DSci529: Security and Privacy In Informatics

Social Media

Prof. Clifford Neuman

Lecture 9
19 March 2021
Online

Course Outline

- Overview of Security and Privacy
- What data is out there and how is it used
- Technical means of protection
- Identification, Authentication, Audit
- Reasonable expectation of privacy
- Big Data – Technology and Privacy
- AI and Bias
- The Internet of Things and Security and Privacy
- **Social Networks and the use of our Data**
- Access to Data by Governments - Privacy in a Pandemic
- Privacy Regulation - GDPR, CCPA, CPRA
- Influence of Social Media – Free Speech – Disinformation
- CryptoCurrency - TOR - Privacy Preserving Technologies

Today's Agenda

- 12:00 – 12:05 Introduction and Announcements
- 12:05 – 13:55 Student Presentations – Social Media
  - 10 minutes for each presentation
- 13:50 – 14:00 Break
- 14:00 – 14:30 Class Discussion on Social Networks
- 14:30 – 14:55 Class Discussion of Mid-Term exam
- 14:55 – 15:20 Current Event Discussion

Upcomming Presentations Pandemic/Govt Data Use – March 26th

Pandemic (40 minutes)

- Yuemeng Gao
- Tanmay Ghai – Privacy Preserving Contact Tracing
- Yi Lin – Big Data in China related to the COVID Pandemic
- Gan Xin – Health QR Code in China

Other government use of data (50 min)

- Yi Jin – How US and China collect and use personal data
- Congrui Li
- Michelle Muldoon – Law Enforcement and Privacy w.r.t. Data Brokers
- Griffin Weinhold – Decentralized Search and Search Histories in Court
- Xihao Zhou – Use of Data by Governments
- Jinglun Chen – Use of location data
- Jiemin Tang – Security and Privacy regulation for food delivery services

Upcoming Presentations
Privacy&Security Regulation – April 2nd

- Jia Yu Lee
- Yansong Wang
- Kaifan Lu – Assessing China's Cybersecurity Law

- 30 minutes for this group to present

Upcoming Presentations Healthcare – April 2nd

- Vartan Batmazyan
- Phuong Ngo
- Sharad Sharma (DNA Databases)
- Ye Zheng - Fitness apps

- This group will have 40 minutes to present.

Upcoming Presentations – April 9th Free Expression - Disinformation

- Adriana Nana – Deep Fakes and Privacy
- Resherle Verna – Should Social Media company's have right of censorship

  – This group will have 20 minutes to present.

Upcoming Presentations Privacy and Finance – April 16th

- Jonathan De Leon – Privacy in Finance
- Sidong Wang – History and Technologies for Cryptocurrencies
- Saurabh Jain – Privacy of Credit Card/Payment card information
- Yifeng Shi -Financial value of data gathered through free services

- 40 minutes

Secure Communication – Privacy Preserving Technologies – April 16th

- Zihuan Ran – Privacy Preserving Database Technologies
- Aziza Saulebay – 5G and Data Privacy
- Carol Varkey – Messaging Application Privacy
- Francisco Ventura – Encryption Technologies and implications

- 40 minutes

Upcoming Presentations
Other Security Topics – April 23rd

- Yo-Shuan Liu – User experience and Multi-Factor Authentication
- Philana Williams – Security for Web App Development
- Haonan Xu – Privacy issues in Cloud Computing
- Pratishtha Singh – Card privacy Concerns in India

DSci529: Security and Privacy In Informatics

Social Media

Student Presentations

Lecture 9
19 March 2021
Online

Upcoming Presentations
Social Media – March 19th

- Addison Allred
- Yixiang Cao
- Lei Gao
- Mingliao Xu
- Shengwang Zhang
- Zixin Zheng
- Hehan Xie
- Chengyuan Zhou
- Hehan Xie
- Brianna Hefferin

