Probabilistic Prediction of Privacy Risks in User Search Histories

Joanna Biega
Ida Mele
Gerhard Weikum

PSBD@CIKM, Shanghai, 07.11.2014
Or rather:

On diverging towards user-centric privacy
Traditional privacy protection scenario

<table>
<thead>
<tr>
<th>gender</th>
<th>age</th>
<th>disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>male</td>
<td>37</td>
</tr>
<tr>
<td>user2</td>
<td>male</td>
<td>37</td>
</tr>
<tr>
<td>user3</td>
<td>female</td>
<td>42</td>
</tr>
</tbody>
</table>
Traditional privacy protection scenario

<table>
<thead>
<tr>
<th></th>
<th>gender</th>
<th>age</th>
<th>disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>male</td>
<td>37</td>
<td>cancer</td>
</tr>
<tr>
<td>user2</td>
<td>male</td>
<td>37</td>
<td>heart d.</td>
</tr>
<tr>
<td>user3</td>
<td>female</td>
<td>42</td>
<td>cancer</td>
</tr>
</tbody>
</table>

Is this Molly?

Adversary
Traditional privacy protection scenario

<table>
<thead>
<tr>
<th></th>
<th>gender</th>
<th>age</th>
<th>disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>male</td>
<td>37</td>
<td>cancer</td>
</tr>
<tr>
<td>user2</td>
<td>male</td>
<td>37</td>
<td>heart d.</td>
</tr>
<tr>
<td>user3</td>
<td>female</td>
<td>42</td>
<td>cancer</td>
</tr>
</tbody>
</table>

Is this Molly?

Adversary

k-anonymity
l-diversity
t-closeness
differential privacy
Traditional privacy protection scenario

<table>
<thead>
<tr>
<th>gender</th>
<th>age</th>
<th>disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>male</td>
<td>37</td>
</tr>
<tr>
<td>user2</td>
<td>male</td>
<td>37</td>
</tr>
<tr>
<td>user3</td>
<td>female</td>
<td>42</td>
</tr>
</tbody>
</table>

Is this Molly?

This can be orthogonal

Adversary

k-anonymity
l-diversity
t-closeness
differential privacy
Traditional privacy protection scenario

<table>
<thead>
<tr>
<th>gender</th>
<th>age</th>
<th>disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>male</td>
<td>37</td>
</tr>
<tr>
<td>user2</td>
<td>male</td>
<td>37</td>
</tr>
<tr>
<td>user3</td>
<td>female</td>
<td>42</td>
</tr>
</tbody>
</table>

Probabilistic inference

Adversary

This can be orthogonal

Is this Molly?

k-anonymity
l-diversity
t-closeness
differential privacy
Traditional privacy protection scenario

<table>
<thead>
<tr>
<th>gender</th>
<th>age</th>
<th>disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>male</td>
<td>37</td>
</tr>
<tr>
<td>user2</td>
<td>male</td>
<td>37</td>
</tr>
<tr>
<td>user3</td>
<td>female</td>
<td>42</td>
</tr>
</tbody>
</table>

Probabilistic inference

Is this Molly?

This can be orthogonal

Adversary

Only part of the dataset known

k-anonymity

l-diversity

t-closeness

differential privacy
The concerns of a modern user
The concerns of a modern user

I’m falling into depression. I don’t want my insurance company to know before I take an action!
The concerns of a modern user

I’m falling into depression. I don’t want my insurance company to know before I take an action!

I’m a female user in an online tech community. Can I earn reputation easily?
The concerns of a modern user

I’m a female user in an online tech community. Can I earn reputation easily?

I’m falling into depression. I don’t want my insurance company to know before I take an action!

I’m pregnant but don’t want my employer to know yet.
The concerns of a modern user

I’m falling into depression. I don’t want my insurance company to know before I take an action!

I’m rich and buying online. Do I get the same price?

I’m a female user in an online tech community. Can I earn reputation easily?

I’m pregnant but don’t want my employer to know yet.
What are the side effects of Xanax?

anxiety
psychotherapist NY
Xanax side effects

More privacy control...

<table>
<thead>
<tr>
<th></th>
<th>gender</th>
<th>age</th>
<th>disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>male</td>
<td>37</td>
<td>cancer</td>
</tr>
<tr>
<td>user2</td>
<td>male</td>
<td>37</td>
<td>heart d.</td>
</tr>
<tr>
<td>user3</td>
<td>female</td>
<td>42</td>
<td>cancer</td>
</tr>
</tbody>
</table>
What are the side effects of Xanax?
More privacy control on the user side!

