User privacy in social media

Saptarshi Ghosh
and Mainack Mondal

CS 60017
Autumn 2019

Now we will talk about privacy

- Two broad dimensions
  - Preserving privacy from the background actors, e.g., advertisers or even the social media platform
  - Preserving privacy of data from other users, e.g., your ex

“What” of privacy?

Some **s**lides borrowed from Blase Ur, UChicago

Warren and Brandeis (1890)

HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar *v.* Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only

Warren and Brandeis's Argument

- Libel and slander are insufficient in considering only damage to reputation
- Considers property rights
- The right to prevent, rather than profit from, publication
- **"The right to be let alone"**
- Excludes topics of general interest

Privacy as Control / Secrecy (1967)

"Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

"…each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication…."

Alan Westin, Privacy and Freedom, 1967

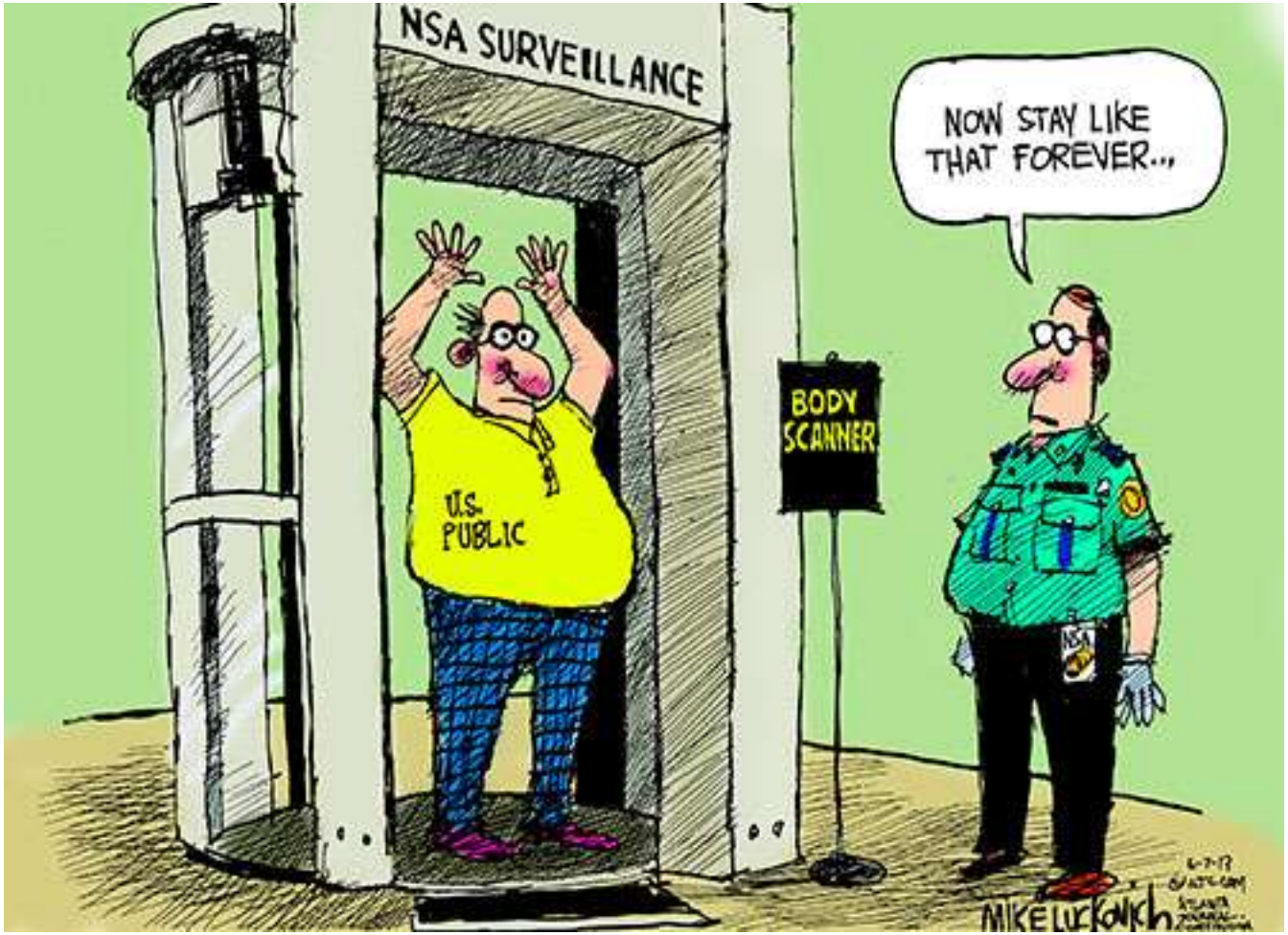
Privacy Regulation Theory (1975)

