Advertising systems in social media (2)

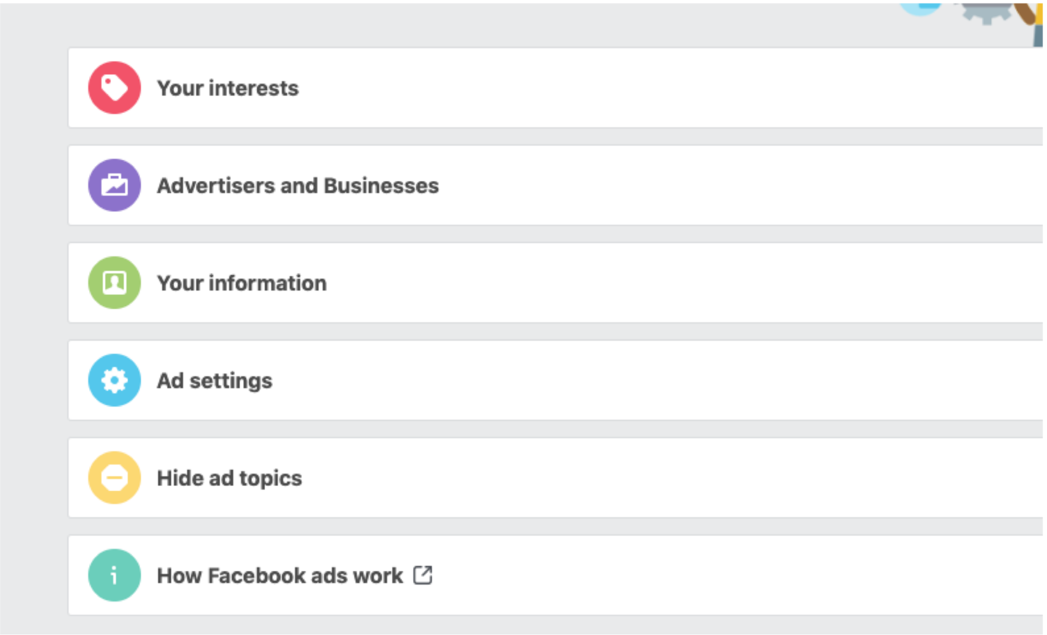
Saptarshi Ghosh
and Mainack Mondal

CS 60017
Autumn 2019

- Social advertising systems
  - Why bother about them?
  - The curious case of Facebook ads
  - How can we leverage these systems for doing good
- Abuse of the advertising systems
  - Why is targeted advertising bad?
  - Privacy risks with PII based targeting

First take a look at what Facebook thinks of you

- Go to: https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen



Your interests

Advertisers and Businesses

Your information

Ad settings

Hide ad topics

How Facebook ads work

Measuring this at scale: http://www.eurecom.fr/~andreou/papers/Facebook-NDSS2019.pdf

Abuse of social advertising systems

What kind of abuses are we going to talk about?

- Inferring private attributes of a user using Facebookl ads
  - https://theory.stanford.edu/~korolova/Privacy_violations_using_microtargeted_ads.pdf [A. Korolova 2011]
  - https://www.ftc.gov/system/files/documents/public_events/1223263/p155407privacyconmislove_1.pdf [Venkatadri et al 2018]

Attacker goals

- Infer private information about a user using Facebook ad interface
  - your age / sexual orientation/interests shared only with your friends
  - Knowing information like your phone number from your email id

- This attacks are mitigated (Somewhat)

Attack 1

- Privacy Violations Using Microtargeted Ads: A Case Study [2011]

- Recall that, Facebook's ad platform targeting is extremely detailed
  - Also Facebook knows everything your upload irrespective of your privacy setting

Inferencing attack on private attribute

- Assumption
  - Let’s say attacker can target “Alice” very very specifically
  - E.g., Alice is from city X working in Y, went to a college Z
- Goal
  - knowing Alice’s private attribute Attr (e.g., sexual orientation)
- The inferencing attack
  - Attacker created an ad microtargeted to Alice
  - Attacker created variants of this same ad but with an additional targeting parameter – different sexual orientations
  - Whichever of those variants register a ad viewing/ad clicking, Alice has corresponding sexual orientation