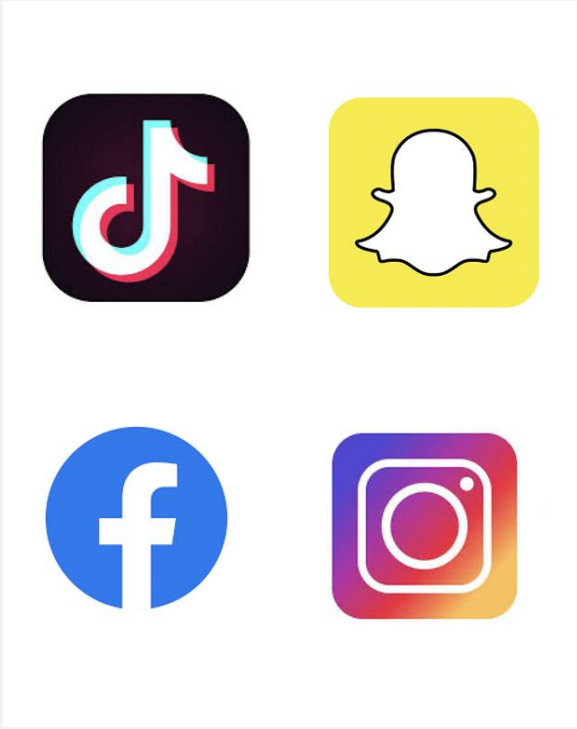
PRIVACY AND SECURITY IN SOCIAL MEDIA

Addison Allred

DSCI 529 – Security and Privacy in Informatics

SOCIAL MEDIA INTRODUCTION

- Social Media refers to websites and applications that allow individuals to share content and interact with other users
- Facebook is the most widely used social media platform, with 2.8 billion monthly active users
- 79% of Americans use a social media platform
- The average American spends 2 hours and 3 minutes on social media every day
- One of the top 4 forms of communications for those between ages of 18-29



DATA PRIVACY CONCERNS

- Biggest privacy issues users face when using social media platforms is their data being collected
- Platforms collect every action you have executed on their platform: messages you have sent, post you have liked, users you follow, ads you have interacted with, etc.
- Data mined by social media platforms is then utilized by the company to provide insights for improvements they can make, common trends in user activity, and most importantly for ads
- Social media companies have sold users personal data to 3rd parties
- When users sign up for a social media platform, they are required to sign a terms and agreement document, this provides consent for the company to collect user's data legally

SECURITY IN SOCIAL MEDIA

Facebook

- VPN protection
- Encrypted email with OpenPGP

Twitter

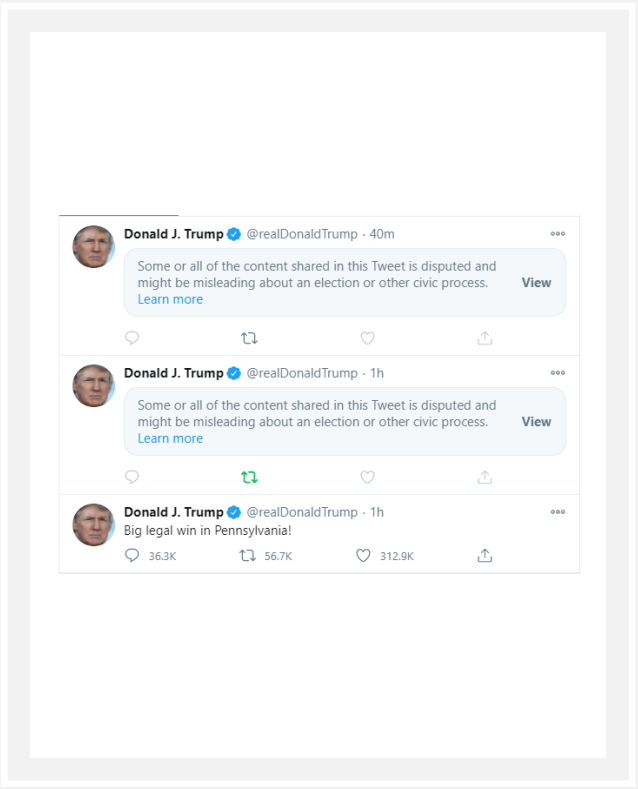
- Removal of Bots
- Email encryption

LinkedIn

- Three level security for cloud services
- Identifying fake accounts by comparing names grouped in clusters

