DSC 291 Privacy-sensitive Data Systems (week 7a)

Haojian Jin

Logistics

1. Final project
    1. Abstract due Feb. 15.
    2. Final report due Mar. 19
2. Grades
    1. Would be more strict.

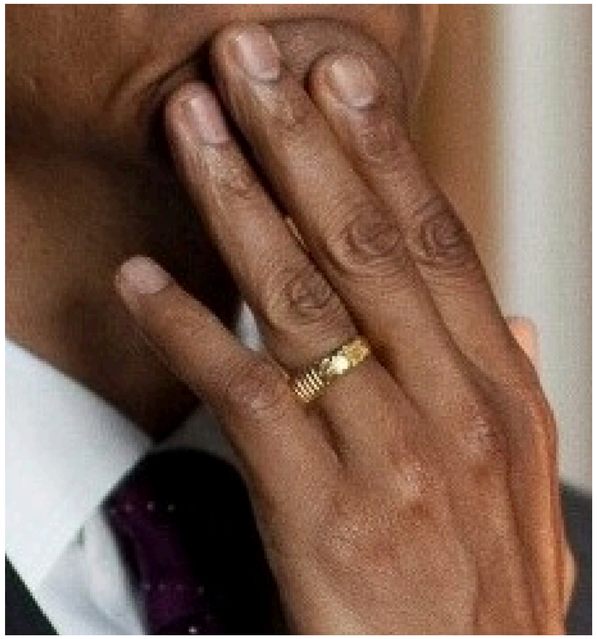
Recap

1. K-anonymity
2. Differential privacy
3. Implementation
4. No free lunch in data privacy

Today's class: Social network privacy & inclusive privacy

1. Social network
2. IPV, Election, Inclusive privacy

Inference example



1. Fact: the guy wears a ring on his ring finger.
2. Rule: People who wear a ring on their ring finger are married.
3. Output: The guy in the picture is married.

You are who you know

You Are Who You Know: Inferring User Profiles in Online Social Networks

Alan Mislove[†‡§], Bimal Viswanath[†], Krishna P. Gummadi[†], Peter Druschel[†]
[†]MPI-SWS, Saarbrücken, Germany
[‡]Rice University, Houston, TX, USA
[§]Northeastern University, Boston, MA, USA
amislove@ccs.neu.edu, {bviswana, gummadi, druschel}@mpi-sws.org

ABSTRACT

Online social networks are now a popular way for users to connect, express themselves, and share content. Users in today's online social networks often post a profile, consisting of attributes like geographic location, interests, and schools attended. Such profile information is used on the sites as a basis for grouping users, for sharing content, and for suggesting users who may benefit from interaction. However, in practice, not all users provide these attributes.

In this paper, we ask the question: given attributes for some fraction of the users in an online social network, can we *infer* the attributes of the remaining users? In other words, can the attributes of users, in combination with the social network graph, be used to predict the attributes of another user in the network? To answer this question, we gather fine-grained data from two social networks and try to infer user profile attributes. We find that users with common attributes are more likely to be friends and often form dense communities, and we propose a method of inferring

ple, MySpace (over 275 million users)[1], Facebook (over 300 million users), Orkut (over 67 million users), and LinkedIn (over 50 million "professionals") are examples of wildly popular networks used to find and organize contacts. Some networks such as Flickr, YouTube, and Picasa are used to share multimedia content, and others like LiveJournal and BlogSpot are popular networks for sharing blogs.

Users often post profiles to today's online social networks, consisting of *attributes* like geographic location, interests, and schools attended. Such profile information is used as a basis for grouping users, for sharing content, and for recommending or introducing people who would likely benefit from direct interaction. Today's online social networks rely on users to manually input profile attributes, representing a significant burden on users, especially when users are members of multiple online social networks. Thus, in practice, not all users provide these attributes, thereby reducing the usefulness of the social network applications.

In this paper, we ask the question: is it possible to *infer* the missing attributes of a user in an online social network

Mislove et al. You Are Who You Know: Inferring User Profiles in Online Social Networks. Conference on Web Search and Data Mining, pages 251–260, 2010

Research questions

1. Is it possible to infer missing attributes of a user in an online social network from other users' attributes and their relations with the user in subject?

2. What user attributes and social links are necessary to infer another user's attributes?

Intuition

1. Physical channel
    1. Geographic location
    2. Schools attended

2. Virtual channel
    1. Support same sports clubs
    2. Date similar people
    3. Interests

Social network implications

- A user’s privacy no longer depends on what they reveal.
  - Your friends also reveals information about you.

Datasets

- Dataset 1: Rice university
  - 4000 students and alumni of Rice University collected from Facebook
  - Attributes collected:
    - Major of study, Year of matriculation, Dormitory
- Data set 2: New Orleans
  - 63,000 users in the New Orleans Facebook Regional network
  - Attributes collected from Facebook profile page.
    - Some attributes are private

Revealed attributes in New Orleans Network

Attribute	Fraction revealed
high school	68.9%
university	58.3%
employer	42.3%
interests	35.5%
location	19.3%

Method: Social Network as a Graph

- G = (V, E)
- Users are nodes (V)
- Friend links are edges (E)

Method: Affinity Values

- Fraction of links for which users share the same value of attribute a
- $S_a = \frac{|(i,j) \in E : a_i = a_j|}{|E|}$
- Divide that by E_a, expected if attributes are placed randomly.
- Affinity = S_a / E_a
- Values > 1 indicate that links are positively correlated with attributes.

Exercise: Affinity Values

Users	Attribute	Affinity
Rice undergrads	college major year	
Rice grads	department school year	
New Orleans	high school hometown political views	

Exercise: Affinity Values

Users	Attribute	Affinity
Rice undergrads	college	4.49
	major	2.33
	year	1.97
Rice grads	department	9.71
	school	4.02
	year	1.79
New Orleans	high school	53.2
	hometown	2.87
	political views	1.86

Self-disclosure

Self-disclosure refers to a social process of sharing private information with another.

Social network implications

- A user’s privacy no longer depends on what they reveal.
- Temporal changes in preferences

Silent Listeners: The Evolution of Privacy and Disclosure on Facebook

Silent Listeners: The Evolution of Privacy and Disclosure on Facebook

Fred Stutzman*, Ralph Gross†, Alessandro Acquisti‡

Abstract. Over the past decade, social network sites have experienced dramatic growth in popularity, reaching most demographics and providing new opportunities for interaction and socialization. Through this growth, users have been challenged to manage novel privacy concerns and balance nuanced trade-offs between disclosing and withholding personal information. To date, however, no study has documented how privacy and disclosure evolved on social network sites over an extended period of time. In this manuscript we use profile data from a longitudinal panel of 5,076 Facebook users to understand how their privacy and disclosure behavior changed between 2005—the early days of the network—and 2011. Our analysis highlights three contrasting trends. First, over time Facebook users in our dataset exhibited increasingly privacy-seeking behavior, progressively decreasing the amount of personal data shared publicly with unconnected profiles in the same network. However, and second, changes implemented by Facebook near the end of the period of time under our observation arrested or in some cases inverted that trend. Third, the amount and scope of personal information that Facebook users revealed privately to other connected profiles actually increased over time—and because of that, so did disclosures to "silent listeners" on the network: Facebook itself, third-party apps, and (indirectly) advertisers. These findings highlight the tension between privacy choices as expressions of individual subjective preferences, and the role of the environment in shaping those choices.

Research questions

- How do sharing behaviors of users change over time?
- How do disclosures to “silent listeners” evolve?

Method

- 6-year longitudinal study of privacy and sharing behaviors on Facebook at CMU (2005-2011)
- Dataset: 5076 members of CMU Facebook network
- Early joiners of Facebook

Common findings

- Progressively limit content to strangers
- Consistent among all profile elements
- Intended audiences not necessarily map to actual audiences
- Mitigation strategies:
  - Self-censorship, withdrawal of content

CMU Yearly Snapshot Dataset

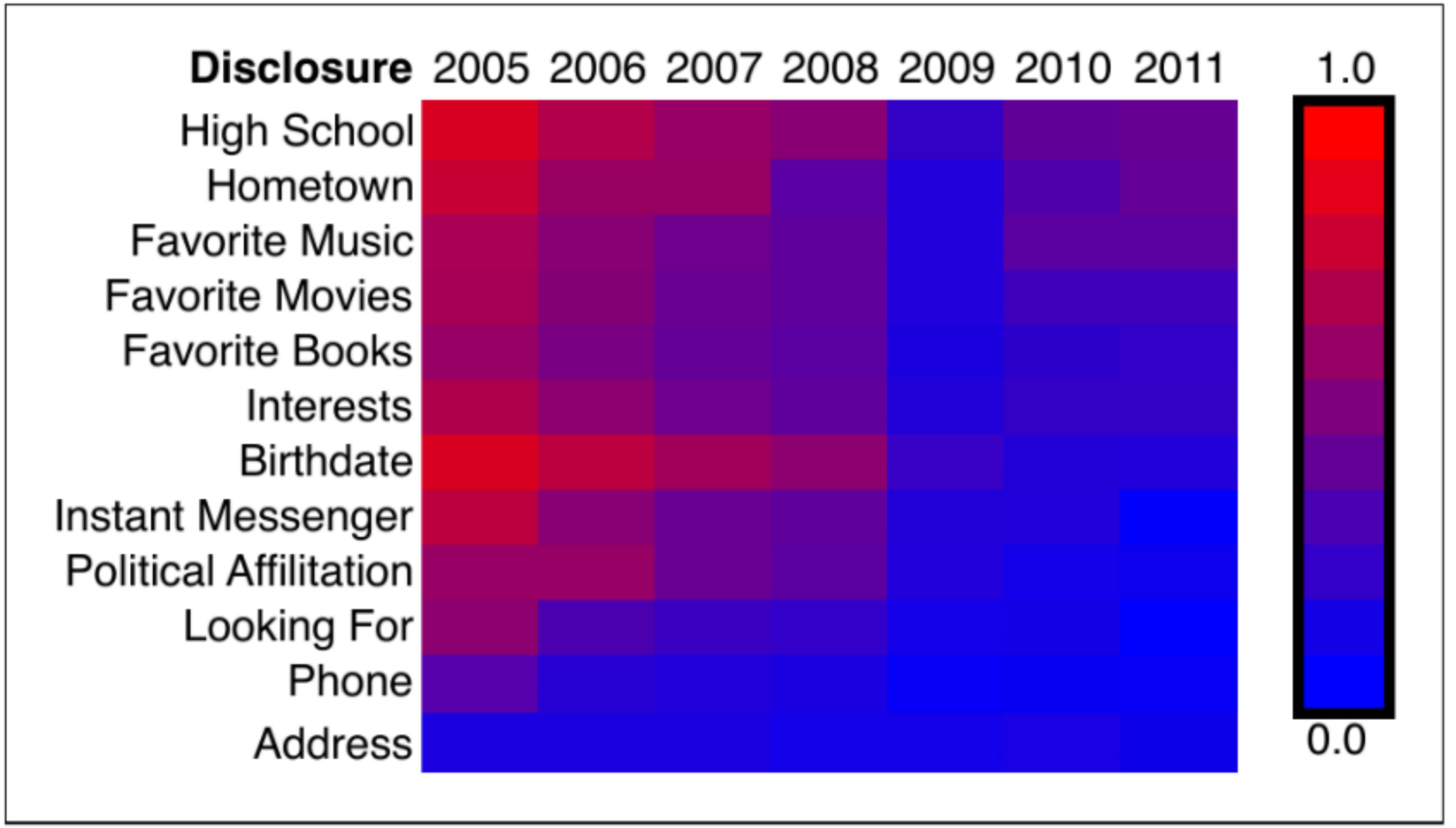
Time	Year	Collection Date	Total Obs.	Panel Obs.
t_0	2005	Nov 20	6380	5076
t_1	2006	Nov 29	10254	5076
t_2	2007	Nov 02	15041	5076
t_3	2008	Mar 01	15324	5076
t_4	2009	Oct 04	15024	5076
t_5	2010	Nov 12	15731	5076
t_6	2011	May 5	22124	5076

