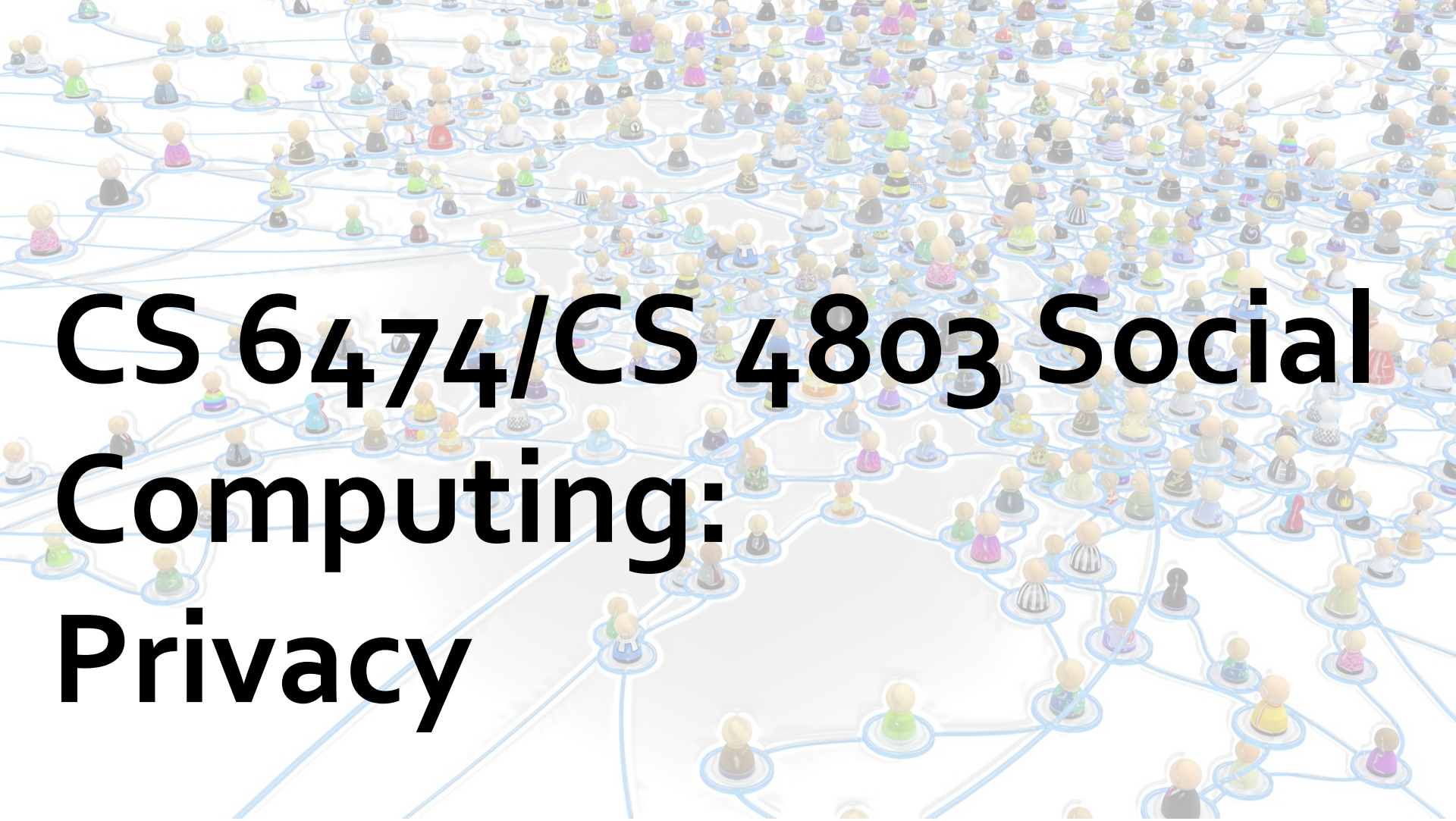


CS 6474/CS 4803 Social Computing: Privacy

Munmun De Choudhury

munmund@gatech.edu

Week 15 | April 17, 2023

Social Computing Systems Erode Privacy

- Information collection, exchange, combination, and distribution easier than ever means less privacy
- Scott McNealy (Sun Microsystems) in 1999: “You have zero privacy anyway. Get over it.”
- Zuckerberg in 2010 said that the social norm is to share everything, so people are little concerned about their privacy.

