Privacy of profile-based ad targeting

Alexander Smal
and
Ilya Mironov

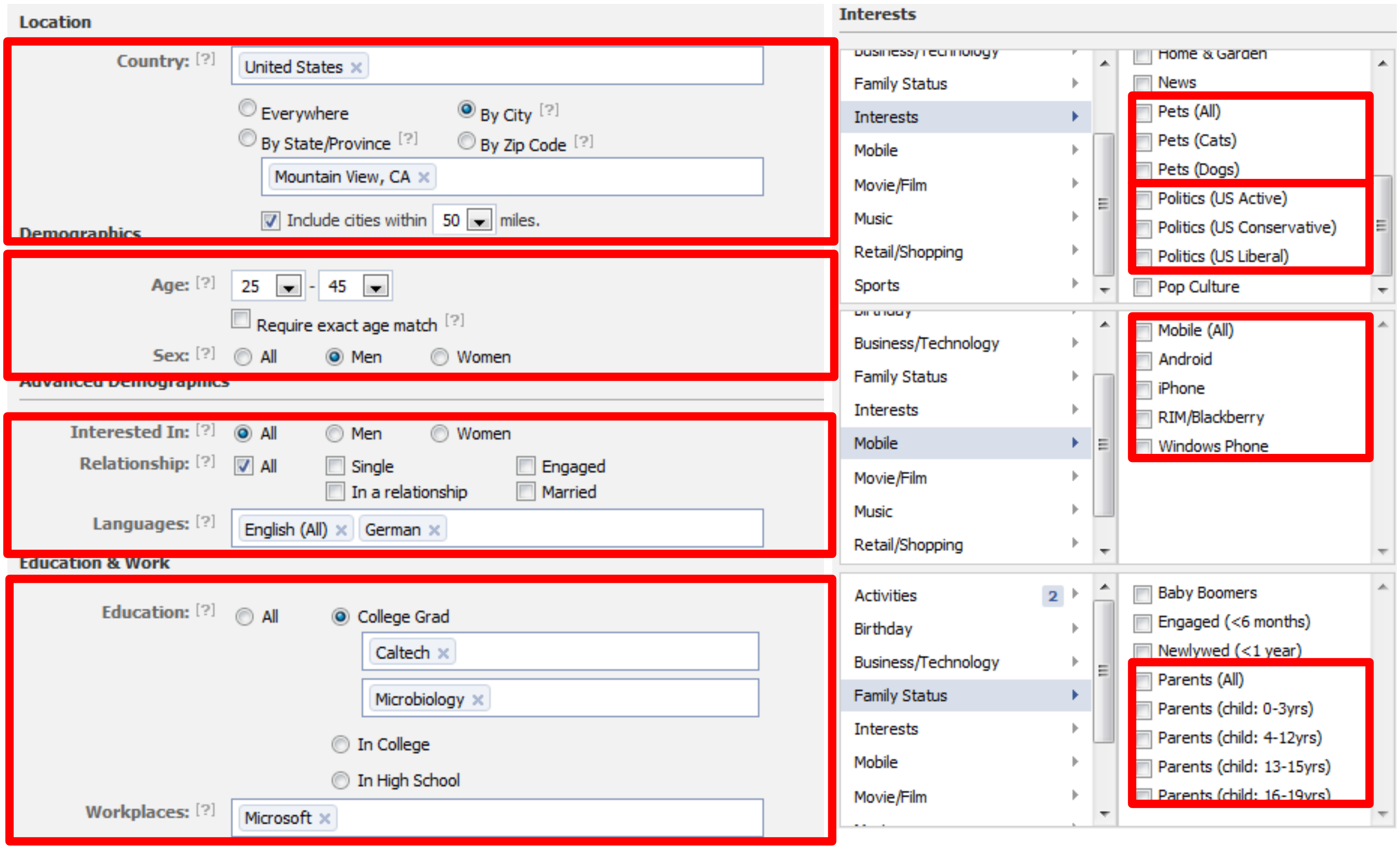
User-profile targeting

- Goal: increase impact of your ads by targeting a group potentially interested in your product.
- Examples:
  - Social Network