Facebook Profile Elements

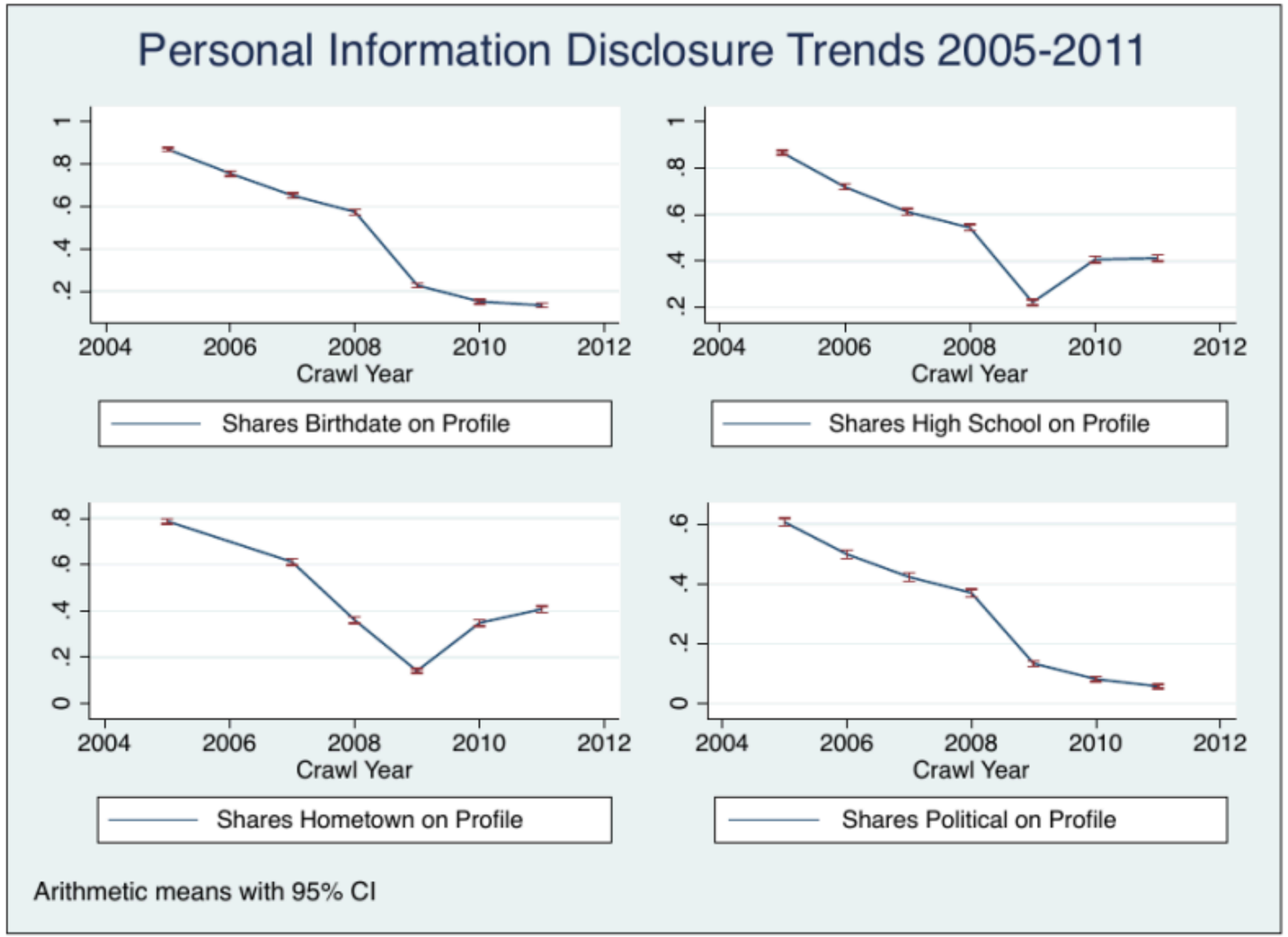
Element	Disclosure Category	Note
Birthdate	Personal	FT (mm-dd-yyyy)
High School	Personal	FT
Hometown	Personal	FT
Political Affiliation	Personal	Initially DD, later FT
Instant Messenger	Contact	FT, any IM (AIM, Skype, Y!, etc)
Phone	Contact	FT, any phone (mobile or landline)
Address	Contact	FT
Looking For	Contact	DD
Interests	Interests	Initially FT, later L
Favorite Music	Interests	Initially FT, later L
Favorite Books	Interests	Initially FT, later L
Favorite Movies	Interests	Initially FT, later L