Perspectives on Privacy

An Old Definition of Privacy

- Privacy rights have evolved from property rights: "a man's home is his castle"; no one should be allowed in without permission
  - Privacy: "right to be left alone"
- Samuel Warren (Harvard graduate businessman) and Louis Brandeis (Boston attorney; later Supreme Court justice)
  - Influential paper from 1890
- This led to 3rd Amendment to U.S. Constitution – principle of home as a sanctuary in the Bill of Rights:
- No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

Is There a Natural Right to Privacy?

- Judith Jarvis Thomson: the definition of privacy as "the right to be left alone" is problematic
  - Smith being monitored at his home with a video camera without his knowledge – he is left alone technically, but it is a privacy violation
- Judith Jarvis Thomson: "Privacy rights" overlap other rights; violation of privacy is often a violation of some other right in this cluster
- *Conclusion: Privacy is not a natural right, but it is a prudential right*

Modern Definition of Privacy

- Privacy is a “zone of inaccessibility”

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?

Legal-ease

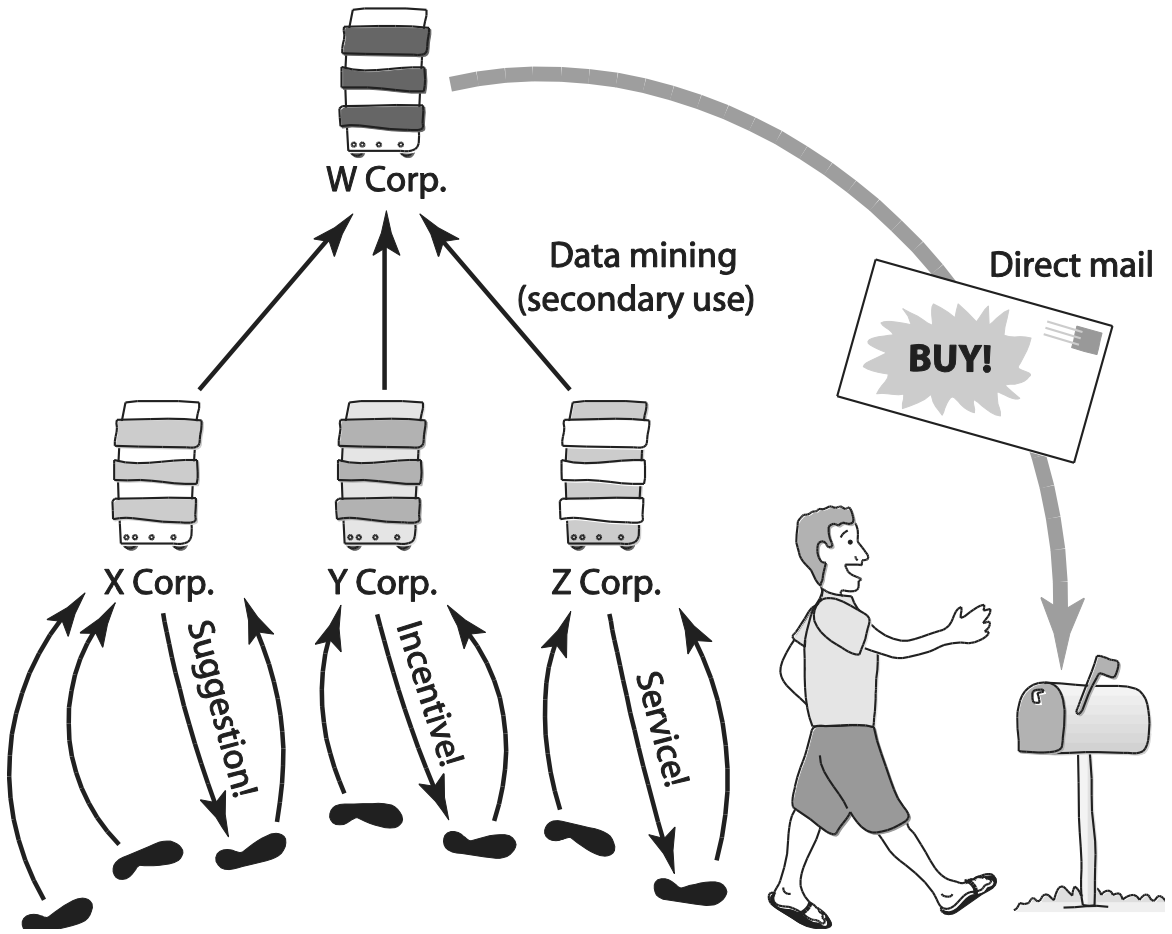
- Legally, read all platforms terms of service (TOS) for the nitty gritty, social media platforms can share some of your basic information.
- But why?
  - Social networks that provide their services without user fees make a profit by selling advertising. This is often done through behavioral advertising, 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.