CENSORSHIP

- Over the past couple of years, the role of censorship within a social media platform has become a central focus of social media companies
- Social media platforms must ensure that the content that is being uploaded is appropriate and will not cause harm upon others
- Fact checking has become one of the main focuses of censorship on twitter to ensure that a misleading post isn't incorrectly interpreted by others
- New social media sites, such as Parler, have emerged since individuals no longer want be censored for what they want to say
- This has brought into the question the freedom of speech, and the way in which social media companies should respect this right all the while protecting their users from harmful and insensitive content



A INSIDE LOOK

- No Facebook employee can access any data without requesting access to the data set
- Data is utilized for identifying improvements to make within the platform, promote the right ads to users, and identifying gaps to develop new tools and features
- All data is encrypted, preventing employees from being able to identify who the data is associated with
- Data stored throughout various data centers owned by Facebook

CONCLUSION

- Social media is a daily part of the majority of everyone's life
- It is very important that as users, we become more aware of the privacy that we are giving up when utilizing social media platforms
- Censorship on social media platforms is very complex as it infringes upon freedom of speech while also providing protection from those who post harmful content

REFERENCES

- https://www.thebalancesmb.com/what-is-social-media-2890301
- https://www.statista.com/statistics/346167/facebook-global-dau/#:~:text=With%20roughly%202.8%20billion%20monthly,most%20popular%20social%20network%20worldwide.
- https://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/#:~:text=This%20equals%20approximately%20247%20million%20U.S.%20social%20media%20users%20as%20of%202019.&text=According%20to%20estimates%2C%20the%20number,3.5%20billion%20in%20April%202019.
- https://news.gallup.com/poll/179288/new-era-communication-americans.aspx#:~:text=Texting%20is%20the%20most%20frequently,those%20aged%2065%20and%20older.
- https://www.digitalmarketing.org/blog/how-much-time-does-the-average-person-spend-on-social-media
- https://law.yale.edu/mfia/case-disclosed/social-media-mining-effects-big-data-age-social-media#:~:text=Social%20media%20mining%20is%20%E2%80%9Cthe,about%20the%20populations%20of%20these
- https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html
- https://www.business2community.com/cybersecurity/7-social-media-security-issues-business-faces-02024378
- https://www.varonis.com/blog/social-media-security/
- https://www.bbc.com/news/technology-54698186
- https://www.forbes.com/sites/petersuciu/2021/01/11/do-social-media-companies-have-the-right-to-silence-the-masses--and-is-this-censoring-the-government/?sh=352221ae48e2

PRIVACY & SOCIAL MEDIA

Recommender System and privacy

Yixiang Cao

The development of social media

- The development of technology
  - Artificial Intelligence Algorithm
  - Data mining

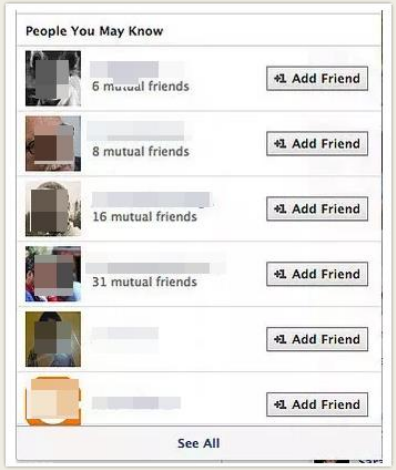
- Improve the competitiveness of enterprise products
  - Improve user experience
  - Provide more functions

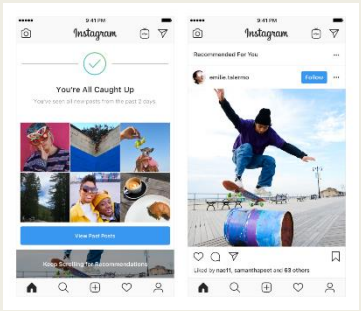
- The product pursues a more diversified profit mode
  - Embed ads in social media software