- Irwin Altman (social psychology)
  - Preceded by Altman and Taylor's Social Penetration Theory (1973) about intimacy in relationships
- Dialectic and dynamic process of boundary regulation
  - Continuous movement on a continuum
- Goal: optimum balance of privacy and social interaction

CPM Theory (1991)

- Sandra Petronio (communications)
  - Communication Privacy Management Theory
- Regulate boundaries based on perceived costs and benefits
  - Movement on a continuum
- Expect rule-based management
- Boundary turbulence related to clashing expectations

Purpose Matters (?)



Privacy as Contextual Integrity (2004)

- Helen Nissenbaum (philosophy)
- “Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context.”

Privacy as Contextual Integrity

- Appropriate flows of information
- Appropriate flows conform to contextual information norms
- Norms refer to the data subject, sender, recipient, information type, and transmission principle
- Conceptions of privacy evolve over time and are grounded in ethics

Dan Solove's Pluralistic Conceptions

- Some data isn't "sensitive," but its collection and use impact privacy
  - Impact power relationships
  - Kafka-esque
- Solove's privacy taxonomy
  - Information collection
  - Information processing
  - Information dissemination
  - Invasion

Privacy laws around the world

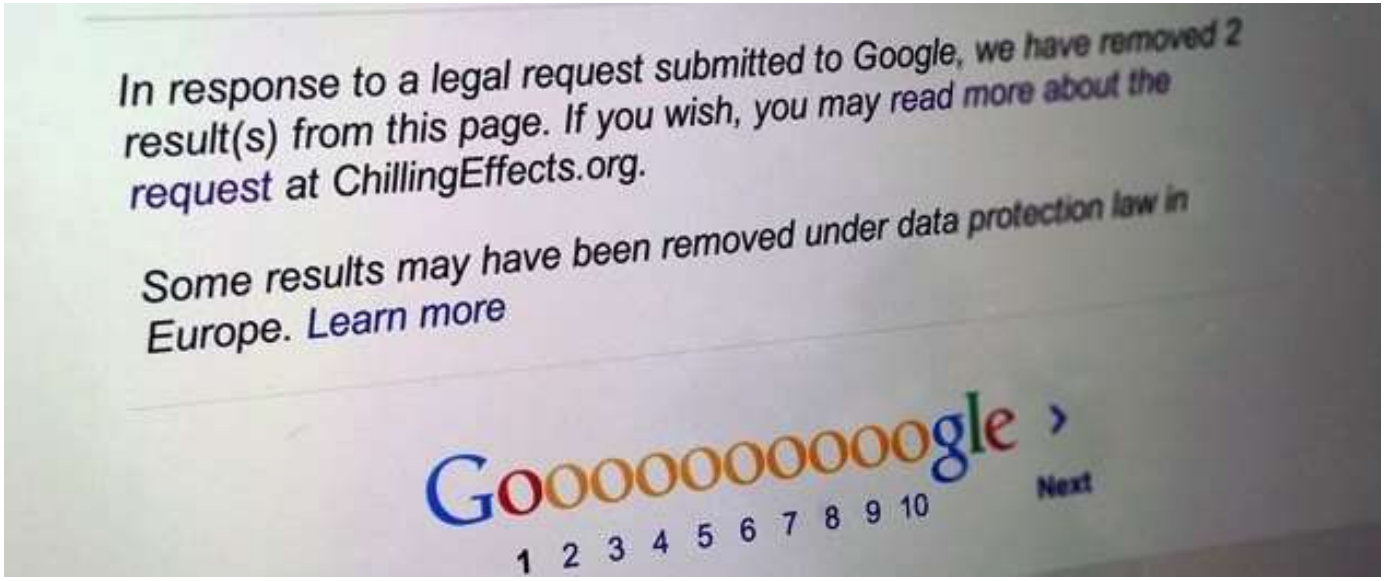
- US has sector-specific laws, minimal protections
  - No explicit constitutional right to privacy or general privacy law
  - Some privacy rights inferred from constitution
  - Narrow regulations for health, credit, education, videos, children, financial information
  - FTC investigates fraud & deceptive practices
  - FCC regulates telecommunications
  - Some state and local laws (California)