Facebook Tags

Secondary Uses of Information



How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

What's at Stake: Characterizing Risk Perceptions of Emerging Technologies

Michael Skirpan
University of Colorado
Boulder, CO
michael.skirpan@colorado.edu

Tom Yeh
University of Colorado
Boulder, CO
tom.yeh@colorado.edu

Casey Fielser
University of Colorado
Boulder, CO
casey.fiesler@colorado.edu

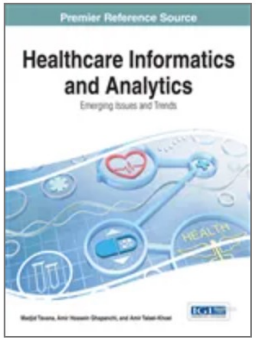
ABSTRACT
One contributing factor to how people choose to use technology is their perceptions of associated risk. In order to explore this influence, we adapted a survey instrument from risk perception literature to assess mental models of users and technologists around risks of emerging, data-driven technologies (e.g., identity theft, personalized filter bubbles). We surveyed 175 individuals for comparative and individual assessments of risk, including characterizations using psychological factors. We report our observations around group differences (e.g., expert versus non-expert) in how people assess risk, and what factors may structure their conceptions of technological harm. Our findings suggest that technologists see these risks as posing a bigger threat to society than do non-experts. Moreover, across groups, participants did not see technological risks as voluntarily assumed. Differences in how people characterize risk have implications for the future of design, decision-making, and public communications, which we discuss through a lens we call risk-sensitive design.

ACM Classification Keywords
H.1.2 User/Machine Systems: Human Factors; H.5.m. Information Interfaces and Presentation (e.g. HCI): Miscellaneous

and behavior-driven design. These users must rely on the companies and parties to whom they have given their data (knowingly or not) to be ethical.

Yet, we already know that many impacts (e.g., privacy, ethical, legal) and constraints (e.g., protocols, technological capabilities) of online technologies are poorly understood by users [24, 8, 36, 15]. We also know that, when asked, users are often uncomfortable or find undesirable the practices of online behavioral advertising (OBA) and personalization [37, 34]. This misalignment is often framed as a consumer trade-off between privacy and personal benefit [13, 40]. Framing it this way leads to an assumption that the benefit of web services must outweigh consumer's privacy concerns since users are not opting out of services.

However, if consumers really are performing this cost-benefit analysis and making a conscious decision, then why we do we see such hype and panic around risks and harms caused by technology in the media? Daily news headlines relay injustice [19, 1, 4, 33], personal boundary violations [32], and gloom [26, 18, 14] over the impacts of technology on society. Some of these problems may indeed warrant concern from the public and social advocates; others might be overblown



Privacy Perceptions of Older Adults when Using Social Media Technologies

Dan Dumbrell (The University of Sydney, Australia) and Robert Steele (The University of Sydney, Australia)

Source Title: Healthcare Informatics and Analytics: Emerging Issues and Trends
 | Pages: 16