- FT: Free text input, DD: Drop down list, L: Like button

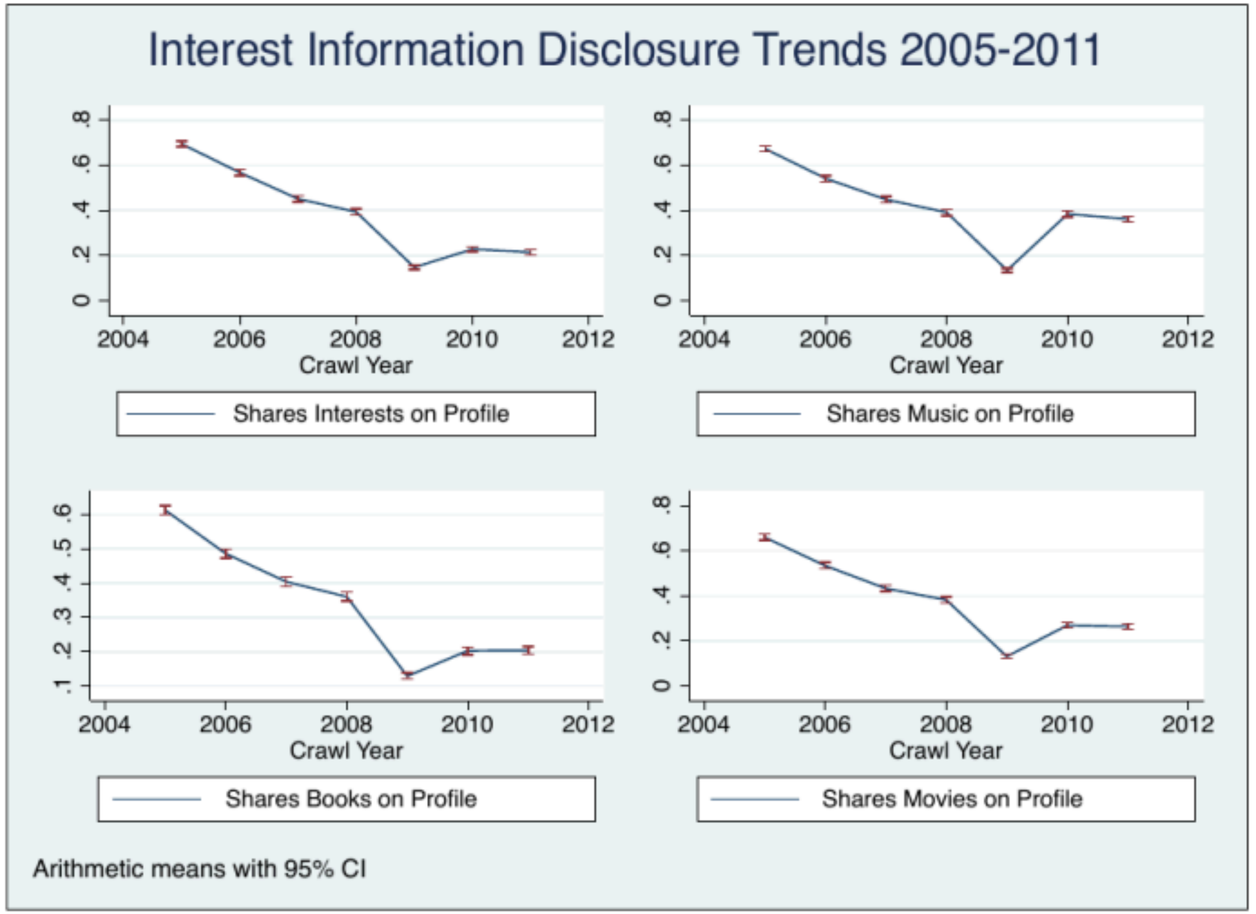
Sharing Trends



Disclosure: Personal Information

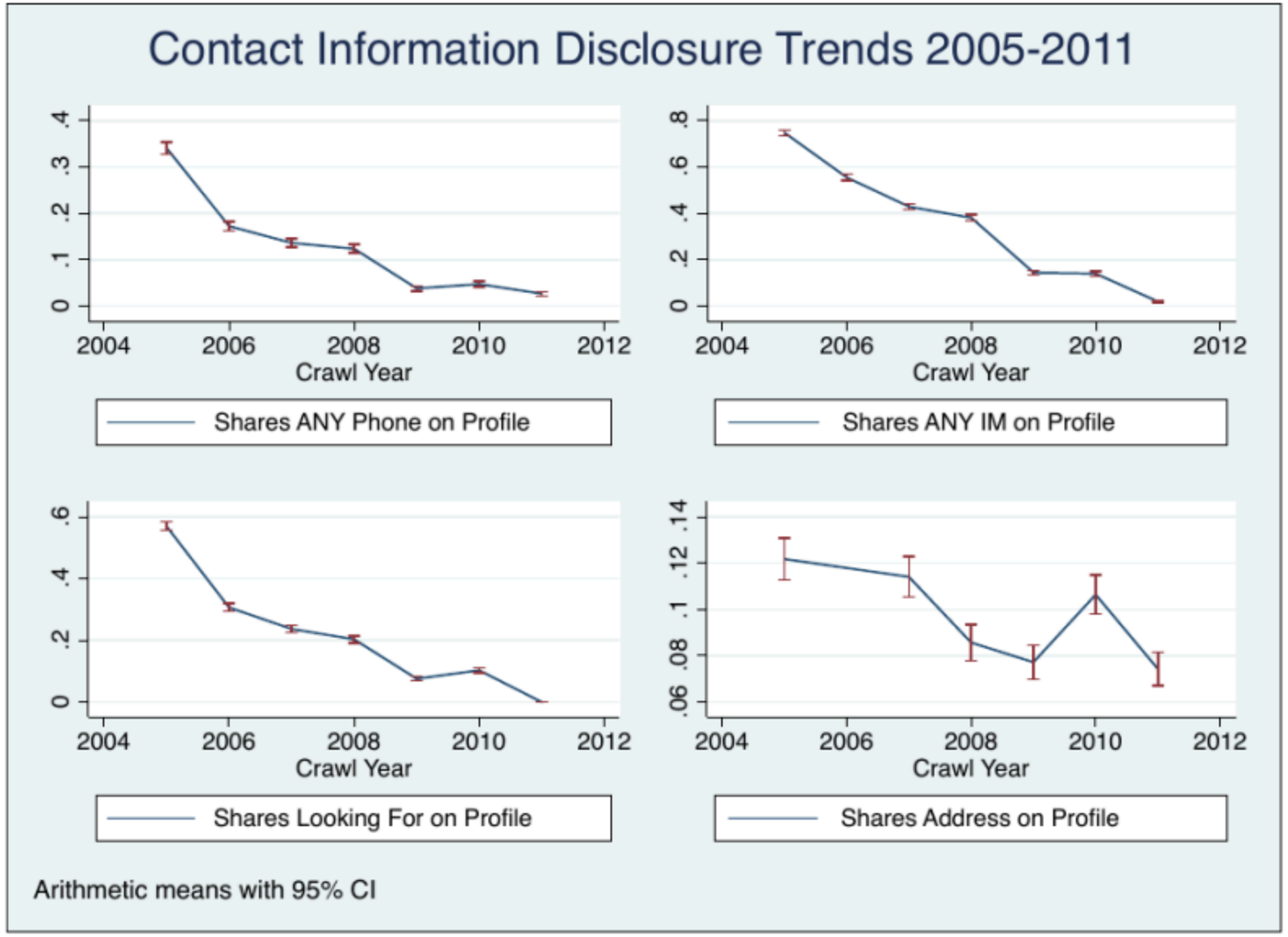


Disclosure: Interests

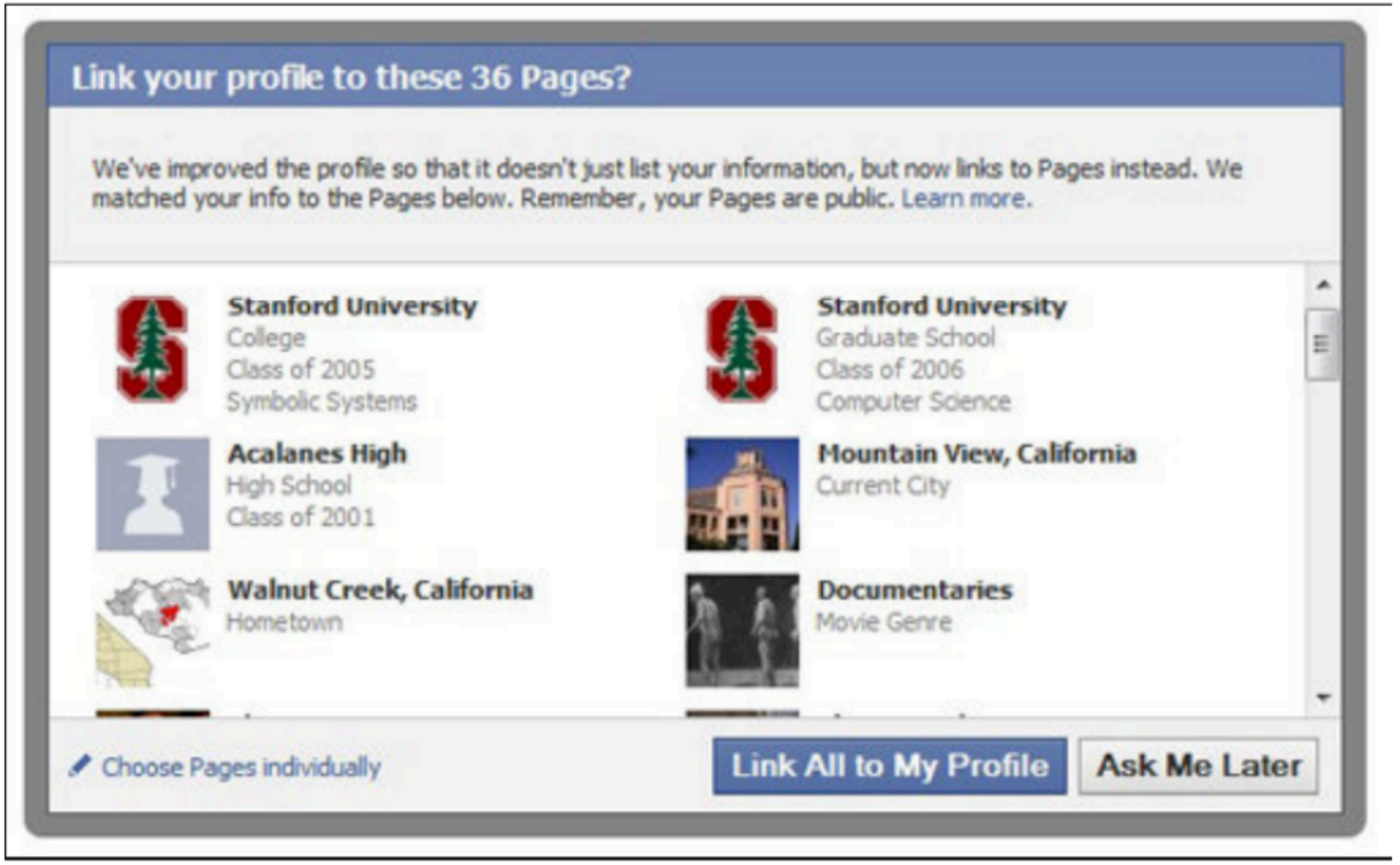


- What might have happened in 2009–2010?

Disclosure: Interests



Community Pages



Silent listeners

- While public disclosures decreased, private sharing of content increased
- This, in turn, increases disclosures to “silent listeners”
  - Facebook itself
  - Third party apps
  - Advertisers
- Disclosure without awareness or explicit consent Users underestimate their audience: They can only guess 27% of their true audience

Facebook Apps

AppName	Type	Data
ChefVille	Game	Food preferences
TripAdvisor	Travel	Trip recs./history/checkins
Yahoo! Social Bar	News/Social Reader	Yahoo activity reported
Instagram	Photo	Photo sharing/check-ins (FB)
Microsoft Live	Utilities/Communication	Social/search engine
Bing	Utilities	Social/search engine
Spotify	Music/Entertainment	Music choices
Scribd	Utilities	Interests for reading/publishing
SchoolFeed	Online Communications	Connects users to others
Between You and Me	Dating	Dating
MyPad for iPad	FB for iPad	Recreates FB for an iPad
Skype	Utilities	Communications/networking
FourSquare	Utilities	Aggregates Check-ins

Social network implications

- A user's privacy no longer depends on what they reveal.
- Temporal changes in preferences
- "Imagined audience" may not align with actual audience


Verizon
8:28 AM
72%
Girls Around Me
girlsaround.me
Verizon
9:45 AM
100%
Yawkey
Fenway Park
Van Ness St
Boylston St
Ipswich St
Fenway Victory Gardens
Riverway
Fenway/ Kenmore
Peterborough St
Queensberry St
Back Bay Fens
Park Dr
Fenway
Museum of Fine Arts
Blackfan Cir
Huntington Ave
Longwood Med Area - Outbound
Ruggles St
Ruggles
Ward St
Prentiss St
Smith St
Parker St
St Alphonsus St
Leon St
Google

What went wrong?

- Root cause: what went wrong?
- If it was not intentional, what was the original aim?
- Mitigation: prevention, detection, recovery

SNSs are a wide category

- Many different sites: Facebook, TwiMer, Google+, Snapchat, Tumblr, etc.
- Varied functionalities, focuses, norms, etc.
- Different types of users
- Range of privacy threats/options

Twitter regrets

"I read my Twitter the next morning and was astonished" A Conversational Perspective on Twitter Regrets

Manya Sleeper*, Justin Cranshaw*, Patrick Gage Kelley†, Blase Ur*, Alessandro Acquisti*, Lorrie Faith Cranor*, Norman Sadeh*

*Carnegie Mellon University
{msleeper, jcransh, bur, acquisti, lorrie, sadeh}@cmu.edu

†University of New Mexico
pgk@unm.edu

ABSTRACT

We present the results of an online survey of 1,221 Twitter users, comparing messages individuals regretted either saying during in-person conversations or posting on Twitter. Participants generally reported similar types of regrets in person and on Twitter. In particular, they often regretted messages that were critical of others. However, regretted messages that were cathartic/expressive or revealed too much information were reported at a higher rate for Twitter. Regretted messages on Twitter also reached broader audiences. In addition, we found that participants who posted on Twitter became aware of, and tried to repair, regret more slowly than those reporting in-person regrets. From this comparison of Twitter and in-person regrets, we provide preliminary ideas for tools to help Twitter users avoid and cope with regret.

Author Keywords

Thus it is worthwhile to investigate regret both on Twitter and for in-person conversations. Past studies of in-person regret have identified factors that lead to regret, methods for becoming aware of regret, and strategies for repairing harm [8, 15, 16]. However, Twitter presents different features and limitations than offline conversation. Beyond offering wider audiences and increased message persistence, Twitter lacks face-to-face channels, such as body language, for transmitting apologies or indicating offense.

We explore regretted messages Twitter users posted on Twitter or said during in-person conversations. We aim to improve understanding of regrets on Twitter by comparing them with in-person regrets. By examining these regrets, as well as how people became aware of regrets in person and on Twitter, we also identify preliminary design directions for preventing and ameliorating regrets on Twitter.

Social network implications

- A user's privacy no longer depends on what they reveal.
- Temporal changes in preferences
- "Imagined audience" may not align with actual audience
- "Context collapse" combines separate offline groups (e.g., friends, family, coworkers)

If you turned up dead, no one would miss you!

It's easy to **say** something you **regret**.

I hate you!

You look like you've gained a lot of weight…

Past research analyzed in-person regret

- Factors leading to regret
- Types of regret
- Awareness of regret
- Strategies to repair regret

It’s also possible to tweet something you regret

Thanks for putting me at risk of getting fired

Maybe, if you would take your stupid elsewhere…I wouldn’t have to be so blunt

Man, I hate you, you are the worst person ever, should’ve never been born

What's new in Twitter

- Wider audiences
- Lack of face-to-face channel
- Increased persistence

Regretted messages on Twitter and in person

- What states lead to regret?
- What types of regret occurred?
- How did people become aware of regretted messages?
- What repair strategies did people use to cope with regretted messages?

Large-scale online survey

- Amazon Mechanical Turk
- 1,221 Twitter users
  - English proficiency
  - Relatively frequent Twitter use
  - Reported a regret

Survey with two conditions

- Conversational and Twitter conditions
- Asked to “recall an occasion when” said or tweeted something and then regretted it •
- Described:
  - Regret
  - Circumstances leading to regret
  - How became aware of regret
  - Repair strategies

Data coding and analysis

- Coded open response questions based on in-person conversational regrets literature
- Did not perform statistical comparisons across conditions
  - Different contexts (Twitter/conversation)
  - Qualitative explored themes/trends
  - Performed statistical tests within conditions

States leading to regret

- Negative emotional (common)
  - Stress
  - Anger
  - Frustration
- Positive emotions (less common)

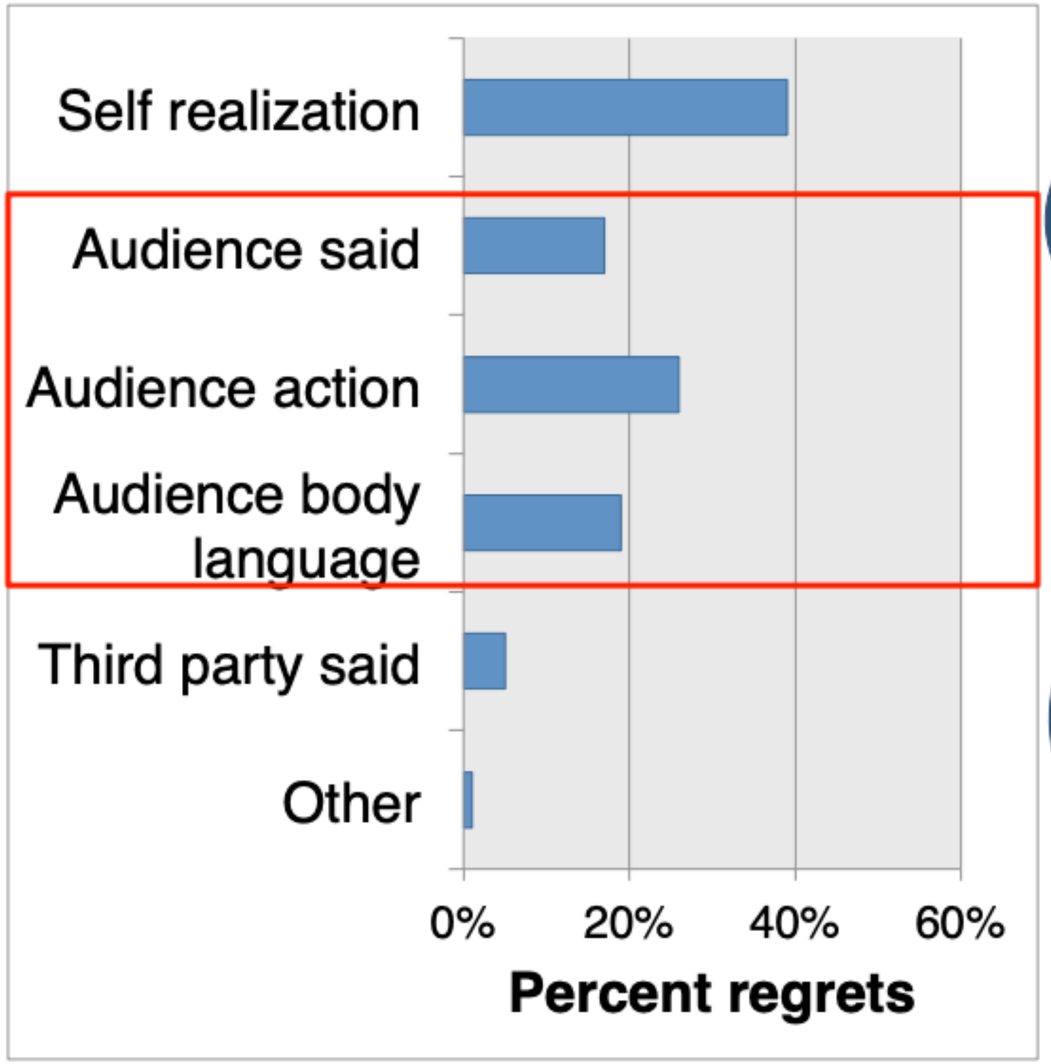
Types of regrets

- Most common:
  - Direct criticism
  - Direct attack
  - Implied criticism
  - Expressive
  - Revealed too much
  - Blunder