EU GDPR (2016/679)

- General Data Protection Regulation
- Disclose collection, automated decisions
- Data protection by design and default
- Right of access
- Right of erasure (right to be forgotten)
- Data breach notification within 72 hours
- Penalty: Up to 2%/4% of worldwide turnover

Right to be forgotten

- Should a person have the agency to cause items from the past to be removed?
- Who owns information?
- EU



Fair Information practice principles (FIPP)

- Notice/Awareness: Consumers should be given notice of an entity's information practices before any personal information is collected from them

Fair Information practice principles (FIPP)

- Notice/Awareness: Consumers should be given notice of an entity's information practices before any personal information is collected from them
- Choice/Consent: Choice and consent in an on-line information-gathering sense means giving consumers options to control how their data is used

Fair Information practice principles (FIPP)

- Notice/Awareness: Consumers should be given notice of an entity's information practices before any personal information is collected from them
- Choice/Consent: Choice and consent in an on-line information-gathering sense means giving consumers options to control how their data is used
- Access/Participation: Not only a consumer's ability to view the data collected, but also to verify and contest its accuracy in inexpensive and timely manner

Fair Information practice principles (FIPP)

- Notice/Awareness: Consumers should be given notice of an entity's information practices before any personal information is collected from them
- Choice/Consent: Choice and consent in an on-line information-gathering sense means giving consumers options to control how their data is used
- Access/Participation: Not only a consumer's ability to view the data collected, but also to verify and contest its accuracy in inexpensive and timely manner
- Integrity/Security: Information collectors should ensure that the data they collect is accurate and secure

Fair Information practice principles (FIPP)

- Notice/Awareness: Consumers should be given notice of an entity's information practices before any personal information is collected from them
- Choice/Consent: Choice and consent in an on-line information-gathering sense means giving consumers options to control how their data is used
- Access/Participation: Not only a consumer's ability to view the data collected, but also to verify and contest its accuracy in inexpensive and timely manner
- Integrity/Security: Information collectors should ensure that the data they collect is accurate and secure
- Enforcement/Redress: In order to ensure that companies follow the Fair Information Practice Principles, there must be enforcement measures (self-regulation, sue by users, Government regulation)

Understanding privacy

We reviewed a number of definitions

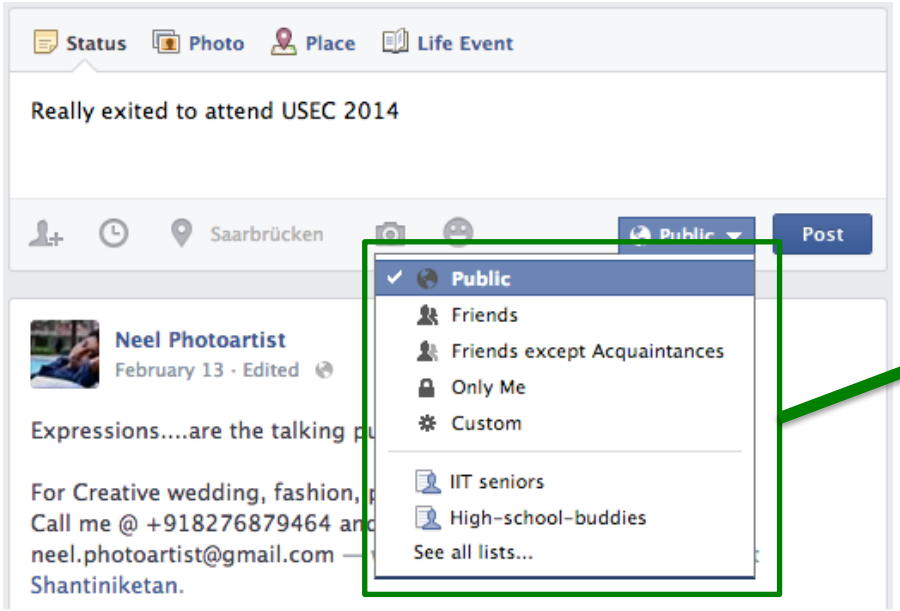
- Warren and Brandeis (1890)
- Westin's definition (1967)
- •
- •
- •
- Solove's taxonomy of privacy (2008)
- Nissenbaum's privacy as contextual integrity (2010)

Identified different **aspects of privacy** from these definitions

A **subsequent** step is to **build mechanisms** to cover these aspects

“How” of privacy?