ISBN13: 9781466663169 | ISBN10: 1466663162 | EISBN13: 9781466663176

DOI: 10.4018/978-1-4666-6316-9.ch004

Abstract

Social media technologies represent an emerging means by which older adults can access health and community information, engage in peer-to-peer information sharing, and also potentially decrease social isolation. Privacy concerns, however, have been consistently identified as a barrier for older adults' use of the Web and social media technologies. The authors conduct a preliminary study involving 150 older adult participants, investigating their use and perceptions of social media technologies. The trial involved first providing the participants with brief training in three common social media technologies: Facebook, Twitter, and Skype. The authors carried out a quantitative and qualitative analysis of the participant's use and privacy perceptions of these technologies. Overall, the results are promising as to the potential to address privacy concerns to enable older adults to further utilize these technologies for improved mental, physical, and social health. Implications for future research and usage within the older adult community are also discussed.

Managing Disclosure through Social Media: How Snapchat is Shaking Boundaries of Privacy Perceptions

Justin C. Velten, Rauf Arif, & Delane Moehring

Abstract

The rise of online human communication tools commonly referred to as social media apps are changing the dynam-

Data, Privacy, and the Greater Good

Privacy Safeguards

Institutional Review Boards

- Formal review procedures for institutional human subject studies were originally developed in direct response to research abuses in the 20th century, such as Milgram's obedience study or Tuskegee Syphilis experiment.

Federal Policy for the Protection of Human Subjects ('Common Rule')

The current U.S. system of protection for human research subjects is heavily influenced by the Belmont Report, written in 1979 by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont Report outlines the basic ethical principles in research involving human subjects. In 1981, with this report as foundational background, HHS and the Food and Drug Administration revised, and made as compatible as possible under their respective statutory authorities, their existing human subjects regulations.

The Federal Policy for the Protection of Human Subjects or the "Common Rule" was published in 1991 and codified in separate regulations by 15 Federal departments and agencies, as listed below. The HHS regulations, 45 CFR part 46, include four subparts: subpart A, also known as the Federal Policy or the "Common Rule"; subpart B, additional protections for pregnant women, human fetuses, and neonates; subpart C, additional protections for prisoners; and subpart D, additional protections for children. Each agency includes in its chapter of the Code of Federal Regulations [CFR] section numbers and language that are identical to those of the HHS codification at 45 CFR part 46, subpart A.

Adapting IRB review to Internet era and big data research

POLICY —

"Anonymized" data really isn't—and here's why not

Companies continue to store and sometimes release vast databases of " ...

NATE ANDERSON - 9/8/2009, 7:25 AM

41

The Massachusetts Group Insurance Commission had a bright idea back in the mid-1990s—it decided to release "anonymized" data on state employees that showed every single hospital visit. The goal was to help researchers, and the state spent time removing all obvious identifiers such as name, address, and Social Security number. But a graduate student in computer science saw a chance to make a point about the limits of anonymization.

Latanya Sweeney requested a copy of the data and went to work on her "reidentification" quest. It didn't prove difficult. Law professor Paul Ohm describes Sweeney's work:

> At the time GIC released the data, William Weld, then Governor of Massachusetts, assured the public that GIC had protected patient privacy by deleting identifiers. In

Beyond the Belmont principles: Ethical challenges, practices, and beliefs in the online data research community