Types and audience

- Asked participants for intended audience
- Twitter participants tended to target multiple people (73% reported)
- Types significantly more likely to be targeted at multiple people:
  - Blunders (82%)
  - Expressive content (84%)
  - Content that revealed too much (80%)

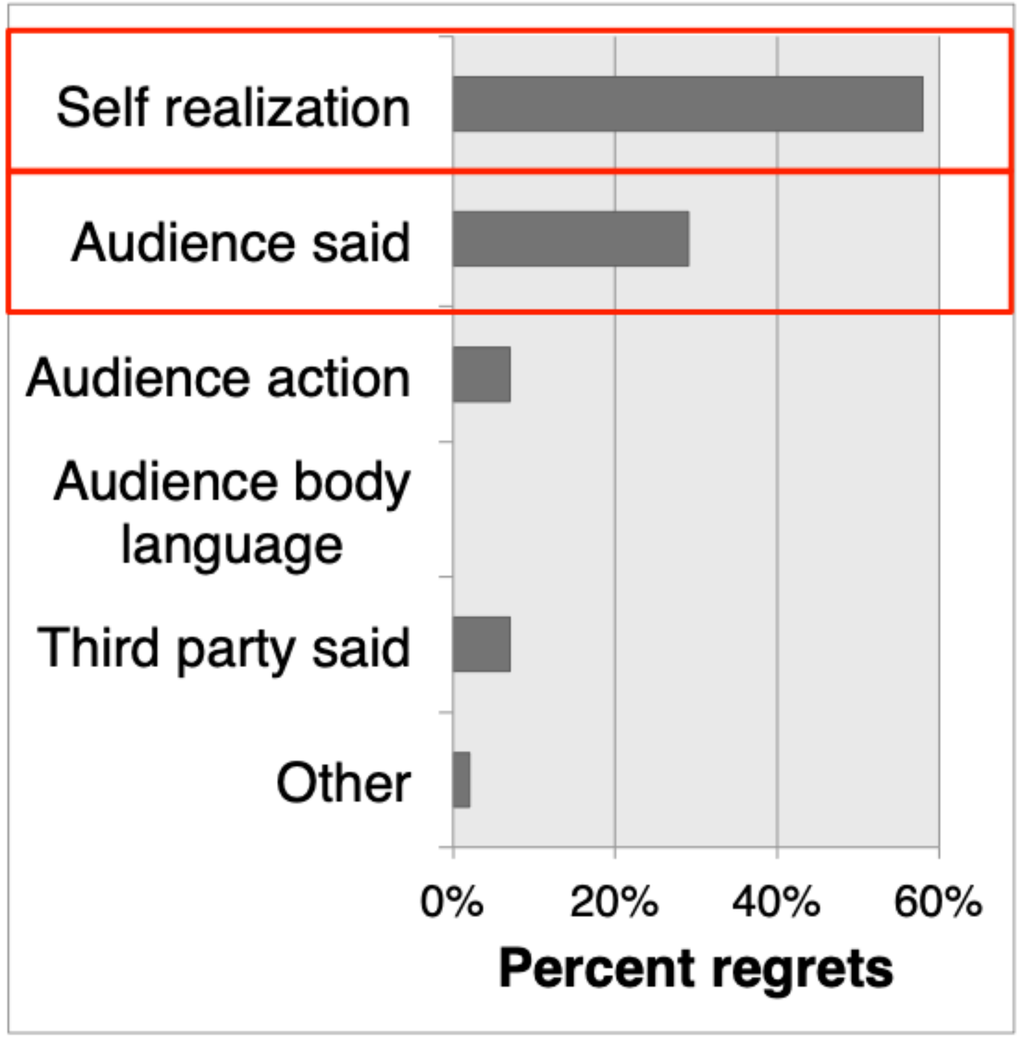
Awareness: Conversation



"When he gave me an angry look and yelled at me"

"When she began to cry I realized how much I hurt her…"

Awareness: Twitter

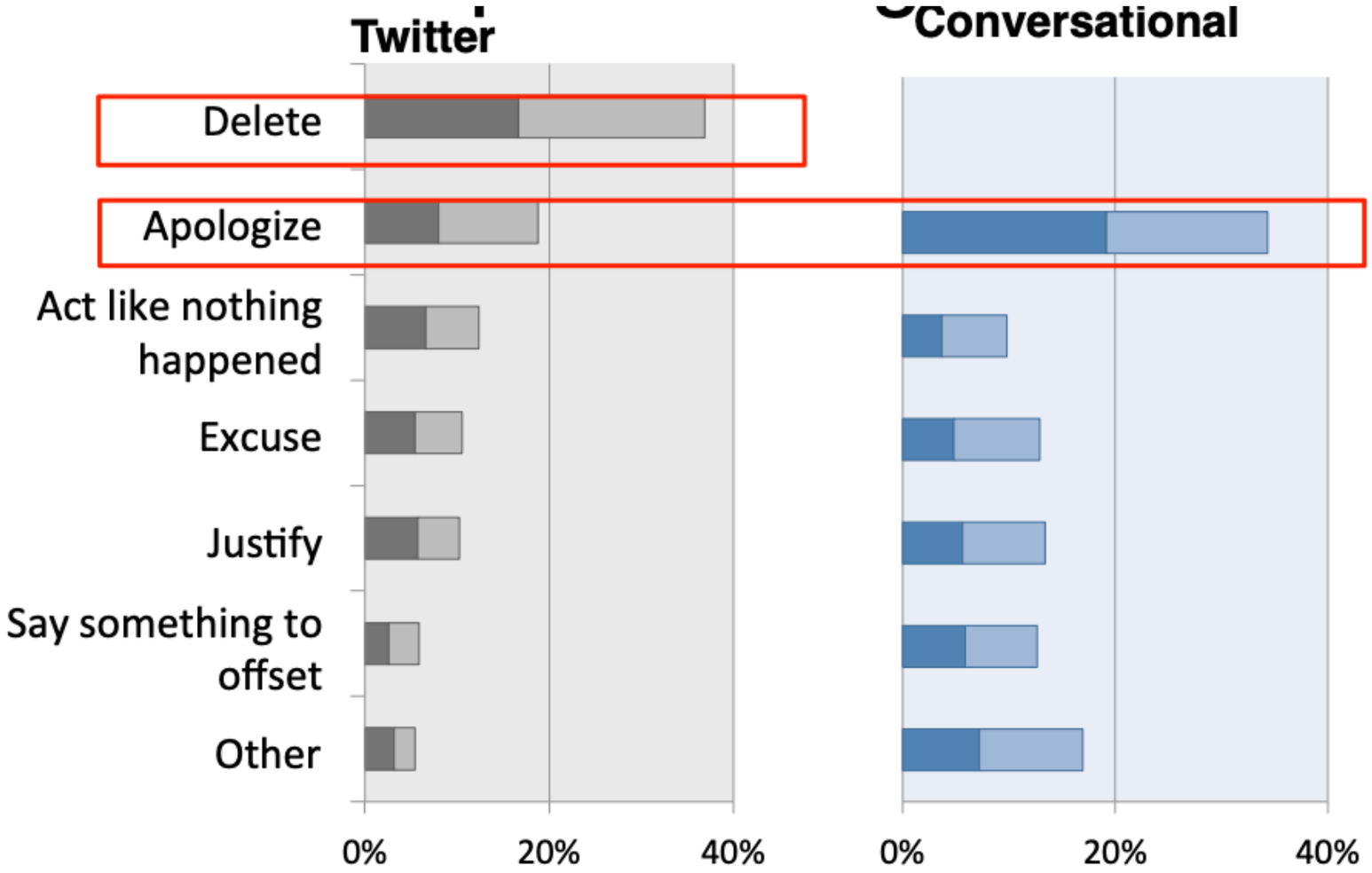


"As soon as I got a text from the girl I had vented on twitter about. She was none to happy."

"Re-reading it the

"Once some of my old classmates and friends DM me and told me to stop and that it was very immature of us."

Repair strategies



Time to awareness and repair

- Most conversational awareness immediate (63%), repaired within few minutes (52%)

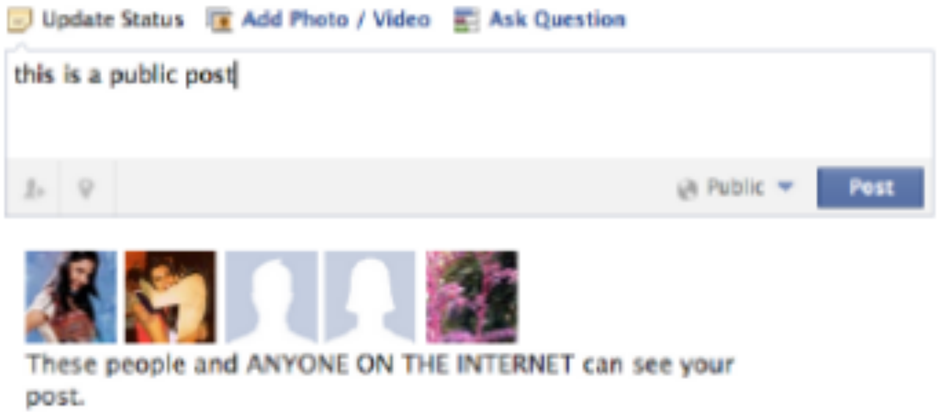
- Twitter participants reported awareness and repair that lagged (hours or days later)

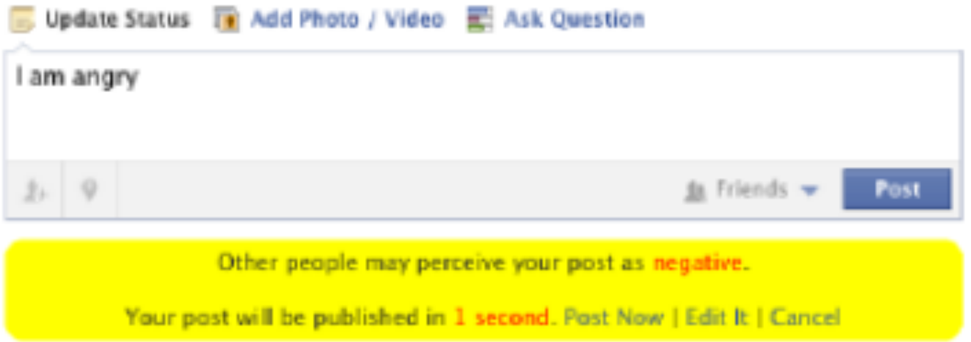
Social network implications

- A user's privacy no longer depends on what they reveal.
- Temporal changes in preferences
- "Imagined audience" may not align with actual audience
- "Context collapse" combines separate offline groups (e.g., friends, family, coworkers)
- Privacy tools may be unclear/hard to use