State of the art: Access control model

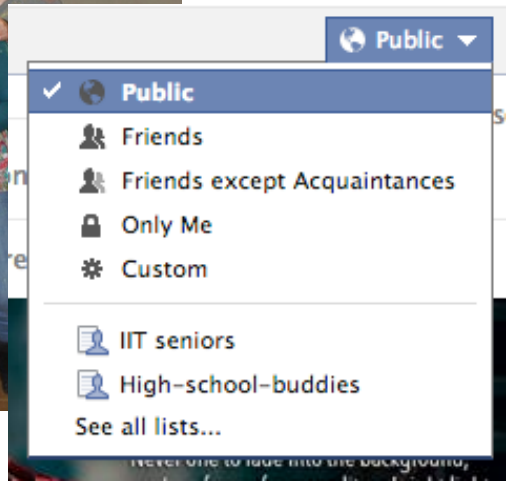


Allow others access to content

Privacy violation from Access Control point of view:

If someone accesses content who the user did not allow

Privacy violations in the real world



reddit

Privacy violation in real world from user's point of view:

If someone accesses content who the user did not intend

ACLs are inadequate to capture many such privacy

Scenario 1: Facebook newsfeed

Facebook pushes your content as updates

Others automatically get your content
when they login to their Facebook page

After Newsfeed: More people actually saw the content

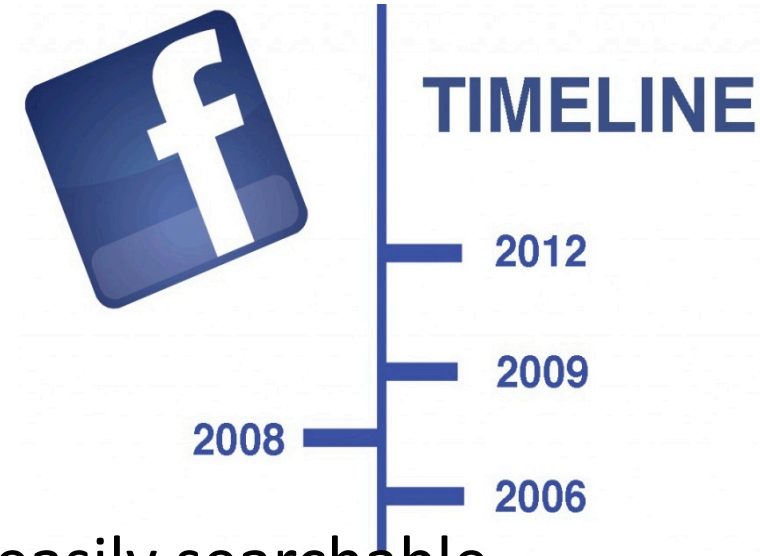
Users complained of privacy violation [Boyd et al. ’08]

Before and after Newsfeed: **access control did not change**!