    Profile = user’s personal information + friends
  - Search Engine

    Profile = search queries + webpages visited by user

Facebook ad targeting



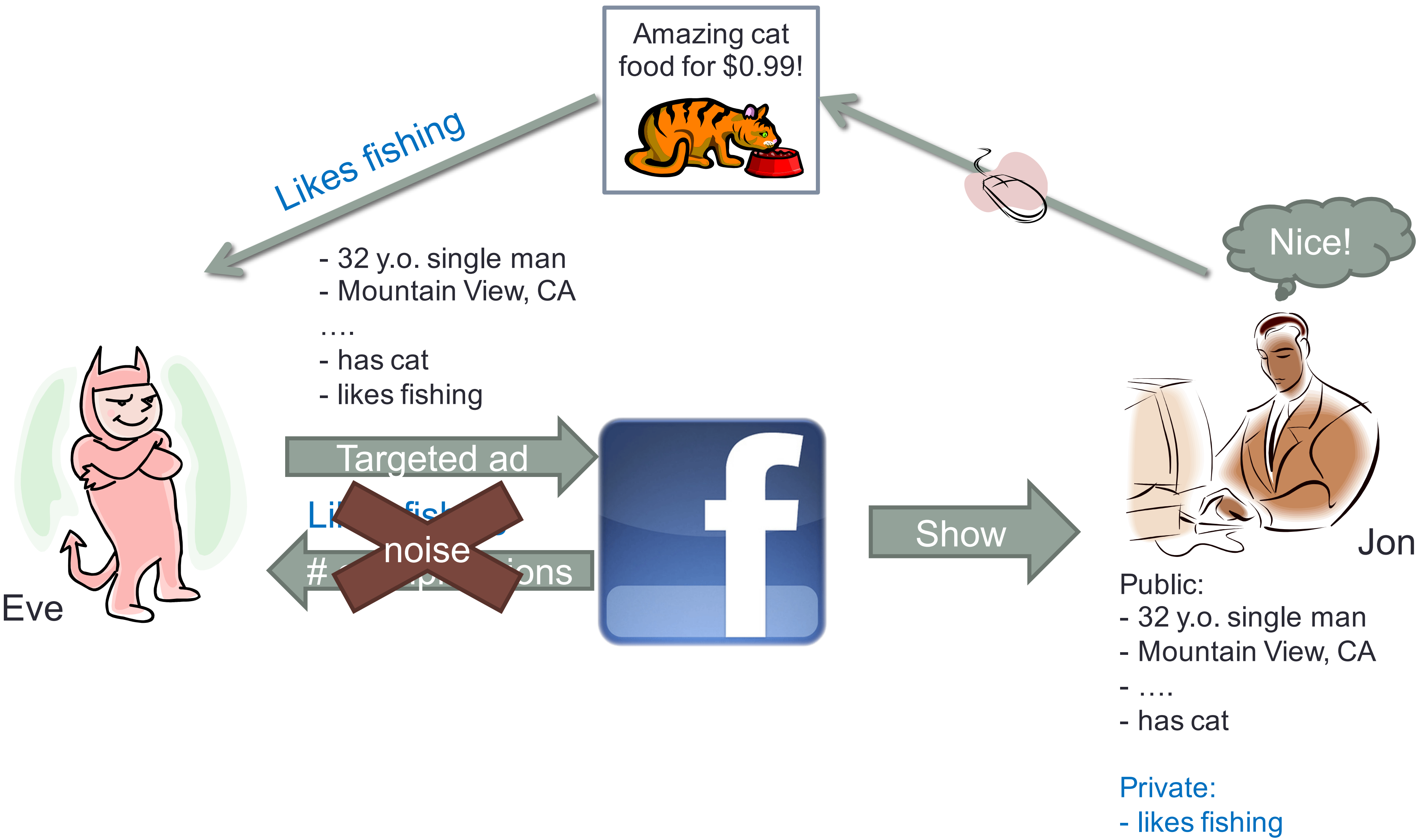
Characters

Advertising company

My system is private!

Privacy researcher

Simple attack [Korolova'10]



Advertising company

My system is private!

How can I target privately?

Privacy researcher

Unless your targeting is not private, it is not!

How to protect information?