Two variants of Attack 1

- Inference from impressions
  - If there is one impression (somebody viewed the ad) in any one of the variants then attacker can infer correctly

- Inference from click
  - If there is a click then inference will work
  - However click == the victim is interested in the ad topic
  - Example: Interested in a marriage councilor or a divorce attorney

Results from the paper

- Inference from impressions
    - Author inferred friend’s age
    - Author inferred friend’s sexual orientation
    - Both were private attributes
- Inference from click
    - If a user is hiring for his team
    - Whether a person is interested in a thematic event

Facebook’s implemented solution

- Put a threshold on microtargeting
  - Don’t show ads if less than 20 users in that targeted category

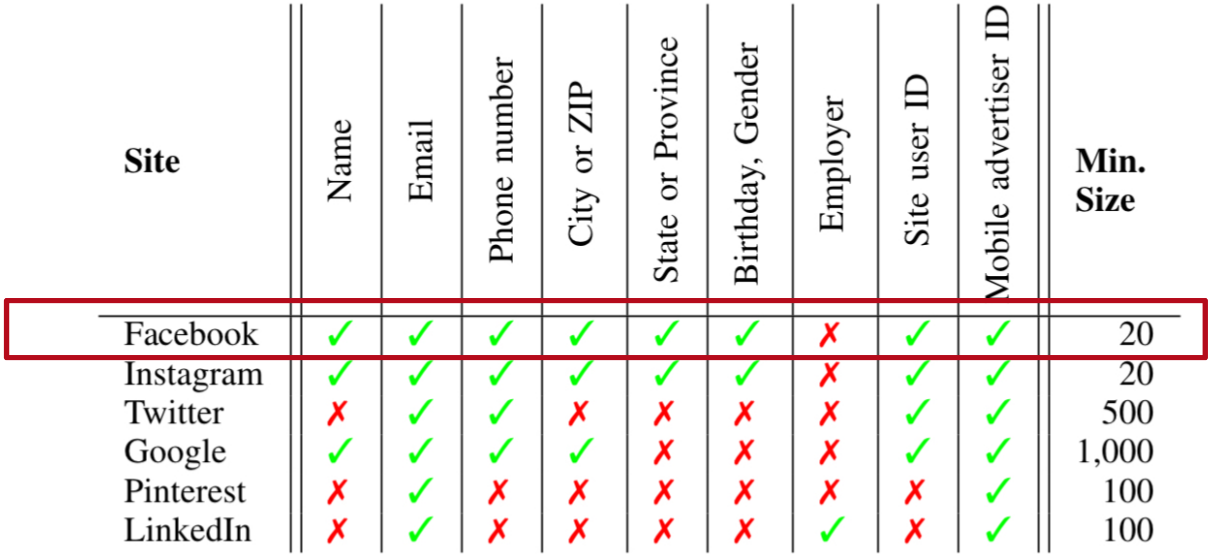
- How to defeat this improved policy?
  - Create 20 fake Facebook profiles
  - Give them attributes as your targeted victim
  - Repeat the old attack

Attack 2

- Privacy risks with Facebook’s PII-based targeting: auditing a data broker’s advertising interface [2018]

- Facebook’s ad platform had a brand new tool
    - Custom audience
    - A business can collect email ids/other PII (personally identifiable information) of its customers
    - Upload it on Facebook custom audience portal
    - Facebook searches Facebook-users for match and build an audience to show ads

Custom audiences exist not only for Facebook



Site	Name	Email	Phone number	City or ZIP	State or Province	Birthday, Gender	Employer	Site user ID	Mobile advertiser ID	Min. Size
Facebook	✓	✓	✓	✓	✓	✓	✗	✓	✓	20
Instagram	✓	✓	✓	✓	✓	✓	✗	✓	✓	20
Twitter	✗	✓	✓	✗	✗	✗	✗	✓	✓	500
Google	✓	✓	✓	✓	✗	✗	✗	✓	✓	1,000
Pinterest	✗	✓	✗	✗	✗	✗	✗	✗	✓	100
LinkedIn	✗	✓	✗	✗	✗	✗	✓	✗	✓	100

TABLE I: User attributes that advertisers can upload to create custom audiences in various advertising platforms. Also shown is the minimum custom audience size that the sites allow.