Scenario 2: Facebook timeline

Sort your content by upload time

Others can search by time



After timeline: Old content became easily searchable

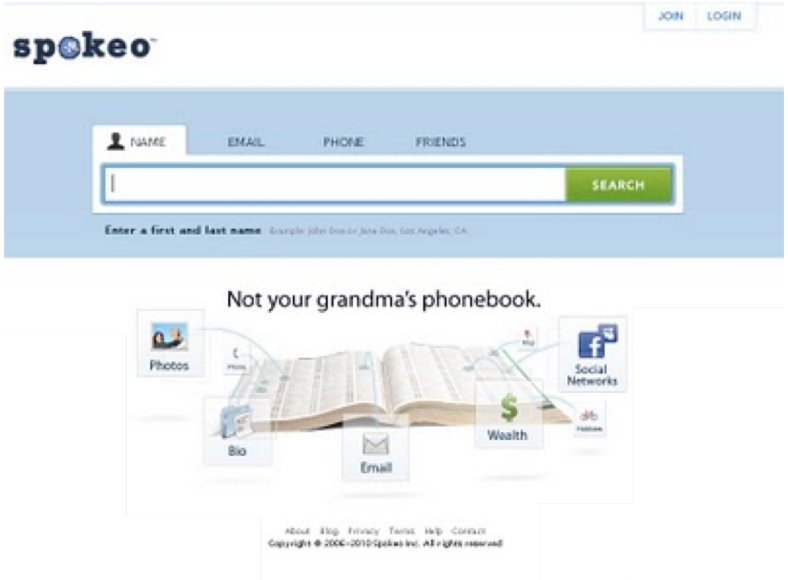
Users felt privacy was violated

Before and after Timeline: **access control did not change**!