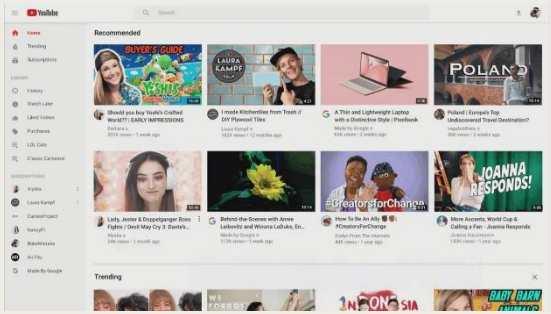
Recommendation System

Recommender System

- Recommended features provided by the product for users







  - 75% of Netflix viewing decisions are from product recommendations.
  - Almost all the video content that users see on tictok is based on user recommendations
- Use the recommendation system to show ads to target customers

Recommender System

- Aim to provide accurate recommendations for users by collecting and processing their personal data using effective approaches [7].

Recommender System

- Recommendation systems can be classified into two categories: CFB recommendation systems and CB recommendation systems.
  - CFB recommend items based on the similarity between users.
  - CB conduct recommendation based on the properties of items

- CFB recommendation systems usually adopt either neighborhood-based approaches or machine learning-based approaches.
  - Neighborhood-based approaches directly compute the similarity relationship between users
  - Machine learning-based approaches first learn a mathematical model from the collected user data,

Privacy Concern: Personal Data Collection

- Personalized recommendations typically require the collection of personal data for analysis
  - Users' identity, demographic profile, behavioral data, purchase history, rating history…
  - The more personal data a recommender collects, the more accurate recommendations users can obtain.

- Who will obtain the obtained private data?
  - Platform data analysis, model construction
  - Advertisers
  - Maliciously leaked
  - Obtained by outside attack

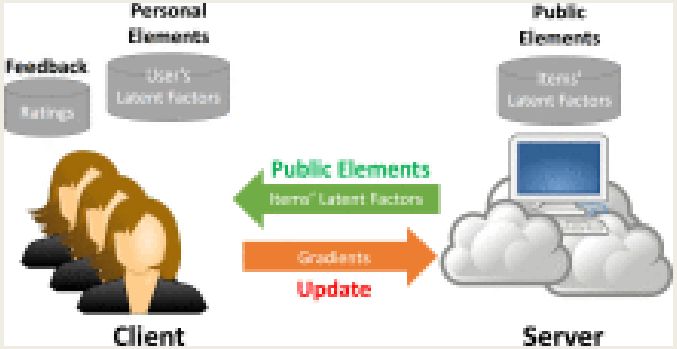
Privacy-preserving CFB recommendation

- Private neighborhood-based approaches
  - Cryptographic techniques： homomorphic encryption (PHE) , (SMC) protocols.
  - Randomization techniques

- Comparison
  - Cryptographic technique-based solutions generally require high computation overhead: not be well-suited for large-scale data.
  - Cryptographic provide strong protection for user data under semantic security while ensuring recommendation accuracy.
  - Randomization has low computation overhead and is much faster than cryptographic technique-based solutions.

Privacy-preserving CFB recommendation

- Private machine learning-based approaches
  - First train a machine learning model over collected user data in a privacy-preserving manner
  - Apply the model to generate personalized recommendations.
  - matrix factorization (MF) and ridge regression (RR),
  - cryptographic techniques that include PHE, fully homomorphic encryption (FHE), and GCs.



Privacy-preserving CB recommendation

- Private targeted advertising
  - Achieve targeted ad delivery and protect user's personal information.
  - local targeting, game theory, anonymization, cryptographic techniques, and obfuscation
- Local targeting (example)
  - Pre-fetches a list of ads and stores them locally before the user visits publishers' pages.
  - Downloading all the non-pre-fetched listed ads, so as to avoid information leakage to the ad network.

personal opinion

- As a customer
  - Understand what you really need in the convenient balance between privacy and recommendation
  - Express your thoughts and opinions bravely on occasions
- As a social media company
  - Improve technological level to protect the privacy of users while ensuring the quality of recommendations
  - Give more choices to your consumers, and make consumer authorization the basis of everything