What are the side effects of Xanax?

Privacy advisor

How about:
- not posting this content?
- posting anonymously?
- posting obfuscating queries?
Quantifying privacy risks

\[ P(\text{IsDepressed} = \text{True}|\text{hasGender} = \text{female}, \text{livesIn} = \text{US}) = 0.01 \]
What are the side effects of Xanax?

\[ P(\text{IsDepressed} = \text{True}|\text{hasGender} = \text{female}, \text{livesIn} = \text{US}) = 0.01 \]
What are the side effects of Xanax?

\[ P(\text{IsDepressed} = \text{True} | \text{hasGender} = \text{female}, \text{livesIn} = \text{US}) = 0.01 \]

\[ P(\text{IsDepressed} = \text{True} | \text{hasGender} = \text{female}, \text{livesIn} = \text{US}, \text{soughtSideEffectsOf} = \text{Xanax}) = 0.3 \]
What are the side effects of Xanax?

\[ P(\text{IsDepressed} = \text{True}|\text{hasGender} = \text{female}, \text{livesIn} = \text{US}) = 0.01 \]

\[ P(\text{IsDepressed} = \text{True}|\text{hasGender} = \text{female}, \text{livesIn} = \text{US}, \text{searchedForSideEffectsOf} = \text{Xanax}) = 0.3 \]

\[ 0.3 - 0.01 > \delta \]
Quantifying privacy risks

$P(\text{IsDepressed} = \text{True}|\text{hasGender} = \text{female}, \text{livesIn} = \text{US}) = 0.01$

What are the side effects of Xanax?

$P(\text{IsDepressed} = \text{True}|\text{hasGender} = \text{female}, \text{livesIn} = \text{US}, \text{searchedForSideEffectsOf} = \text{Xanax}) = 0.3$

$0.3 - 0.01 > \delta$
Risk prediction in search histories
(proof-of-concept)
Risk prediction in search histories
(proof-of-concept)

Sensitive states $\leq$ Sensitive queries
Risk prediction in search histories (proof-of-concept)

Sensitive states <= Sensitive queries

Can we predict sensitive states even though the most obvious cues are masked out?
Alcoholism

Depression

Pregnancy

Sensitive states
Alcoholism:

Indicative (5)  Suggestive (5)  Ambiguous (10)

Depression:

Pregnancy:

Sensitive state vocabulary
Alcoholism: alcohol dependence

Depression: antidepressant

Pregnancy: pregnant

Sensitive state vocabulary
Sensitive state vocabulary

Alcoholism: indicative (5)
- alcohol dependence
- liver therapy

Depression: suggestive (5)
- antidepressant
- anxiety

Pregnancy: ambiguous (10)
- pregnant
- morning sickness
Alcoholism: 
- alcohol dependence
- liver therapy
- anonymous

Depression: 
- antidepressant
- anxiety
- stress

Pregnancy: 
- pregnant
- morning sickness
- labor

Sensitive state vocabulary
Framework

User Search Log

Background Knowledge

Inference model

\[ P(\text{IsDepressed}|\ldots) = 0.3 \]
Framework

User Search Log
- searchedForDepression(U)
- searchedForXanax(U)
- searchedForMedicalCourses(U)

Background Knowledge

Inference model

\[ P(\text{IsDepressed}|...) = 0.3 \]
Inference model

P(IsDepressed|...) = 0.3

User Search Log

searchedForDepression(U)
searchedForXanax(U)
searchedForMedicalCourses(U)

Background Knowledge

Co-occurrence counts:
- depression(317)
- side#effects(391)
- psychotherapy#depression(31)
We want to jointly model a set of variables:

\[ P(X, D, A, O, B) \]

Or specifically:

\[ P(D|A = True, P = psychiatrist) \]
Inference Model: Markov Random Field

- Xanax
- Depression
- Anxiety
- Bipolar disorder
- Occupation

Edges encode variable dependency

Markov property assumption:

$$P(O|X, D, A, B) = P(O|D)$$
Inference Model: Markov Random Field

Edges encode variable dependency

Markov property assumption:
\[ P(O|X, D, A, B) = P(O|D) \]

Clique potential functions
\[ \phi_i(X_1, \ldots, X_n) = w_i^\top \cdot f_i(X_1, \ldots, X_n) \]