Code	Definition	Example Statements
Public Data	Only using public data / public data being okay to collect and analyze	*In general, I feel that what is posted online is a matter of public record, though every case needs to be looked at individually in order to evaluate the ethical risks.*
Do No Harm	Comments related to Golden Rule	*Golden rule, do to others what you'd have them do to you.*
Informed Consent	Always get informed consent / stressing importance of informed consent	*I think at this point for any new study I started using online data, I would try to get informed consent when collecting identifiable information (e.g. usernames).*
Greater Good	Data collection should have a social benefit	*The work I do should address larger social challenges, and not just offer incremental improvements for companies to deploy.*
Established Guidelines	Including Belmont Report, IRBs Terms of Service, legal frameworks, community norms	*I generally follow the ethical guidelines for human subjects research as reflected in the Belmont Report and codified in 45.CFR.46 when collecting online data.*
Risks vs. Benefits	Discussion of weighing potential harms and benefits or gains	*I think I focus on potential harm, and all the ethical procedures I put in place work towards minimizing potential harm.*
Protect Participants	data aggregation, deleting PII, anonymizing / obfuscating data	*I aggregate unique cases into larger categories rather than removing them from the data set.*
Data Judgments	Efforts to not make inferences or judge participants or data	*Do not expose users to the outside world by inferring features that they have not personally disclosed.*
Transparency	Contact with participants or methods of informing participants about research	*I prefer to engage individual participants in the data collection process, and to provide them with explicit information about data collection practices.*

Item	M	SD
...notify participants about why they're collecting online data[1]	3.89	0.96
...share research results with research subjects[1]	3.90	0.80
...Ask colleagues about their research ethics practices[1]	4.27	0.74
...Ask their IRB/internal reviews for advice about research ethics[1]	4.03	0.90
...Think about possible edge cases/outliers when designing studies[1]	4.33	0.71
...Only collect online data when the benefits outweigh the potential harms[1]	3.62	1.10
...Remove individuals from datasets upon their request[1]	4.56	0.71
Researchers should be held to a higher ethical standard than others who use online data[2]	3.46	1.22
I think about ethics a lot when I'm designing a new research project[2]	3.96	0.93
Full Scale (α=.71)	4.00	0.49

[1] Prompt: "I think researchers should...."
[2] Prompt: "To what extent do you agree with the following statements?"
Both sets of items were measured on five point, Likert-type scales (Strongly Agree-Strongly Disagree).

Codification of Ethical Attitudes Measure

Ethics Heuristics for Online Data Research: Beyond the Belmont Report

1. Focus on transparency
   - Openness about data collection
   - Sharing results with community leaders or research subjects
2. Data minimization
   - Collecting only what you need to answer an RQ
   - Letting individuals opt out
   - Sharing data at aggregate levels

3. Increased caution in sharing results
4. Respect the norms of the contexts in which online data was generated.

Beyond researchers, what happens when the risk of privacy lies in the hands of the service provider themselves?