THANK YOU

Privacy concern on social media platform

Lei Gao

$ocial media

1

169.76 million monthly users

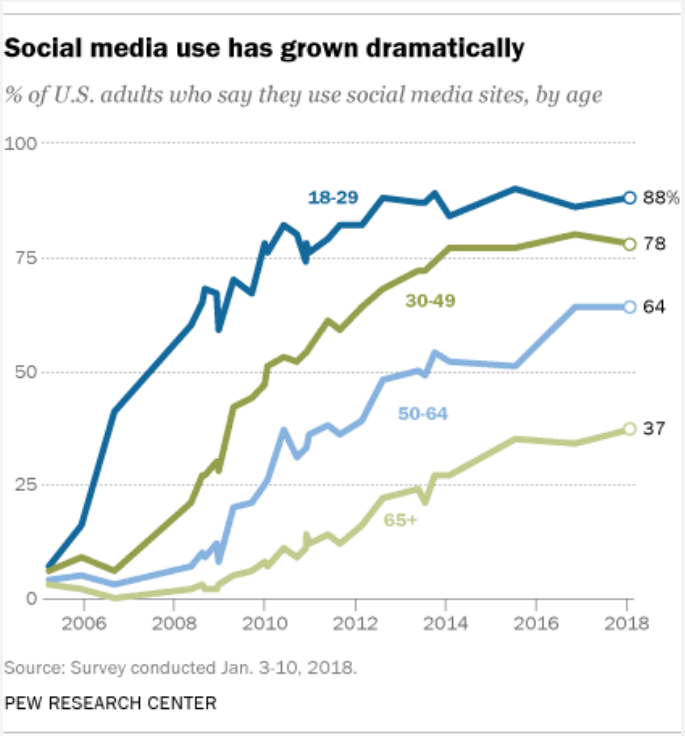
2

121.23 million monthly users

3

81.47 million monthly users

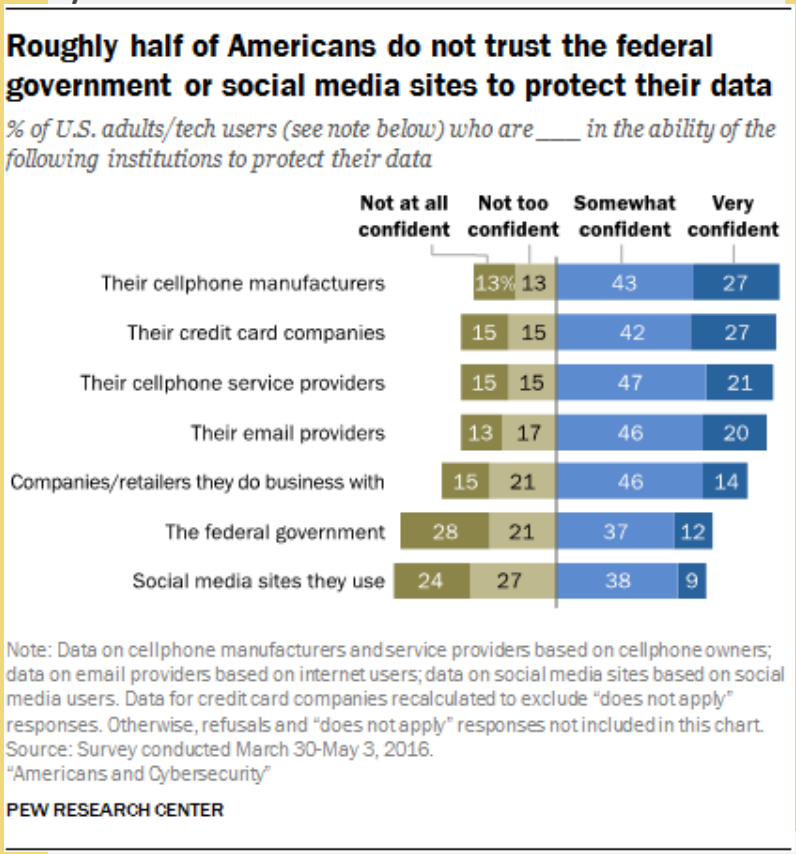
Growth of social media



Source: Pew Research Center

- 69% of American use some kind of social media
- Poll found that people use social media for important social interactions
- Social media is particularly important for teenagers