Privacy “nudges”

- Designed “nudges” for Facebook to encourage users to consider sharing decisions
- 6-week field trial with Facebook users (n=28)
- Some parQcipants found the “nudges” useful, while others found them annoying





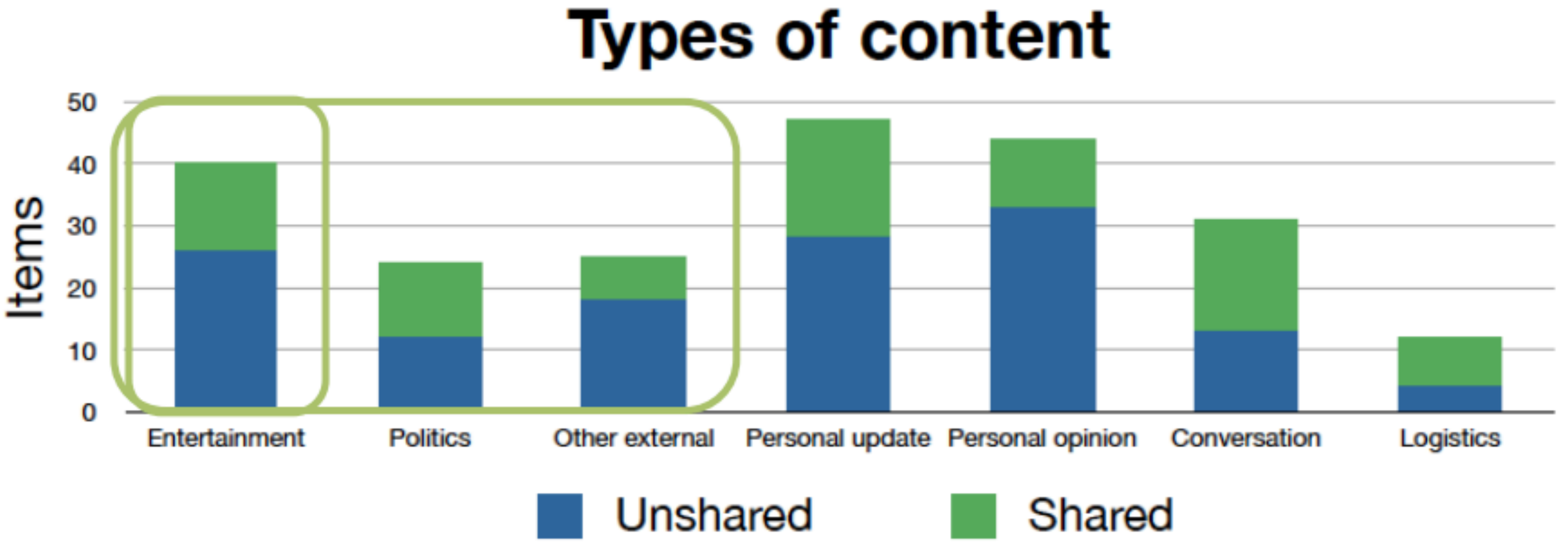
Self-censoryship

- When we look at Facebook we can see what people have <u>posted</u>.

- We don’t see what people don’t post

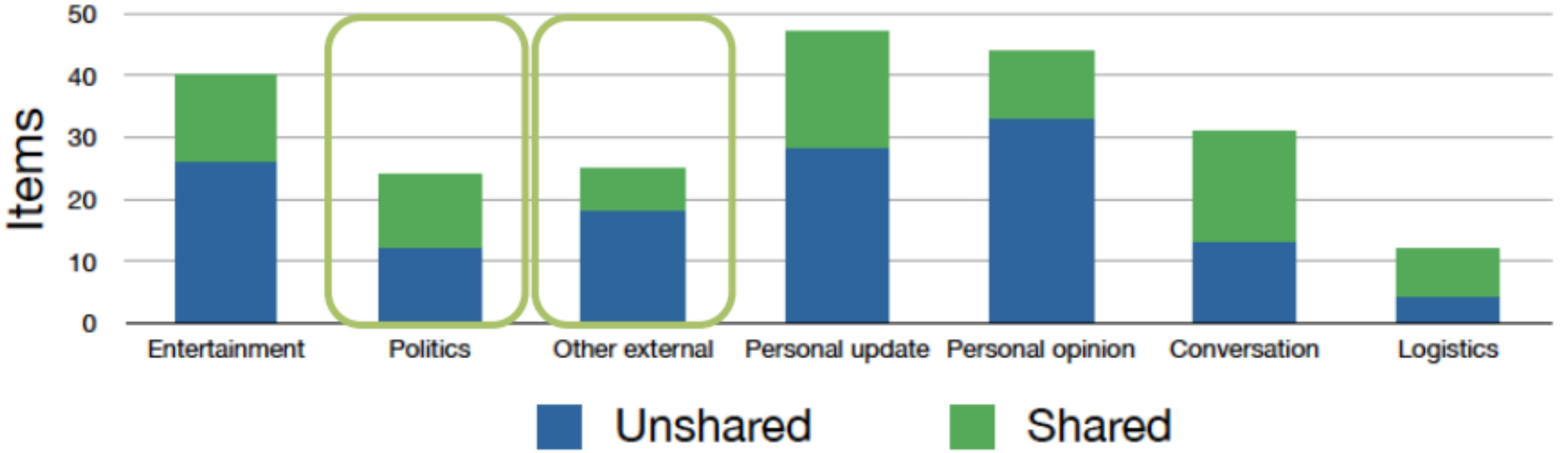
Data coding

- Coded for:
  - Types of content
  - Reasons for not sharing
  - Types of people would have wanted to share with/block (where relevant)
- Used data from nightly surveys and interview
- Iteratively coded all items



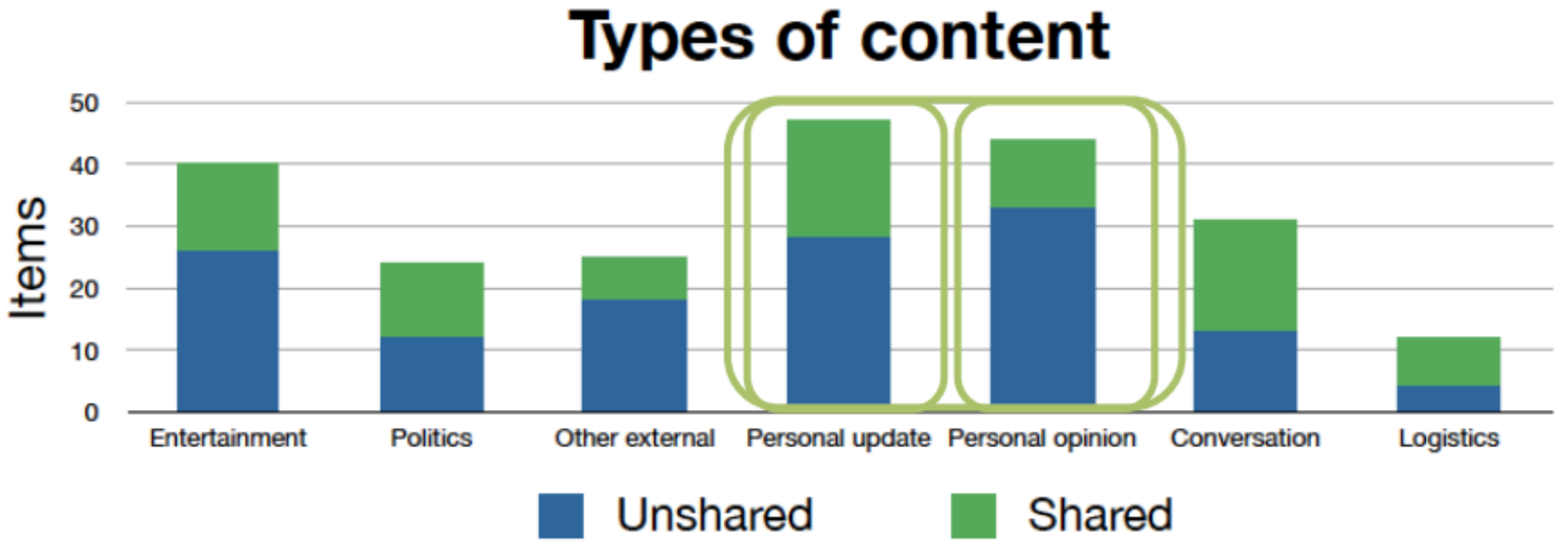
Drug-related video that a participant decided not to share because her “family in Austin is really religious”

Types of content



Decided not to post a “Link to article about young black republicans” to avoid controversy

Wanted to post links to “articles I read on NPR and WeArePowerShift.org – very political stuff” but “I like to keep politics off my Facebook page”



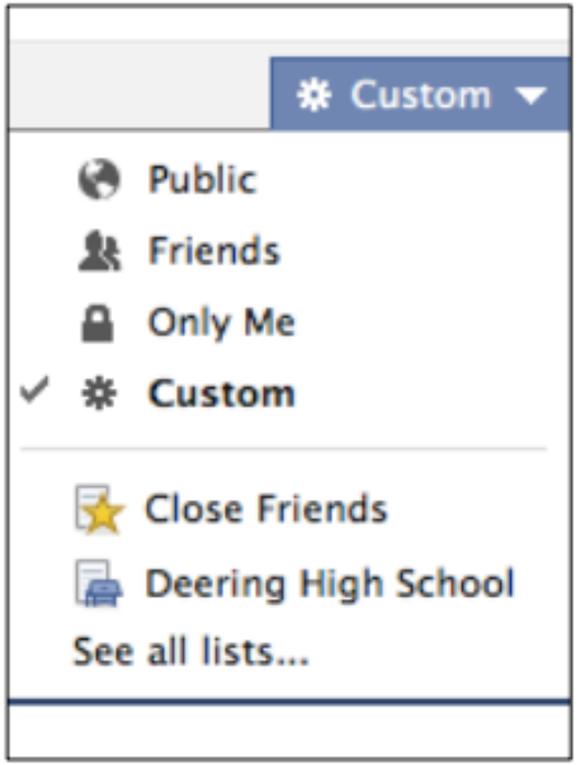
"My brother-in-law wants to get a tattoo and I was going to comment on how stupid it was; but I decided not to"