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

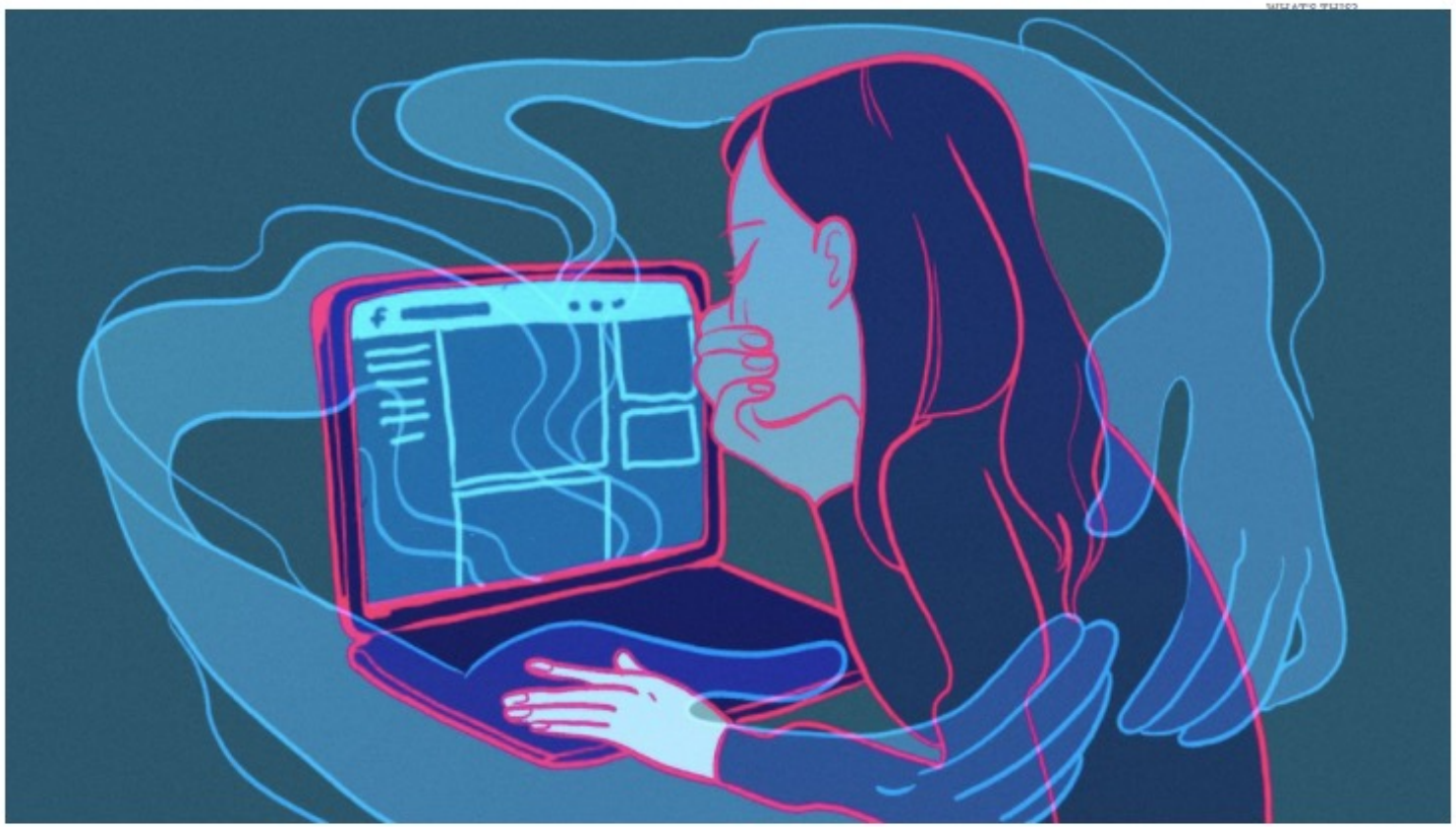


IMAGE: VICKY LETA / MASHABLE

TECHNOLOGY

Suicide hotline shares data with for-profit spinoff, raising ethical questions

The Crisis Text Line's AI-driven chat service has gathered troves of data from its conversations with people suffering life's toughest situations.

Politico Illustration

Class Exercise I: Social media monitoring and health insurance

While the cost of automobile insurance varies from person to person based on the driving record of each individual, health insurance premiums are typically uniform across groups of people, such as all the employees of a company. However, a majority of healthcare costs are incurred by a minority of the population.

Today it is possible to look at somebody's social media, understand their emotional state, even create a "profile" that reveals the person's disposition to certain mental disorders. Debate the proposition that health insurance rates should be tailored to reflect each individual's propensity to mental illness – it is a good or a bad idea?

Beyond researchers, what happens when the government or other similar authorities start to make use of people's online data?

PRIVACY AND SECURITY

China's Social Ranking System Is Getting Closer to Becoming a Terrifying Reality

Catie Keck

Thursday 5:00pm • Filed to: SOCIAL CREDIT

47.8K 62 3

The lifelong social ranking system is set to be adopted in Beijing in 2021, Bloomberg reported Tuesday, with residents to be judged on data based on their social standing by the end of 2020. The program would essentially mark any individuals found to have violated laws or social codes and restrict their access to services like travel or certain programs.

Class Exercise II: Government use of social media data for surveillance.

Somewhat similar to the Chinese government's social surveillance system, enhanced 911 service in the US allows cell phone companies to track the locations of active cell phone users within 100 meters. In a future work, they can also use people's social media activities, including their geolocation, where they go, what they do, how they feel, and who they interact with.

1. Who should have access to such sensitive social media data collected by social media companies?
2. How long should this information be kept?
3. How would you feel about the company releasing comprising information about your whereabouts to the police?
4. Should the police be able to get from the company the names of all users using their service/platform who may be in some way related to/close to a crime scene around the time of the crime?

Takeaways