Privacy concern



Source: Pew Research Center

- People are least confident in social media sites
- Only 9% of respondents are very confident in social media sites

Potential threats

- Ads
- Location tracking
- 3rd party PII
- Identify theft
- Data breaches
- Social engineering
- Phishing
- Malware attack

Data mining and Ads

Data mining tools collect users data without them knowing

Personalized Ads are suggested accordingly

Case study: Cambridge Analytica

Facebook sued over Cambridge Analytica data scandal

By Cristina Criddle
Technology reporter

28 October 2020 | Technology

Facebook is being sued for failing to protect users' personal data in the Cambridge Analytica breach.

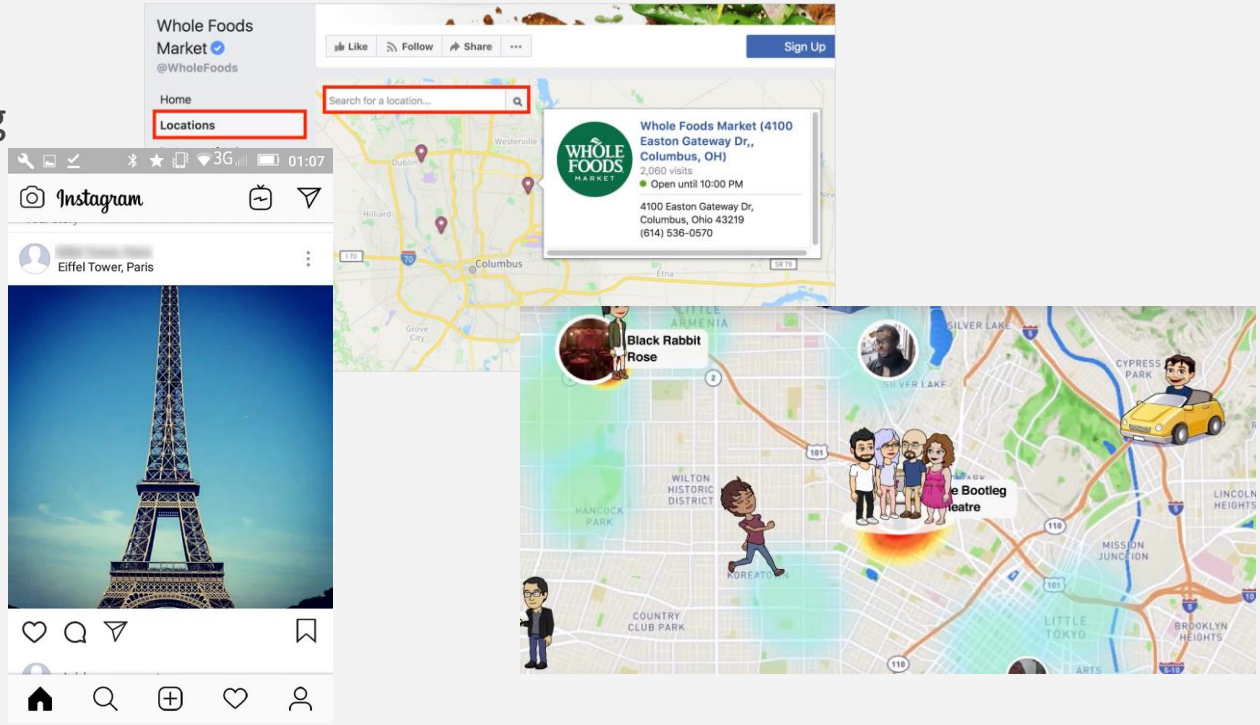
The scandal involved harvested Facebook data of 87 million people being used for advertising during elections.

Mass legal action is being launched against Facebook for misuse of information from almost one million users in England and Wales.