- Basic idea: add some noise
  - Explicitly
  - Implicit in the data
    - noiseless privacy [BBGLT11]
    - natural privacy [BD11]
- Two types of explicit noise
  - Output perturbation
    - Dynamically add noise to answers
  - Input perturbation
    - Modify the database

Advertising company

Privacy researcher

I like input perturbation better…

Input perturbation

- Pro:
  - Pan-private (not storing initial data)
  - Do it once
  - Simpler architecture

Advertising company

Privacy researcher

I like input perturbation better…

Signal is sparse and non-random

Adding noise

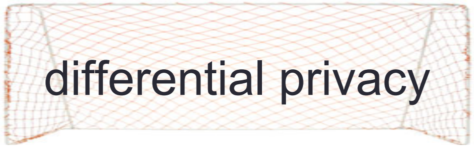
- Two main difficulties in adding noise:
  - Sparse profiles
  - Dependent bits

Sparse profiles

1	0	0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0	1	1
0	0	0	1	0	0	0	0	0	1
0	0	0	1	0	0	1	0	0	0
1	1	1	1	1	0	0	1	0	1
0	0	0	0	1	0	0	1	0	0
0	0	1	0	0	0	0	1	1	0
0	0	0	0	0	0	0	1	0	1
1	0	1	0	0	0	0	0	0	0
0	1	0	1	0	1	0	0	0	0

Dependent bits

1	0	0	1	1	1	0	1	0	0
0	1	0	0	0	0	0	0	1	1
1	0	0	0	0	0	0	0	1	0
1	0	0	1	1	1	1	0	0	0
0	1	1	0	0	0	0	0	1	1
1	0	0	0	1	0	0	1	0	0
0	1	1	1	1	1	0	1	1	1
0	1	0	0	0	0	0	1	0	0
1	0	1	1	1	1	0	0	0	0
0	1	0	0	0	0	0	1	0	1



“Smart noise”

Advertising company

Privacy researcher

I like input perturbation better…

Signal is sparse and non-random

Let’s shoot for deniability, and add “smart noise”!

"Smart noise"

- Consider two extreme cases
  - All bits are independent

    independent noise
  - All bits are correlated with correlation coefficient 1

    correlated noise

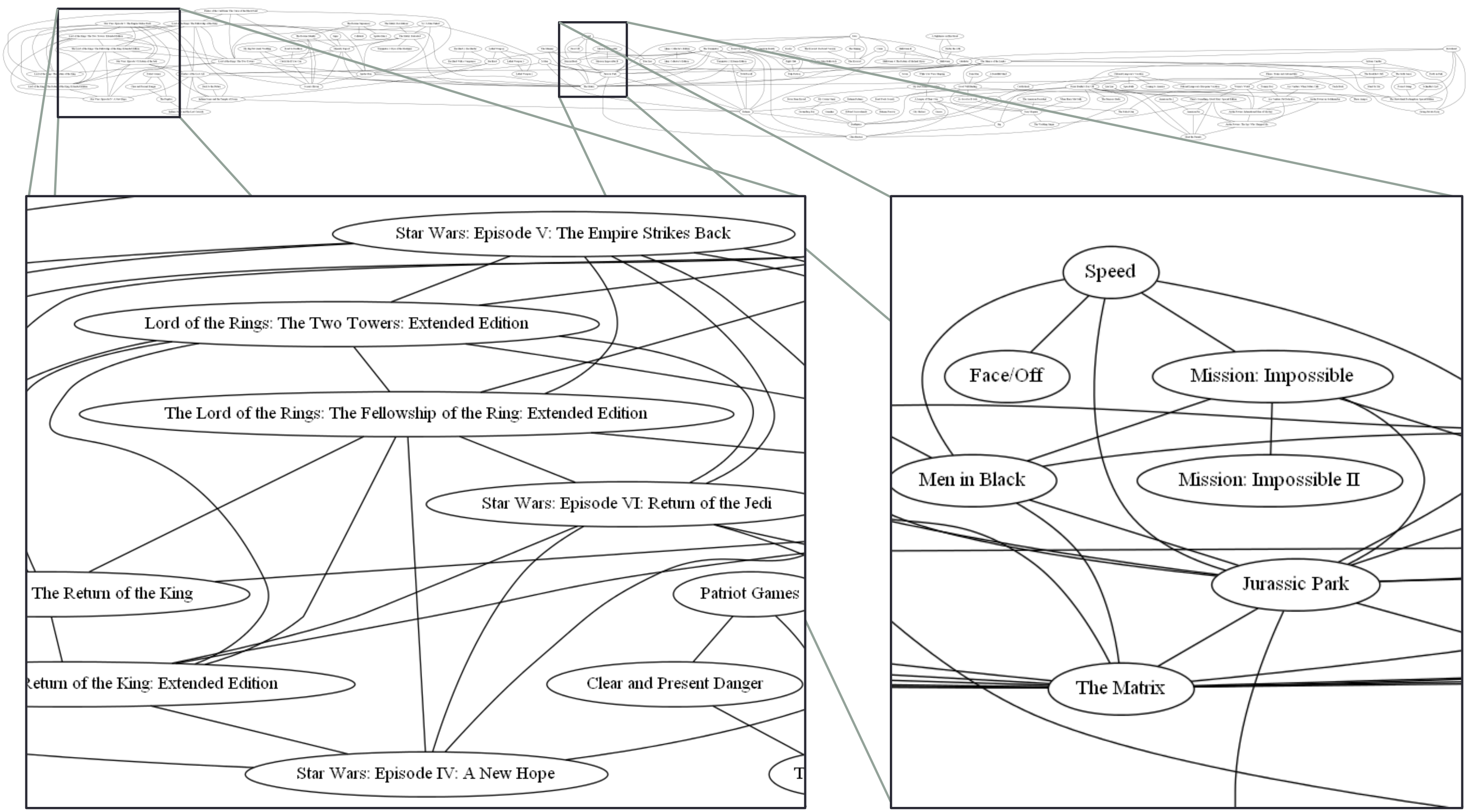
Aha!