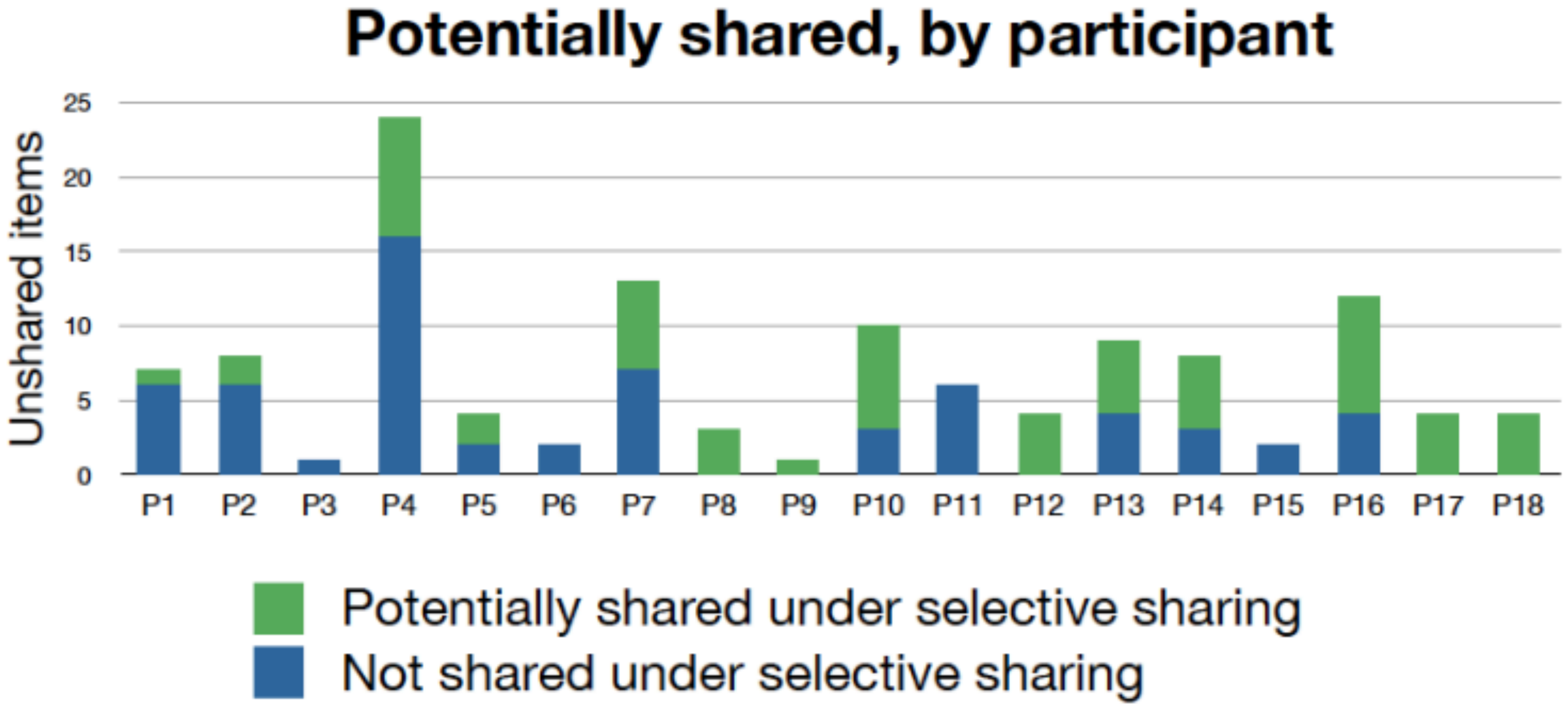
Reasons for not sharing

- Presentation of self
- Potentially offensive
- Boring/repetitive
- Avoid argument/ discussion
- Inconvenient

Selective sharing

- Optimal selective sharing:
  - how much would have shared if could have only targeted particular audiences
- Could have shared item only with people they wanted to share it with
- Could have prevented people they didn't want to see item from viewing it

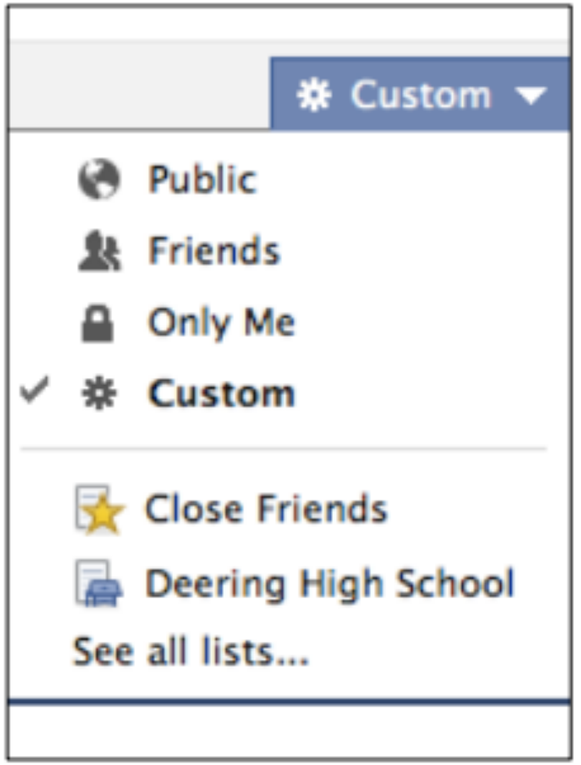




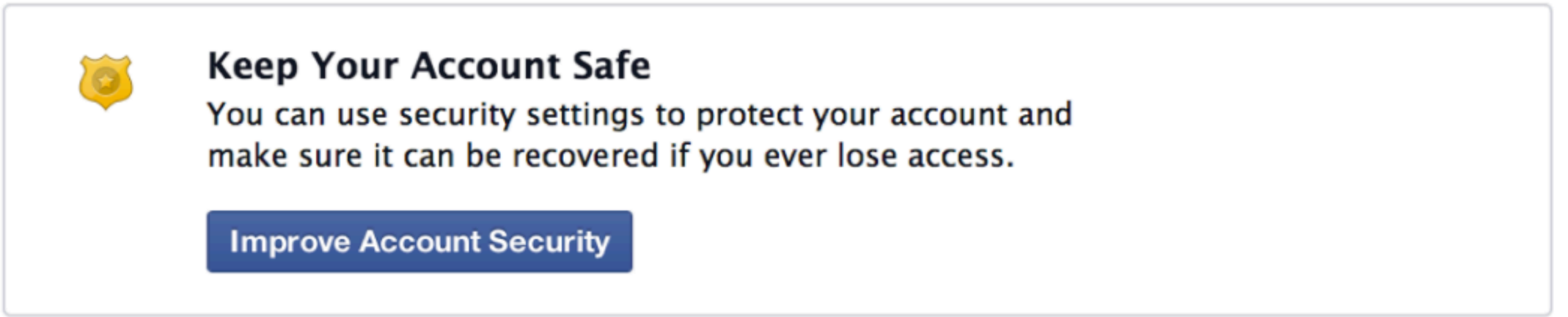
- Approximately half of unshared content would potentially be shared under opQmal selecQve sharing

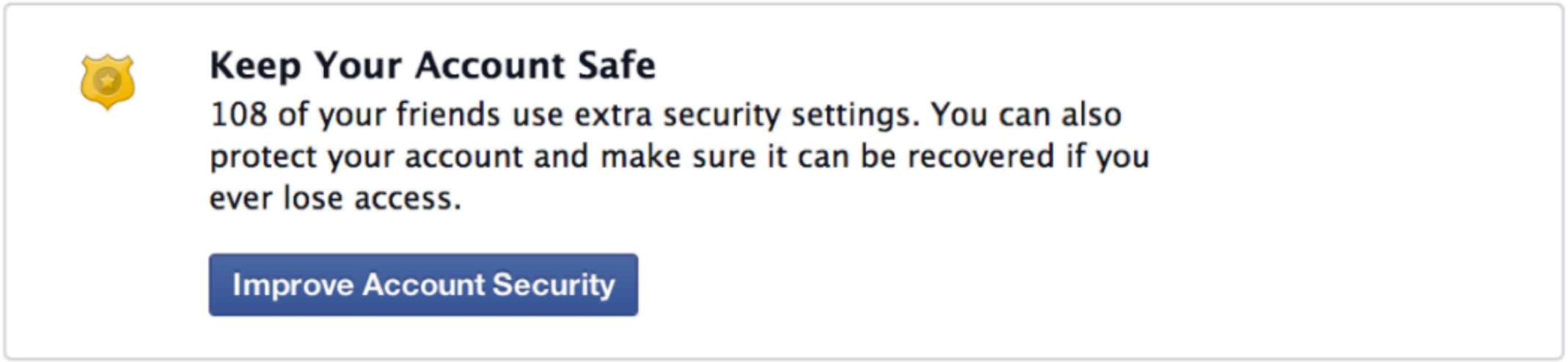
Types of groups for selective sharing

- Interface grouping mechanism
- Manual specification (allow list or deny list)
- Context-specific information?
- Unknown traits?



Social cybersecurity



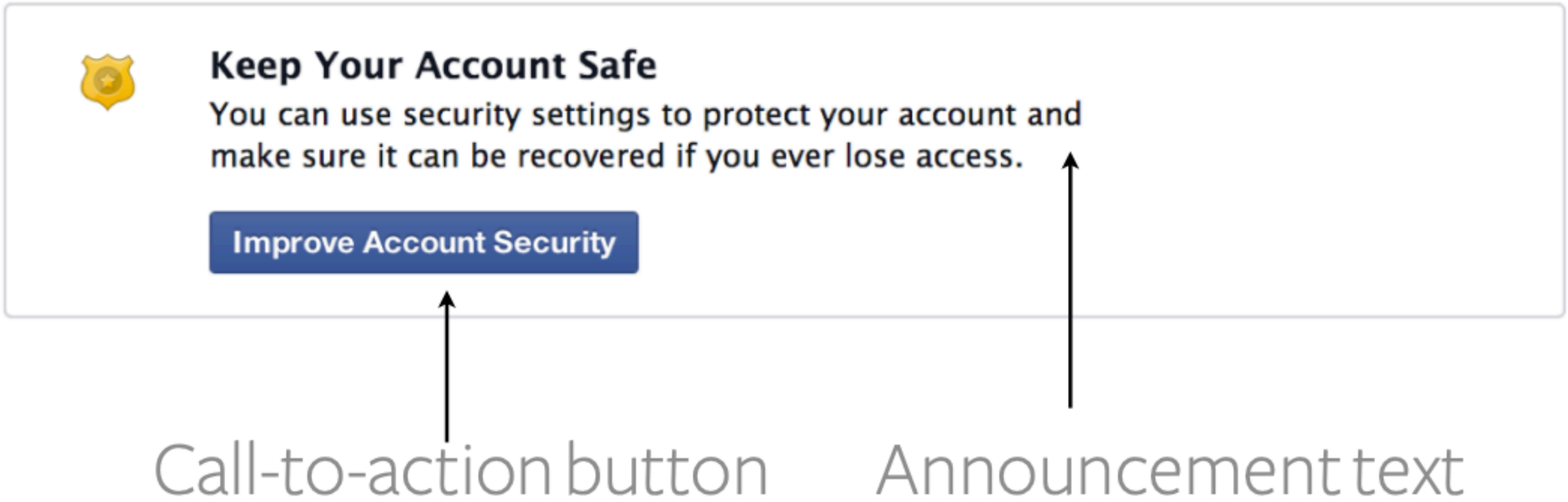


showed 50,000 facebook users an announcement urging them to explore security tools.