Scenario 3: Spokeo

Service aggregating public data from web

Others get all of this data by searching Spokeo



After aggregation: Inferring non public data become easier

Users complained of privacy violation

Before and after aggregation: **access control did not change!**

User reaction suggests each of the cases violated privacy

However access control was not violated in any of the cases

Take away 1: Access control is inadequate to capture user intention

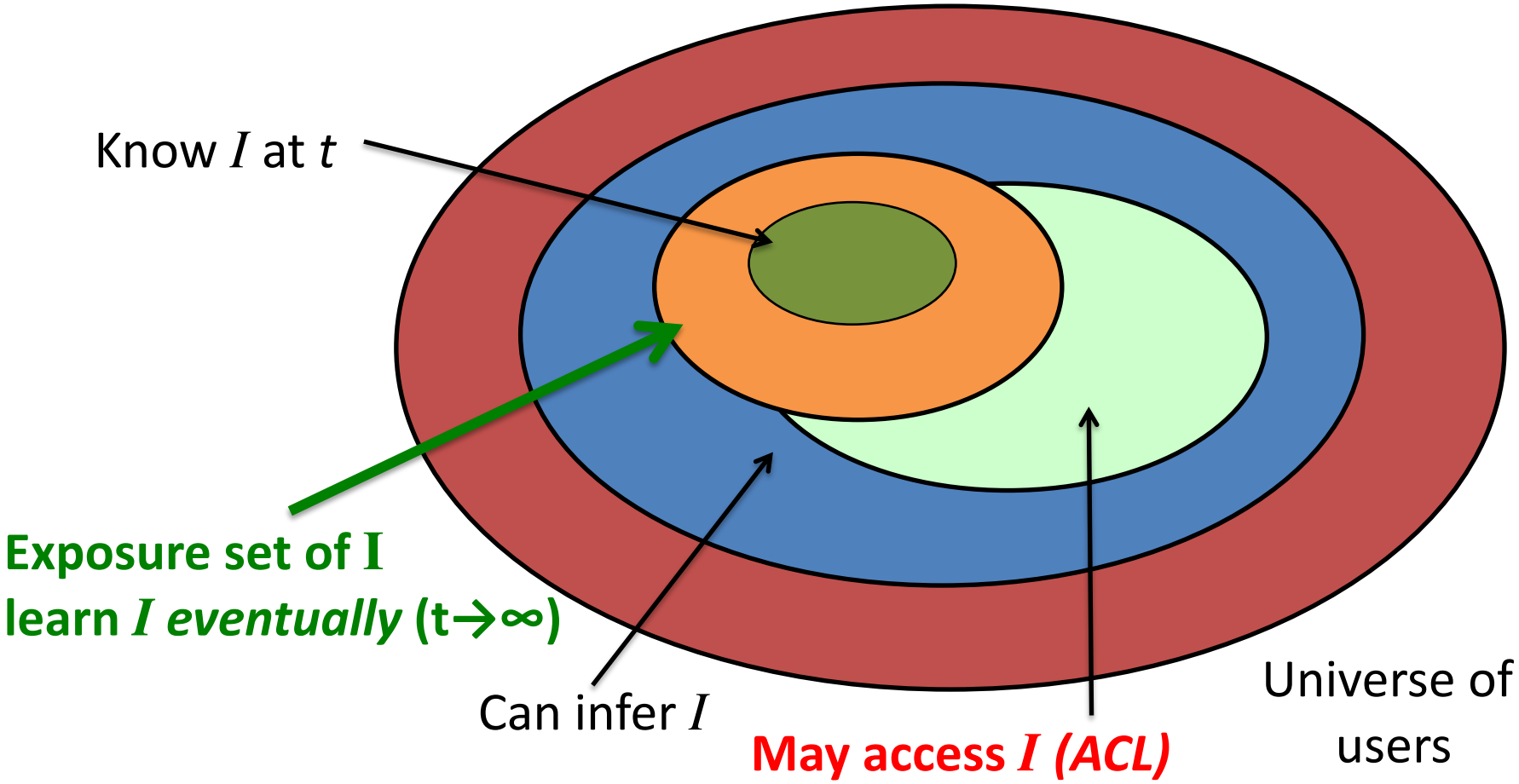
Recap

Access control is inadequate to capture privacy

Exposure: A different concept to capture information privacy

Discussion: How to manage privacy via exposure

Exposure : Definition



Exposure for content I

The set of people who will learn I eventually

How accurately do users estimate exposure?

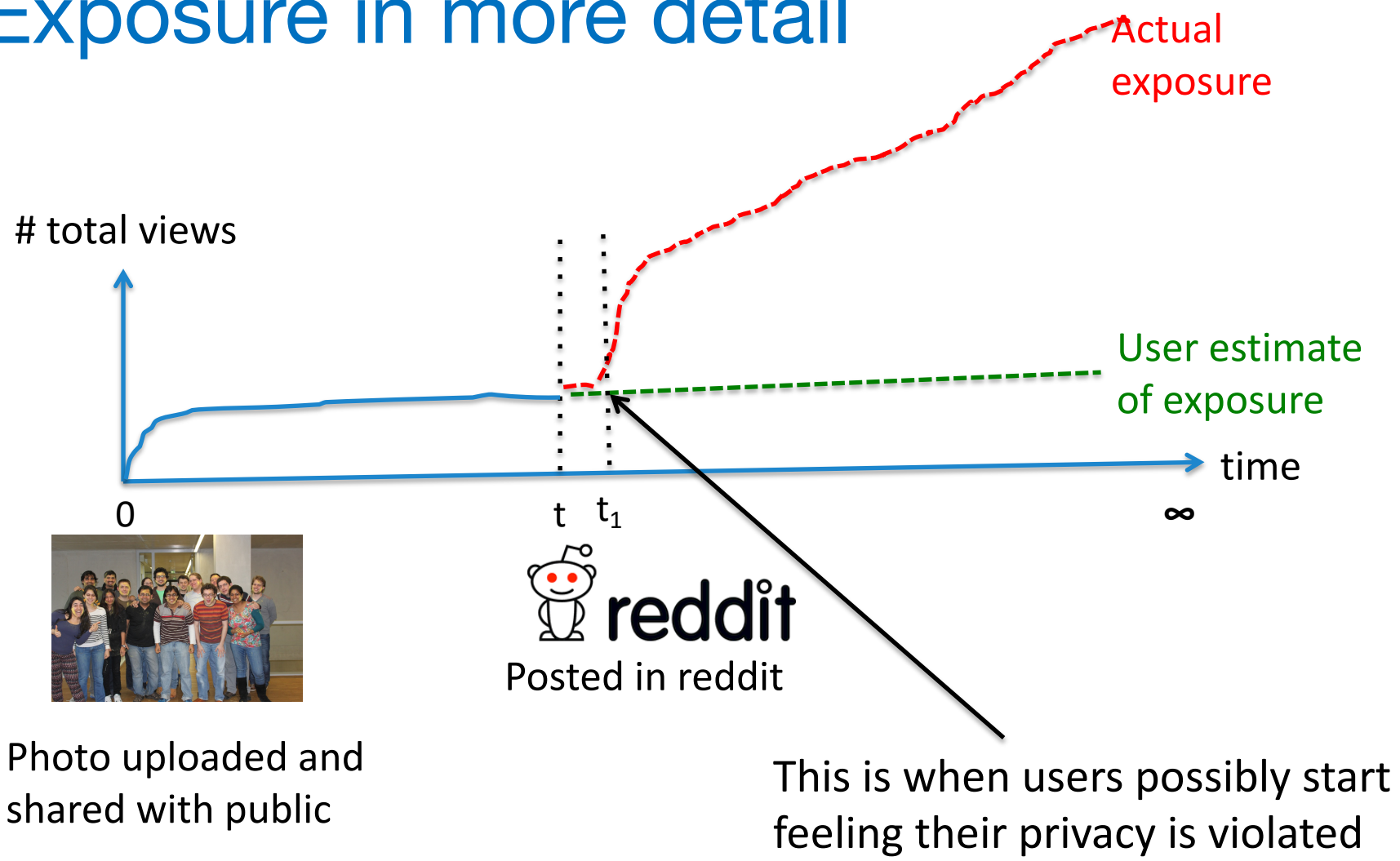
Facebook researchers did a study with 589 us

