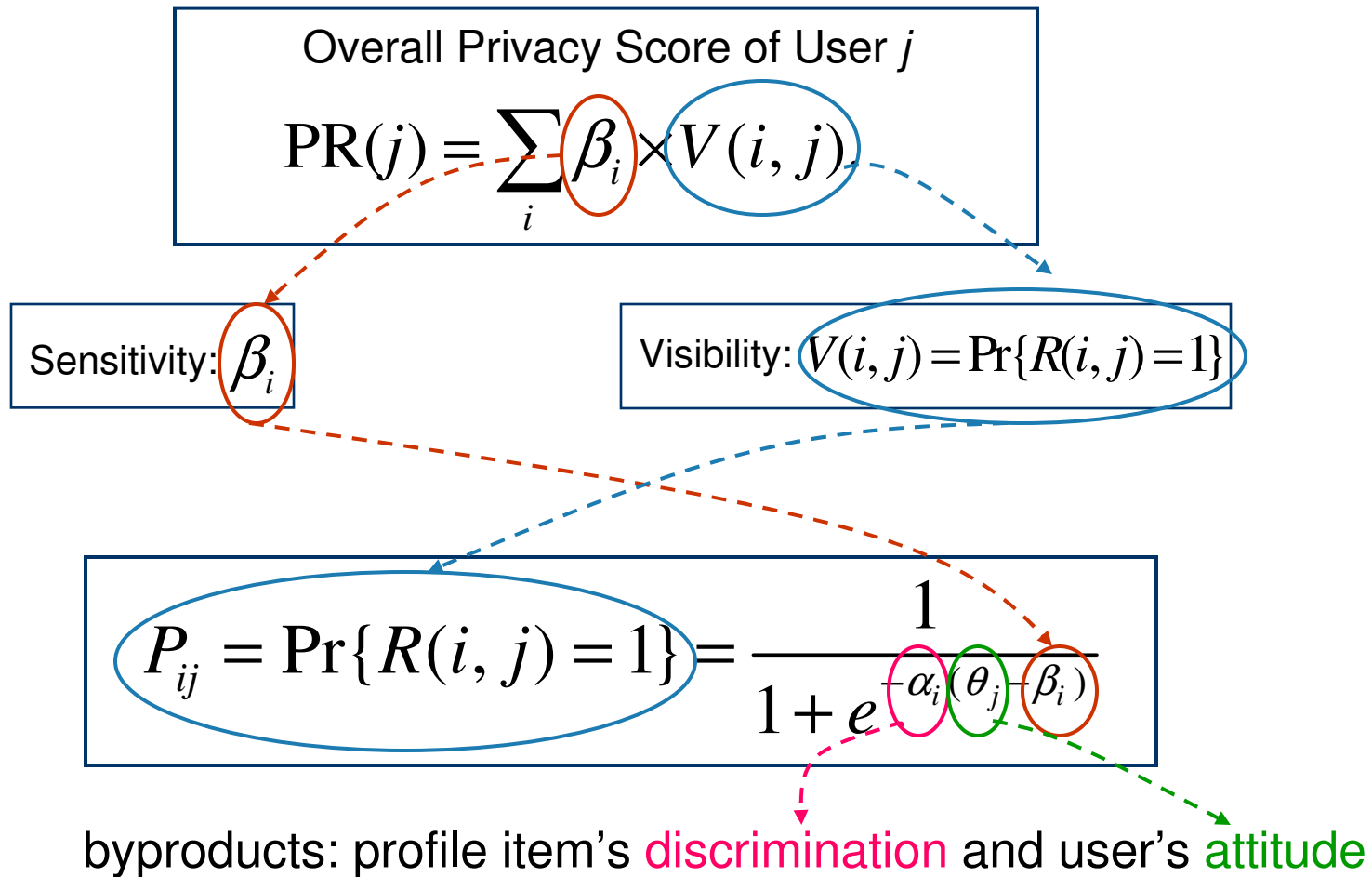
All parameters can be estimated using
Maximum Likelihood Estimation and Expectation-Maximization.

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

Advantages of the IRT Model

- The mathematical model fits the observed data well

- The quantities IRT computes (*i.e.*, sensitivity, attitude and visibility) have intuitive interpretations

- Computation is parallelizable using e.g. MapReduce

- Privacy scores calculated within different social networks are comparable

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

Interesting Results from User Study

We collected the information-sharing preferences of **153 users** on **49 profile items** such as *name, gender, birthday, political views, address, phone number, degree, job*, etc.

Statistics

- 49 profile items
- 153 users from 18 countries/regions
- 53.3% are male and 46.7% are female
- 75.4% are in the age of 23 to 39
- 91.6% hold a college degree or higher
- 76.0% spend 4+ hours online per day

Sensitivity of The Profile Items Computed by IRT Model

Average Privacy Scores Grouped by Geographical Regions
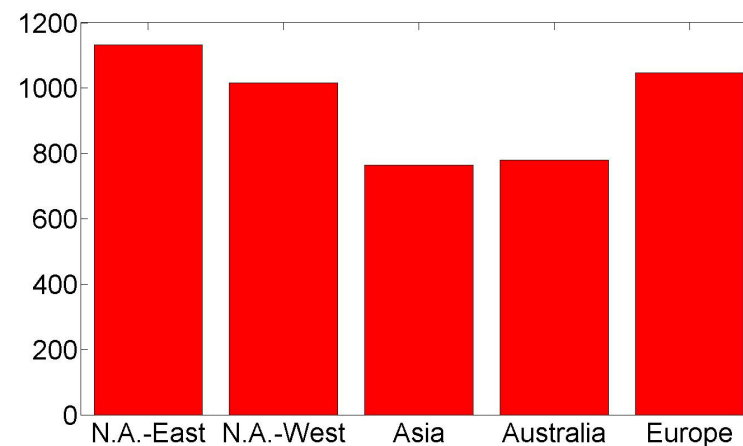
Utilize Privacy Scores

- Privacy Risk Monitoring

- Privacy (Information Sharing) Report

- Privacy Settings Recommendation

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

Roadmap

- Motivation and Goal

- Privacy Score and Its Applications

- **Privacy Score and Facebook/OpenSocial**

- Proof of Concept: The Privacy-Aware Market Place

- Conclusions

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

Privacy Score and Facebook/OpenSocial

Provide native implementation of **Privacy Score** computation.

Enable application developers to implement their own **Privacy Scores.**

Enable application developers to build **Information Sharing Report** modules and **Privacy Settings Recommendation** modules.

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

Roadmap

- Motivation and Goal

- Privacy Score and Its Applications

- Privacy Score and Facebook/OpenSocial

- **Proof of Concept: The Privacy-Aware Market Place**

- Conclusions

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

Privacy-aware Marketplace (PaMP)

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

Conclusions

- In this talk, we have discussed

  - the importance of privacy score and privacy management

  - two ways to compute privacy score using privacy settings

- Our goal is to develop a mechanism and a platform that will

  - Measure/monitor the privacy risk of social-networking users

  - Boost public awareness of privacy

  - Help users to easily manage their information sharing

- We believe that

  - simple and effective privacy management makes one feels safe and comfortable about sharing information online, which will eventually facilitate the information sharing and integration.

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/

Thank you and Questions?

References: http://www.almaden.ibm.com/cs/projects/iis/ppn/