- "Smart noise" hypothesis:
  "If we know the exact model we can add right noise"

Dependent bits in real data

- Netflix prize competition data
  - ~480k users, ~18k movies, ~100m ratings
- Estimate movie-to-movie correlation
  - Fact that a user rated a movie
- Visualize graph of correlations
  - Edge – correlation with correlation coefficient > 0.5

Netflix movie correlations



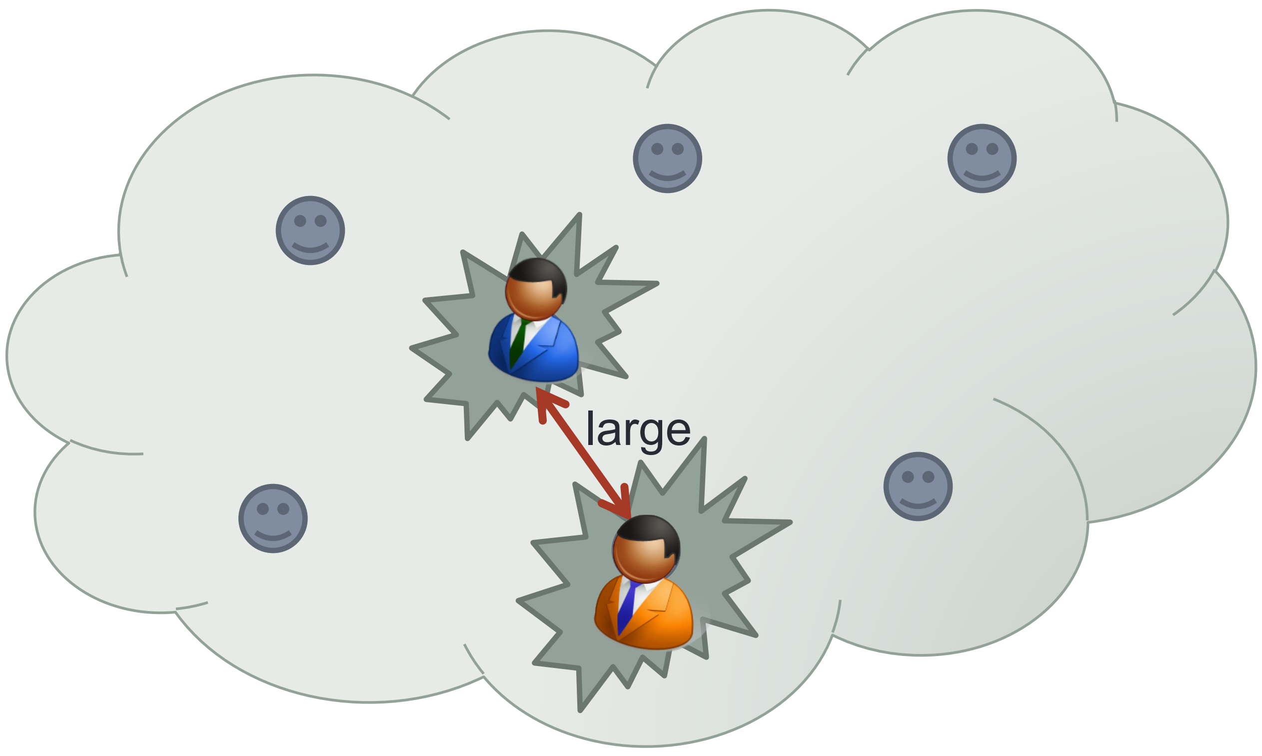
Advertising company

Privacy researcher

Let’s shoot for deniability, and add “smart noise”!