Partition function
\[ P(X, D, A, O, B) = \frac{1}{Z} \exp(\phi_1(X, D, A) + \phi_2(D, O) + \phi_3(A, B)) \]

(normalizing factor)
MRFs as Markov Logic Networks

\[ \phi_i(X_1, ..., X_n) = w_i^T \cdot f_i(X_1, ..., X_n) \]

First-order logic abstraction layer

(0.17) \( \text{Anxiety} \land Xanax \Rightarrow \text{Depression} \)
(0.09) \( \text{Anxiety} \land \neg Xanax \Rightarrow \text{Depression} \)
(0.13) \( \neg \text{Anxiety} \land Xanax \Rightarrow \text{Depression} \)
MLN rules

\[ \text{IndicativeTerm}(U) \iff \text{SensitiveState}(U) \]

\[ \text{Term1}(U) \land \text{Term2}(U) \implies \text{IndicativeTerm}(U) \]
IndicativeTerm($U$) $\iff$ SensitiveState($U$)

$\text{Term1}(U) \land \text{Term2}(U) \implies \text{IndicativeTerm}(U)$
MLN rules

Those will be masked out

\[ \text{IndicativeTerm}(U) \iff \text{SensitiveState}(U) \]

\[ \text{Term}1(U) \land \text{Term}2(U) \implies \text{IndicativeTerm}(U) \]

All pairs of suggestive and ambiguous terms
MLN rules

(0.9) \[ \text{IndicativeTerm}(U) \iff \text{SensitiveState}(U) \]

(0.13) \[ \text{Term1}(U) \land \text{Term2}(U) \implies \text{IndicativeTerm}(U) \]

\[
\frac{\#\text{users}(\text{Term1}, \text{Term2}, \text{IndicativeTerm})}{\#\text{users}(\text{Term1}, \text{Term2})}
\]
Inference model

\[(0.13) \text{side\#effects}(U) \land \text{depression}(U) \Rightarrow \text{xanax}(U)\]

\[(0.07) \text{xanax}(U) \land \text{depressed}(U) \Rightarrow \text{IsDepressed}(U)\]

Framework

P(IsDepressed|\ldots) = 0.3
Proof-of-concept experiment

45 users from the AOL query log:

3x3x5
Proof-of-concept experiment

45 users from the AOL query log:

Sensitive state

3x3x5
Proof-of-concept experiment

45 users from the AOL query log:

Sensitive state

- highest overlap with indicative keywords
- highest overlap with ambiguous keywords
- highest overlap with both
Proof-of-concept experiment

45 users from the AOL query log:

Sensitive state

3x3x5

ground truth by two human assessors

indicative terms masked out for the model

Choice criteria:
- highest overlap with indicative keywords
- highest overlap with ambiguous keywords
- highest overlap with both
Proof-of-concept experiment

45 users from the AOL query log:

Sensitive state

3x3x5

Choice criteria:
- highest overlap with indicative keywords
- highest overlap with ambiguous keywords
- highest overlap with both

ground truth by two human assessors

indicative terms masked out for the model

<table>
<thead>
<tr>
<th></th>
<th>Precision</th>
<th>Recall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alcoholism</td>
<td>0.60</td>
<td>0.75</td>
</tr>
<tr>
<td>Depression</td>
<td>0.67</td>
<td>0.33</td>
</tr>
<tr>
<td>Pregnancy</td>
<td>0.50</td>
<td>0.85</td>
</tr>
</tbody>
</table>
Model limitations

Context

blackout (lyrics)

drinking too much (water)
Model limitations

Context
- blackout (lyrics)
- drinking too much (water)

User background
- ny uni medical courses
- depression symptoms
Model limitations

Context
- blackout (lyrics)
- drinking too much (water)

User background
- ny uni medical courses
- depression symptoms

Temporal dimension
- feeling lonely
- feeling anxious
- depression symptoms
- xanax prescription
- xanax side effects
To sum up

In the modern world of adversaries using Big Data and probabilistic tools, we need **user-centric privacy** to enable privacy control on the user side.
To sum up

In the modern world of adversaries using Big Data and probabilistic tools, we need user-centric privacy to enable privacy control on the user side

Joanna Biega, Ida Mele, Gerhard Weikum: Probabilistic Prediction of Privacy Risks in User Search Histories PSBD @ CIKM 2014

Thank you!