[Bernstein et al. 2013]

Perceived exposure grossly underestimates actual exposure

There may be a feeling of privacy violation when actual exposure is different from perceived exposure

Exposure in more detail



Revisiting scenario 1: Facebook newsfeed

Exposure before newsfeed

Friends who visit profile

Exposure after newsfeed

All the friends who are logged into Facebook

Exposure of uploaded information **after newsfeed** > **Exposure** of uploaded information **before newsfeed**

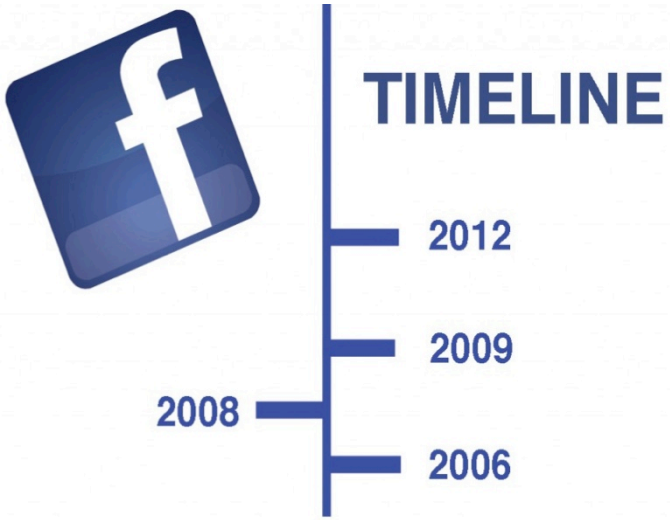
Revisiting scenario 2: Facebook timeline

Exposure of old content before timeline

Users who will scroll down thousands of content

Exposure of old content after timelin

All users who search by time



Exposure of old information **after timeline** > **Exposure** of old information **before timeline**

Revisiting scenario 3: Spokeo

Exposure before aggregation

Users who collect content themselves from multiple source

Exposure after aggregation

Any user who searches in Spokeo

Exposure of inferred information **after aggregation** > **Exposure** of inferred information **before aggregation**

Take away 2: Exposure based privacy model can capture violations which are not captured by access control

Recap

Access control is inadequate to capture privacy

Exposure: A different concept to capture information privacy

Discussion: How to manage privacy via exposure

Discussion: Managing privacy via exposure

Challenge 1:
How to estimate exposure for a content?

Challenge 2:
How to make users aware of the estimated exposure?

Challenge 3:
How to allow users more control over exposure?

Challenge 1: Estimating exposure

Situations where predicting exposure is very hard

Cross site prediction, exposure of inferred information

Situations where predicting exposure is possible

Predicting exposure of content in a site

Lots of research in content popularity growth

[Borghol et al] [Figueiredo et al.]
[Hong et al.] [Zaman et al]
[Bernstein et al.]

Challenge 1: Who can best estimate exposure

OSN operators are in the **best position to predict** exposure accurately with the data they collect

- They log who is accessing what content
- They collect historical data for content access

OSN operators can also **control** exposu

- They decide which content to show other users

Challenge 2: How to make users aware of the exposure?

Prediction can be shown to users at different granularity

- List of predicted people for a content
- Number of predicted people for a content
- Showing the prediction for a certain time period
- Showing the prediction with error bounds
- Showing how a specific dissemination mechanism changes the prediction
  - e.g., 200 more people are likely to see your content due to newsfeed

Challenge 3: How to allow users more control over exposure?

Different “knobs” can be provided to the user

- Change access control to a more restrictive setting
- Disabling particular dissemination mechanisms, e.g. search
- Enabling tripwires
  - Take content offline if more than 50 people view
  - Take content offline after two months

Take away 3: There are lots of open challenges and substantial research opportunities in how to design and deploy exposure based systems