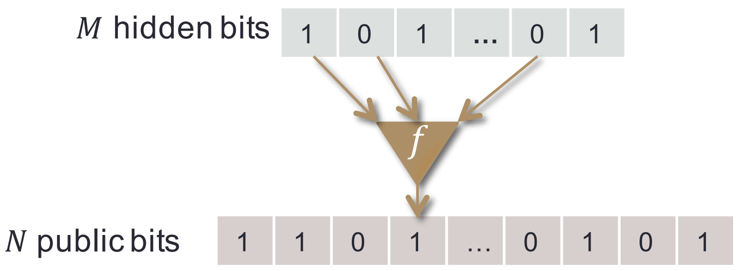
Let’s construct models where “smart noise” fails

How can “smart noise” fail?

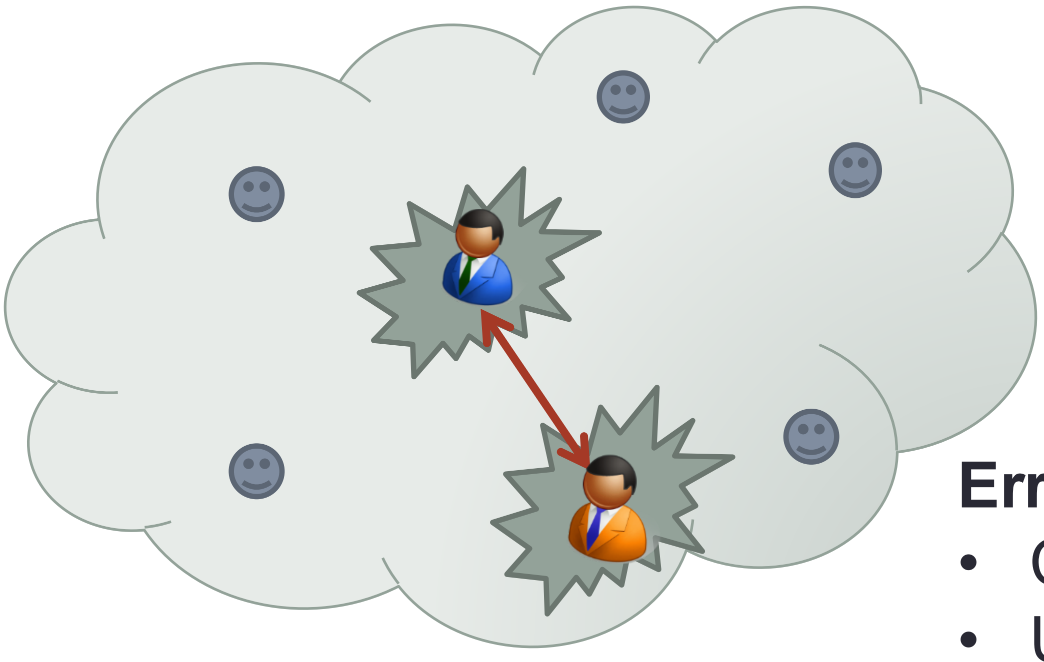


large = relative distance $\Omega(1)$

Models of user profiles



- M hidden independent bits
- N public bits
- Public bits are some functions of hidden bits
- Are users well separated?



Error-correcting codes

- Constant relative distance
- Unique decoding
- Explicit, efficient

Advertising company

Privacy researcher

See — unless the noise is >25%, no privacy

But this model is unrealistic!

Let me see what I can do with monotone functions…

Monotone functions

- Monotone function: for all i and for all values of x_j, $j \neq i$
  $$f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \geq f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$$
- Monotonicity is a natural property
  $$[wants\ Kindle] \leftrightarrow [likes\ reading] + [likes\ gadgets] \times [uses\ Amazon]$$
- Monotone functions are bad for constructing error-correcting codes

Approximate error-correcting codes

- *α-approximate error-correcting code with distance δ:*
  function $f: \{0,1\}^n \to \{0,1\}^m$
  $\forall x, x'$, such that $\|x - x'\|_1 \geq \alpha n$:
  $$\|f(x) - f(x')\|_1 \geq \delta m.$$

- If less than δ fraction of $f(x)$ is corrupted then we can reconstruct x within α fraction of bits.