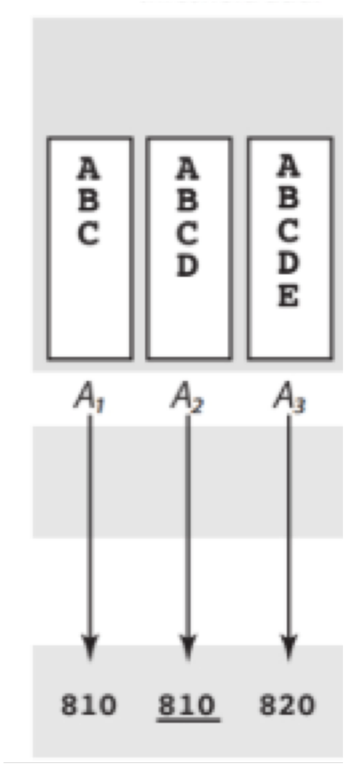
- But Facebook gives result starting from only 20 users

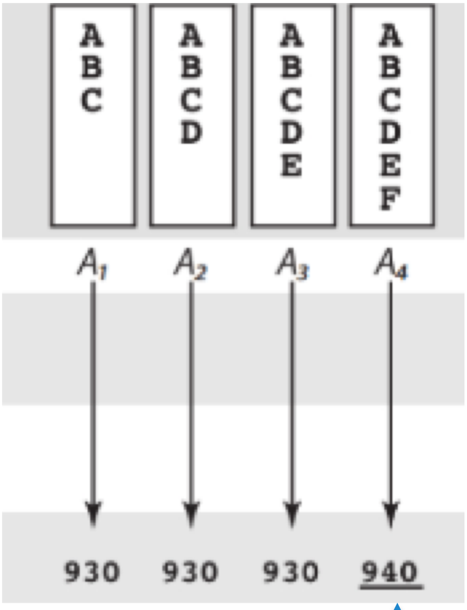
Information available for custom audiences at Facebook

- After the audience has been created, Facebook gives an approximate audience size (#matched records)
- You can create different custom lists
  - Then you can do union and intersection of those audiences
  - Facebook will give you audience size
  - If a user is in two audiences Facebook count them only once
- How do Facebook approximate audience?
  - The found it is by simple rounding
  - Round to closest 10s (upto size 1000) or closest 100s (>1000)

Key ideas

- They introduced the idea of **threshold audience**





Audience size increased with one addition
Lower threshold audience

Audience size increased with one addition
Upper threshold audience

Putting it altogether: know if a celebrity V visited your website

- You have a set of pixel audiences P
    - The set of users who visited your website and have an unique pixel
    - Goal: Is V in P?
- First create a lower threshold audience with a set of random emails
    - Adding just one user might increase the estimate
    - Add V, if the size increases then V is targetable with this lower threshold
- Now create an upper threshold with P and the random emails
    - Check if doing a set removal of a custom list containing only V from this upper threshold decrease the size
    - If it does then V is in P

Even worse attack

- You have a set of email ids
  - You want to have their phone numbers
  - Using this lower threshold and upper threshold approach you can match each phone number to an email id
- Surprisingly fast
  - 140 lists to cover all of Boston
  - 82 lists for France
- They recovered the phone numbers of every visitor to a website

Why does this attack work?

- Because Facebook used a weak algorithm to approximate
    - Facebook solved it by removing the audience estimate for set operations
    - What if you add noise to the audience size instead of round up?
    - Differential privacy!

Differential privacy

- It should not harm you or help you as an individual to enter or to leave a dataset.
- To ensure this property, we need a mechanism whose output is nearly unchanged by the presence or absence of a single respondent in the database.
- In constructing a formal approach, we concentrate on pairs of databases (*D*, *D'*) differing on only one row, with one a subset of the other and the larger database containing a single additional row.
- Next day …