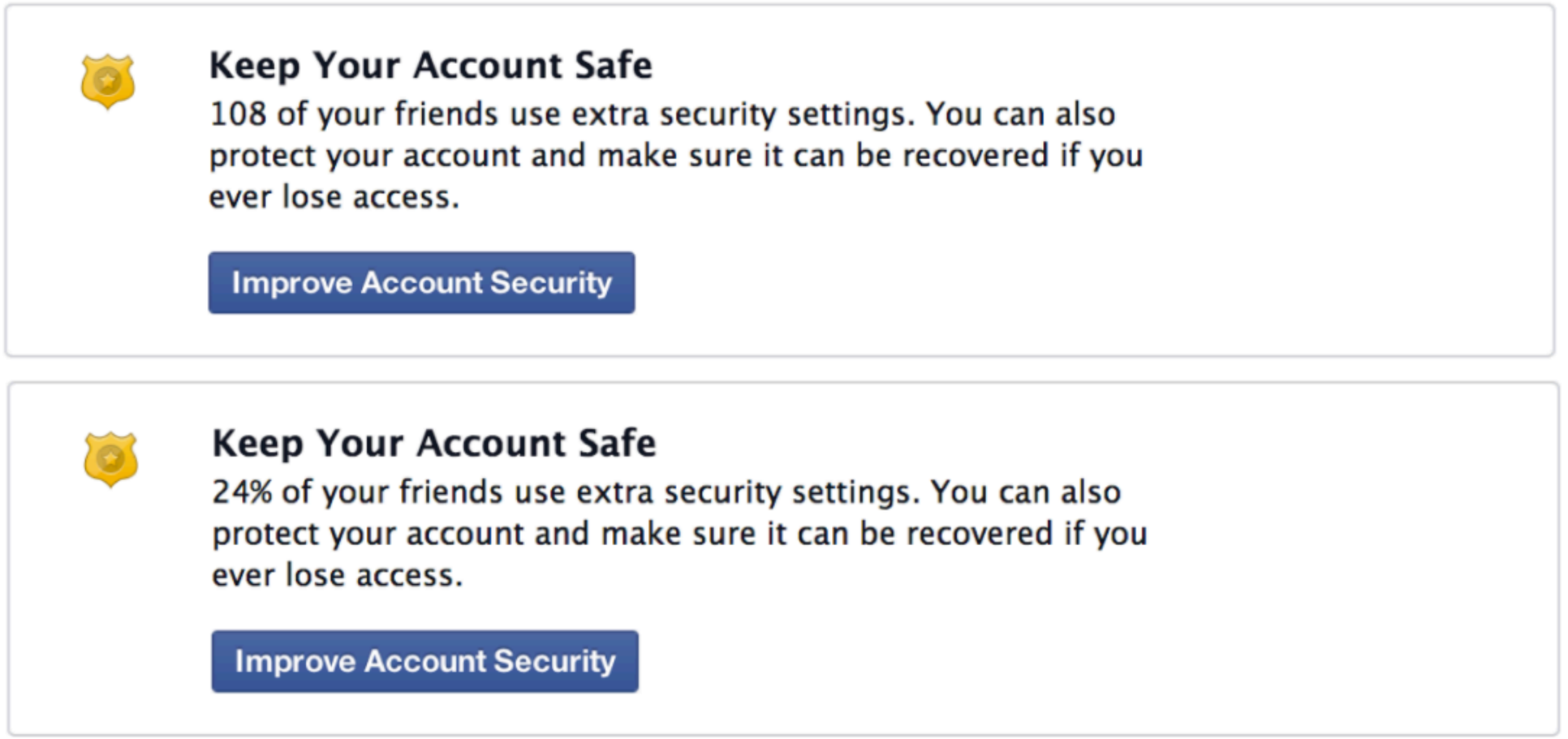
Methods: Social Prompt Experiment

- Controlled, randomized experiment with 50,000 active facebook users.
- Part of annual security awareness campaign run by facebook, promoting the following three voluntaryuse security tools:
  - Login approvals
  - Login notifications
  - Trusted contacts

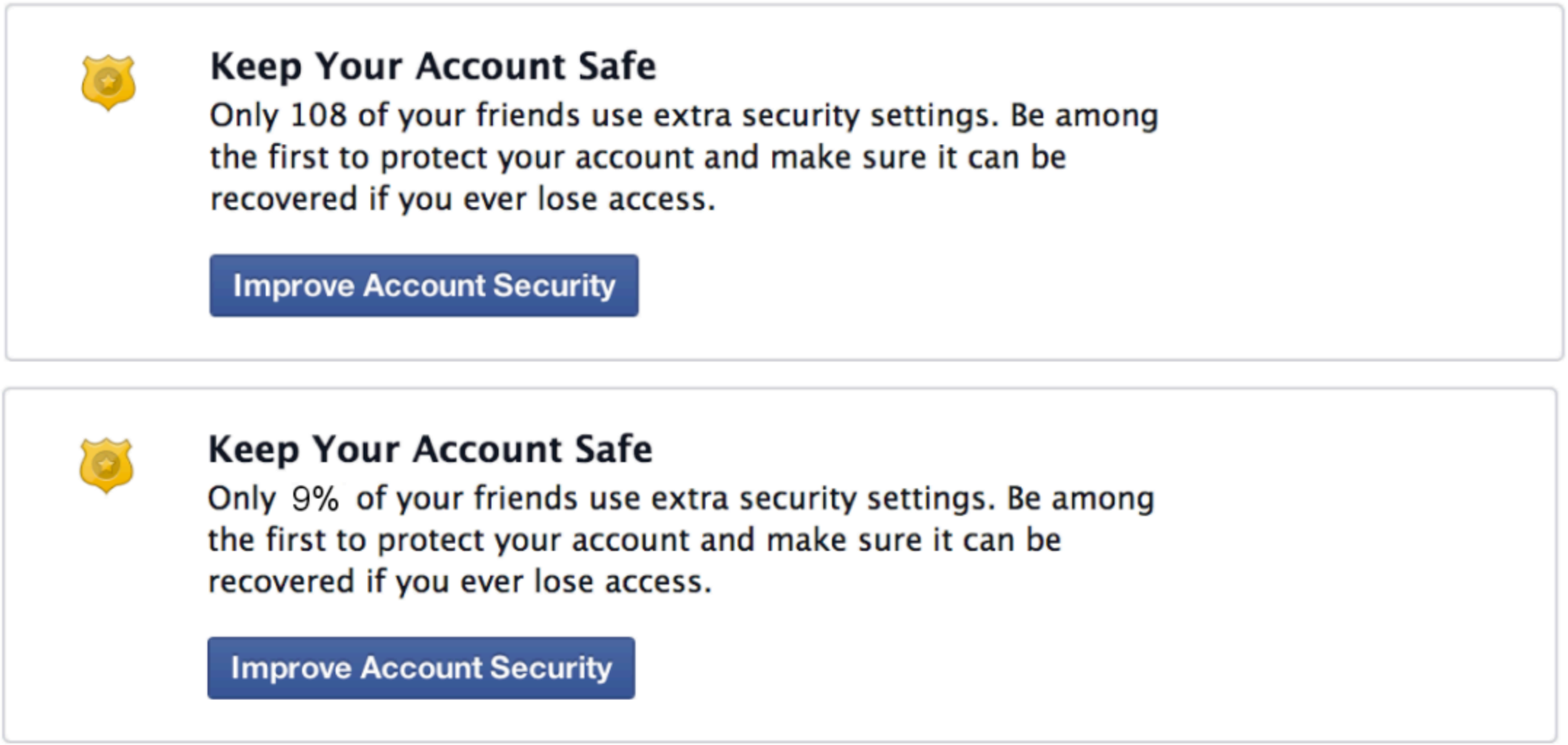
Methods: Social Prompt Experiment



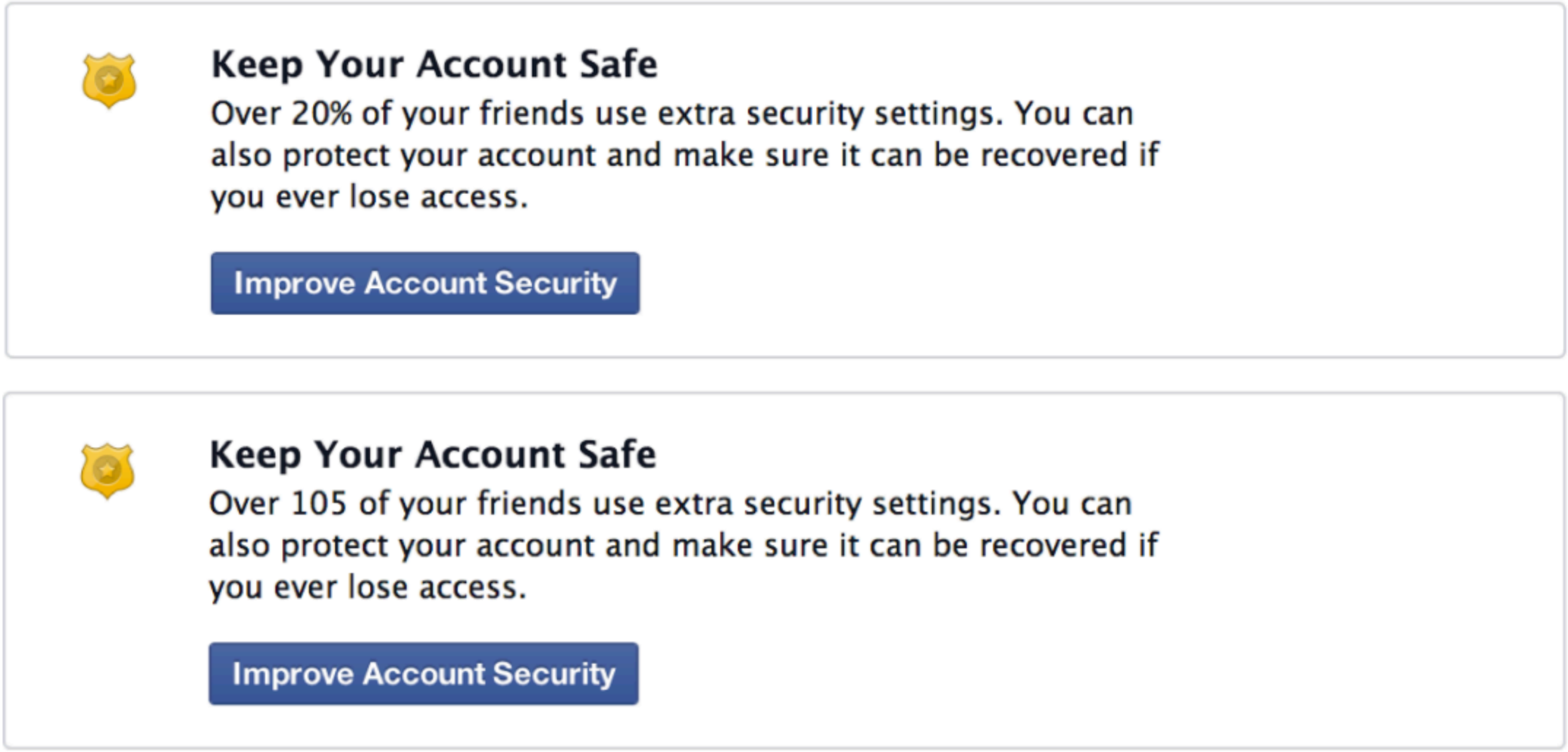
Adding social proof (7 variations) - Neutral



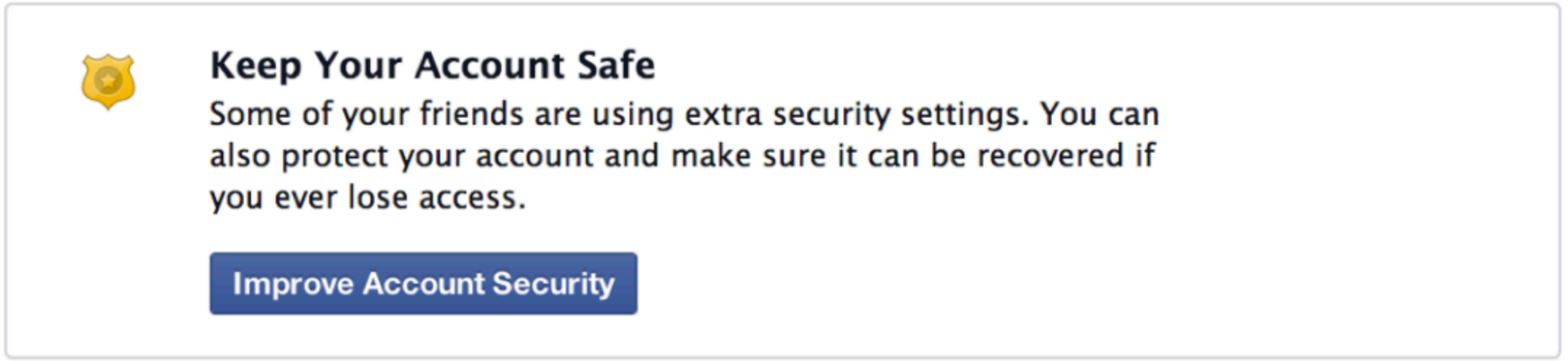
Adding social proof (7 variations) - Negative



Adding social proof (7 variations) - Positive



Adding social proof (7 variations) - Some



Measure

- Click-through rate (awareness)
- 7-day adoptions (motivation)
- 5-month adoptions (motivation)

Raw overview

Group	N	Clicks	7-day adoptions	5-month adoptions
Raw #	5862	846 (14.4%)	280 (4.8%)	623 (10.6%)
Some	5828	835 (14.3%)	243 (4.2%)	602 (10.3%)
Over #	5770	779 (13.5%)	248 (4.3%)	547 (9.5%)
Only #	5668	748 (13.2%)	225 (4.0%)	548 (9.7%)
Over %	5761	724 (12.6%)	223 (3.9%)	557 (9.7%)
Only %	5708	714 (12.5%)	221 (3.9%)	555 (9.7%)
Raw %	5953	730 (12.3%)	225 (3.8%)	573 (9.6%)
Control	5685	595 (10.5%)	208 (3.7%)	550 (9.7%)

Raw overview

Group	N	Clicks	7-day adoptions	5-month adoptions
Raw #	5862	846 (14.4%)	280 (4.8%)	623 (10.6%)
Some	5828	835 (14.3%)	243 (4.2%)	602 (10.3%)
Over #	5770	779 (13.5%)	248 (4.3%)	547 (9.5%)
Only #	5668	748 (13.2%)	225 (4.0%)	548 (9.7%)
Over %	5761	724 (12.6%)	223 (3.9%)	557 (9.7%)
Only %	5708	714 (12.5%)	221 (3.9%)	555 (9.7%)
Raw %	5953	730 (12.3%)	225 (3.8%)	573 (9.6%)
Control	5685	595 (10.5%)	208 (3.7%)	550 (9.7%)

Privacy paradox

If you receive a friendship request, which of the following will you accept?