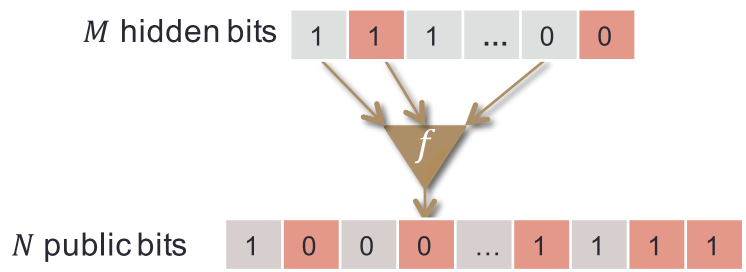
- We need $o(1)$-approximate error-correcting code with constant distance.

blatant non-privacy

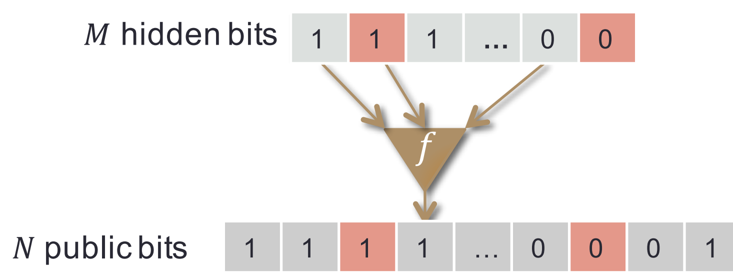
Noise sensitivity

- *Noise sensitivity* of function f:
$$\mathrm{NS}_\epsilon(f) = \mathbf{Pr}_x[f(x) \neq f(y)],$$
where x is chosen uniformly at random, y is formed by flipping each bit of x with probability ϵ.

- If $\mathrm{NS}_\epsilon(f)$ is big $\Rightarrow$



- If $\mathrm{NS}_\epsilon(f)$ is small $\Rightarrow$



Monotone functions

- There exist highly sensitive monotone functions [MO'03].
- **Theorem:** there exists monotone $o(1)$-approximate error-correcting code with constant distance on average.
- **Idea of proof:** Let $f_1, f_2, \ldots, f_m$ be random independent monotone boolean functions, such that $\mathrm{NS}_\epsilon(f_i) \geq c$ and f_i depends only on $o(n)$ bits of x.
- Let $F(x) = \langle f_1(x), \ldots, f_m(x)\rangle$.
- With high probability for random x there is no x' such that $\|x - x'\|_1 \geq \epsilon n$ and $\|F(x) - F(x')\|_1 \leq \frac{cn}{2}$.
- For Talagrand $o(1/\sqrt{n})$-approximate error-correcting code with constant distance on average.

Advertising company

Privacy researcher

If the model is monotone, blatant non-privacy is still possible

Hmmm. Does smart noise ever work?

Linear threshold model

- Function $f\colon\{-1,1\}^n \to \{0,1\}$ is a *linear threshold function*, if there exist real numbers α_i's such that
$$f(x) = \operatorname{sgn}(\alpha_0 + \alpha_1 x_1 + \cdots + \alpha_n x_n).$$

- **Theorem** [Peres'04]: Let f be a linear threshold function, then $\mathrm{NS}_\delta(f) \le 2\sqrt{\delta}$.

$$\Downarrow$$

No *o*(1)-approximate error-correcting code with *O*(1) distance

Conclusion

- Two separate issues with input perturbation:
  - Sparseness
  - Dependencies
- “Smart noise” fallacy:

  Arbitrary
  Monotone
  ~~Linear threshold~~

  Even for a publicly known, relatively simple model, constant corruption of profiles may lead to blatant non-privacy.
- Connection between noise sensitivity of boolean functions and privacy
- Open questions:
  - Linear threshold privacy-preserving mechanism?
  - Existence of interactive privacy-preserving solutions?

Thank for your attention!

Special thanks for Cynthia Dwork, Moises Goldszmidt, Parikshit Gopalan, Frank McSherry, Moni Naor, Kunal Talwar, and Sergey Yekhanin.

- Events $[f_i(x) \neq f_i(y)]$ and $[f_j(x) \neq f_j(y)]$ are independent for random x, $y = \mathrm{N}_\epsilon(x)$, i and j.
- Chernoff bounds: $\mathbf{Pr}_{x,y=\mathrm{N}_\epsilon(x)}\left[\sum_{i=1}^{m} |f_i(x) - f_i(y)| < \frac{mc}{2}\right] < e^{-\frac{mc}{8}}$.