

# CS 6474/CS 4803 Social Computing: Privacy

*Munmun De Choudhury*

[munmund@gatech.edu](mailto:munmund@gatech.edu)

Week 15 | November 29, 2017

Please take the Course Instructor  
Opinion (CIOS) survey!!!

*<http://b.gatech.edu/cios>*

# Final presentation specs

- Room CoC 016 – Mon Dec 4
- Total 9 teams. Each team gets 15 minutes in all
  - 10-12 minutes of presentation
  - 3-5 minutes of Q&A
- Each team member needs to be present
- We will start at 4:30pm. Hoping to wrap up at around 6:45pm.
- Structure:
  - Main idea
  - Background/Motivation
  - Research questions/Goals
  - Data/Social media platform
  - Method
  - Results
  - What you have learned

1. What can we do with data generated from social computing systems?

2. What should we **not** do with these data.

# Data ex Machina: Introduction to Big Data

# Data, Privacy, and the Greater Good

# Defining Privacy

- Privacy related to notion of access
- Privacy is not “being alone”, but defining who has access to what
- Access
  - Physical proximity to a person
  - Knowledge about a person
- Privacy is a “zone of inaccessibility”
- Privacy violations are an affront to human dignity
  - You violate privacy when you treat a person as a means to an end.
  - Some things ought not be known – you look away when your friend is typing their password
- Too much individual privacy can harm society
- Where to draw the line?

# Harms of Privacy

- Cover for illegal or immoral activities
- Hidden dysfunctional families
  - Incidents of domestic violence
- Ignored people on society's fringes
  - People with disability e.g., with mental illness



# Benefits of Privacy

- Individual growth
  - Necessary to blossom into a unique individual
- Individual responsibility
- Freedom to be yourself
  - Nobody likes to be videotaped or “watched” all the time
- Intellectual and spiritual growth
- Development of loving, trusting, caring, intimate relationships

# Class Exercise I

Discuss the harms and benefits of privacy on social computing platforms.


# Rule #1

---

- ❖ It is safe to assume if you put information online it isn't 100% private.
- ❖ A video to get us started:  
[http://www.youtube.com/watch?v=5P\\_0s1TYpJU](http://www.youtube.com/watch?v=5P_0s1TYpJU)



[https://www.youtube.com/watch?v=5P\\_0s1TYpJU](https://www.youtube.com/watch?v=5P_0s1TYpJU)



With your permission, you give us more permission. If you give us information about who some of your friends are, we can probably use some of that information, again, with your permission, or improve the quality of our searches. We don't need you to type at all, because we know where you are, with your permission. We know where you have been, with your permission. We can more or less guess what you are thinking about. – *Eric Schmidt, Google CEO (The Atlantic)*

# Legal-ease

---

- ❖ Legally, read all platforms terms of service (TOS) for the nitty gritty, social media platforms can share some of your basic information.
- ❖ But why?
  - ❖ Social networks that provide their services without user fees make a profit by selling advertising. This is often done through behavioral advertising, also known as targeting. Facebook Pages who boost posts and promote their brands through ads use the same targeting methods when pushing their content.



# Geo-Locate Privacy?

---

❖ If you use Fourquare or Instagram or even have the location settings turned on for Facebook and Twitter than you are sharing your location. On Twitter you are sharing it with everyone and since it is a live update tool then you are letting everyone know exactly where you are and when and with who if you have tagged or taken a photo.



# Settings vary across platforms

---

- ❖ Each social media platform has different privacy settings and they change their rules frequently. Facebook just updated their privacy settings in May of 2014, did you know? Did you just click the “Yes, I Agree” without reading?



# What could Facebook possibly know?

---

- ❖ Anything you provide them. Think about it..

- ❖ Name, City of birth, City of residence, Phone, Email, Current employment, Previous employment, Relationship, Anniversary, Previous relationships, Previous names (aliases), Screen names, Address book, Family members, Birthday, Religious views, Friends, Books you've read, Movies you like, etc....

- ❖ Oh you thought that was all...

- ❖ What about the videos you have watched, the links you have clicked on, the comments you have left with companies, advertising you connected with and advertising that didn't intrigue you, etc.





# Facebook Beacon

- Fandango, eBay, and 42 other online businesses paid Facebook to do “word of mouth” advertising
- Facebook users surprised to learn information about their purchases was shared with friends
- Beacon was based on an opt-out policy
- Beacon strongly criticized by various groups
- Facebook switched to an opt-in policy regarding Beacon

# Instagram's Proposed Change to Terms of Service

- Late 2012: Instagram announced changes
  - Privacy policy
  - Terms of service
- Legal experts: Instagram and Facebook would have right to use photos in ads without permission
- Instagram CEO: New policy misunderstood
- Changed advertising section of terms of service agreement back to original version

# Class Exercise II

As a social media designer, what additional elements would you incorporate on Facebook so that people are more aware of their privacy settings? (People often complain about Facebook changing privacy related setting too often)

## Class Exercise III

Twitter is inherently a public social platform, so is Reddit. Does this mean these platforms pose less of a privacy threat to individuals compared to Facebook? Justify your answer.

But it is not just the third party bad actors;  
what happens when the risk of privacy lies in  
the hands of the service provider  
themselves?

# Class Exercise IV

In the aftermath of the controversial Facebook contagion study, how do you think people's privacy perceptions may have changed? Or did they at all?

# Facebook created an AI tool that can prevent suicide, but won't talk about how it works

[Share on Facebook](#)[Share on Twitter](#)

# Class Debate

Social media monitoring and health insurance



# Google's Personalized Search

- Secondary use: Information collected for one purpose use for another purpose
- Google keeps track of your search queries and Web pages you have visited
  - It uses this information to infer your interests and determine which pages to return
  - Example: “bass” could refer to fishing or music
- Also used by retailers for direct marketing

# Collaborative Filtering

- Form of data mining
- Analyze information about preferences of large number of people to predict what one person may prefer
  - Explicit method: people rank preferences
  - Implicit method: keep track of purchases
- Used by online retailers and movie sites

# Social Network Analysis

- Data mining now incorporating information collected from social networks
- Examples
  - Cell phone companies in India identify “influencers” – provide discounts
  - Police predict locations of big parties
  - Banks evaluate the riskiness of loans

# Class Exercise V

Secondary information use of social media data and privacy