	Q43, N = 6,929
Person of opposite gender	[redacted]
People from my hometown	
Person with nice profile picture	
Strangers (people you do not know)	
Somebody, whom you do not know or recognize but have mutual / common friends with	
Anyone	

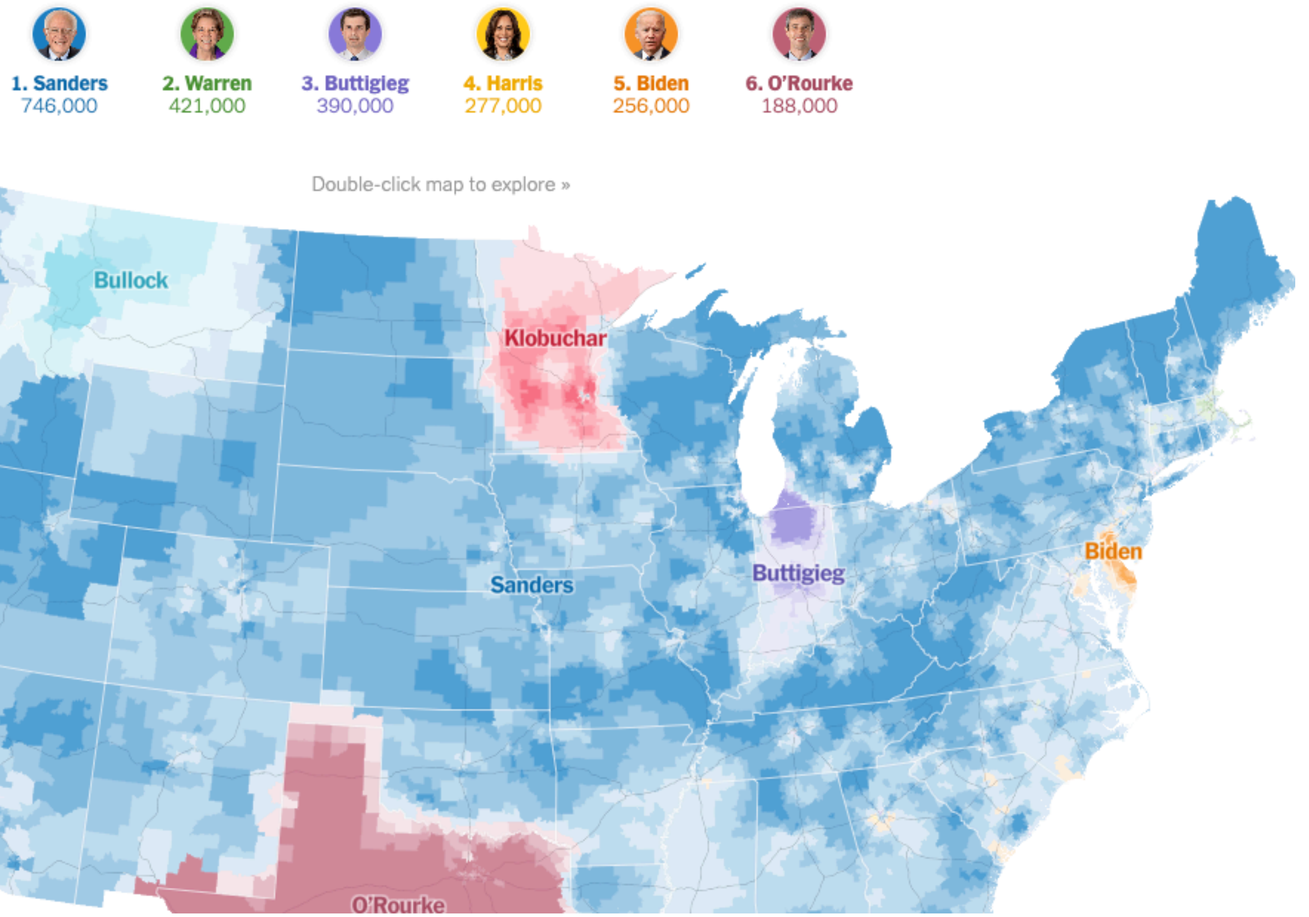
The New York Times

Detailed Maps of the Donors Powering the 2020 Democratic Campaigns

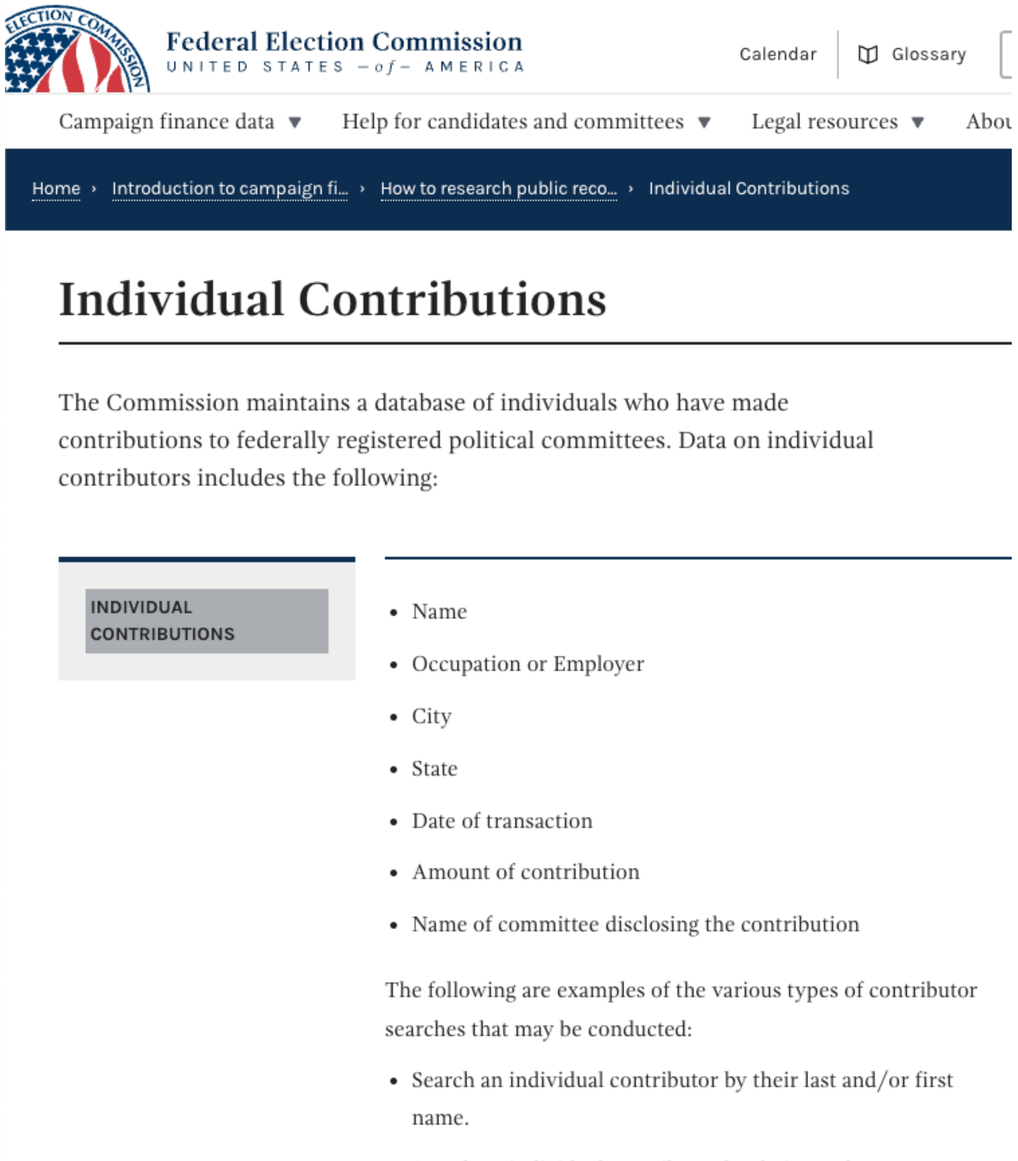
By Josh Katz, K.K. Rebecca Lai, Rachel Shorey and Thomas Kaplan Aug. 2, 2019

Candidates with the most individual donors

Darker shades on the map indicate a greater share of estimated donors.



Political donations are public knowledge in some countries



Federal Election Commission
UNITED STATES —of— AMERICA

Calendar | Glossary

Campaign finance data ▼ Help for candidates and committees ▼ Legal resources ▼ Abou

Home › Introduction to campaign fi… › How to research public reco… › Individual Contributions

Individual Contributions

The Commission maintains a database of individuals who have made contributions to federally registered political committees. Data on individual contributors includes the following:

INDIVIDUAL CONTRIBUTIONS

- Name
- Occupation or Employer
- City
- State
- Date of transaction
- Amount of contribution
- Name of committee disclosing the contribution

The following are examples of the various types of contributor searches that may be conducted:

- Search an individual contributor by their last and/or first name.

https://www.fec.gov/introduction-campaign-finance/how-to-research-public-records/individual-contributions/

You want to donate money to your favorite political candidate, but many of the people you know aren't aware that you support him.

Your boss finds out about your political leanings, and you are passed over for a promotion. You are pretty sure it is because your boss is unsympathetic to your beliefs, but you can't prove it.

You want to donate money to your favorite political candidate, but many of the people you know aren't aware that you support him.

Your next door neighbors find out about your political leanings. You hadn't realized it, but they strongly support the opposing party and they had assumed you did as well. Now every time you see them, they try to change your mind about how you are going to vote. They are polite but extremely annoying.

Inclusive privacy

- Privacy for visually impaired
- Privacy for vulnerable population
- Privacy (settings) for motor impaired

Recap

Social network implications

- A user's privacy no longer depends on what they reveal.
- Temporal changes in preferences
- "Imagined audience" may not align with actual audience
- "Context collapse" combines separate offline groups (e.g., friends, family, coworkers)
- Privacy tools may be unclear/hard to use

Other:
Election, Inclusive privacy

Credit

1. http://cups.cs.cmu.edu/courses/ups-sp16/23-socialnetworks-privacy.pdf
2. https://ozgurkafali.github.io/courses/ncsu/Lecture2-Inference.pdf