Facebook said it has not received any documents

The company harvested data over 87 million Facebook users in illegal manner

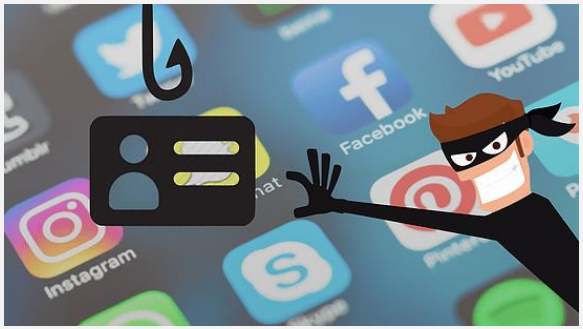
Location tracking



Disclosing location by tagging or allowing apps to access your GPS data cause threats to your privacy

→ Users can easily be tracked

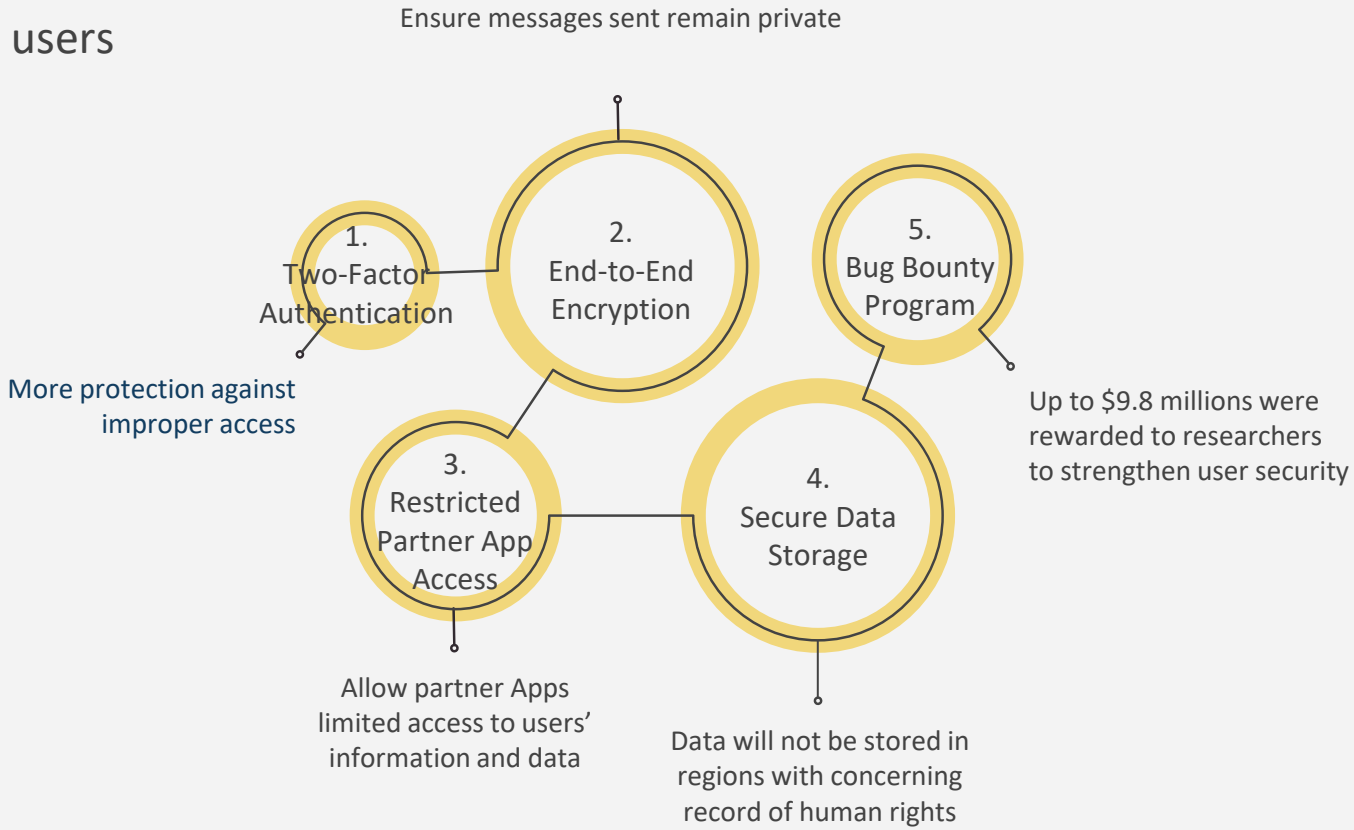
Identity theft



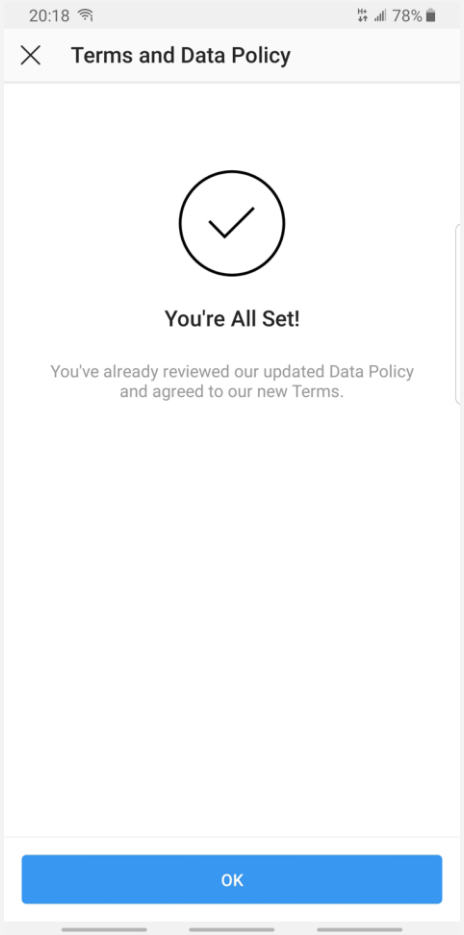
Collect information you post online/ hack into your account through phishing link or data breach

Steal your online identity for potential criminal activities

What has Facebook done to protect users privacy



Instagram



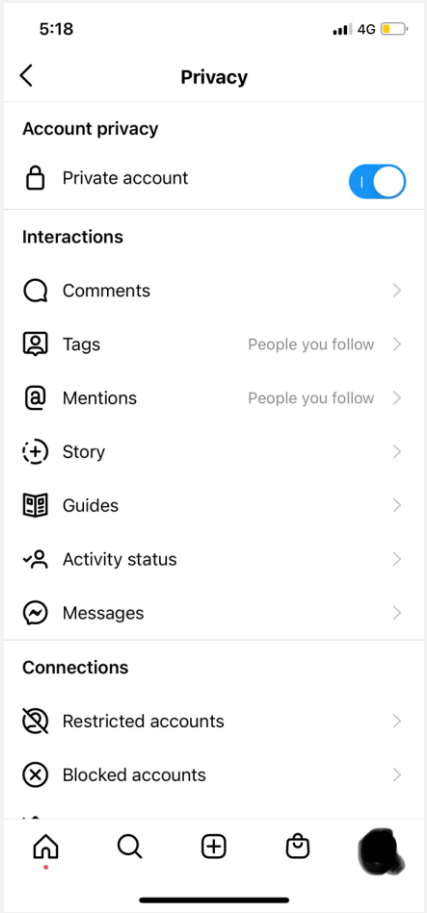
What data is collected by Instagram:

- Names and password
- Captured content
- Data that links users to the photos to took, tagged or liked
- Messages history
- Transactional data from Facebook products & services
- Facial recognition data
- Geolocation data

How are these data used?

- Personalized Ads
- Automatically recognize you when you appear in photos
- Run strategic market research

Instagram



Privacy settings

- Private account
- Remove followers
- Hide story from certain accounts
- Restrict comments
- Restrict direct messages
- Turn off activity status
- Clear search history
- Disallow tag

How to protect your privacy

- Set your account private
- Use two-factor authentication
- Change password regularly
- Choose a strong password
- Do not click on sketchy links
- Do not allow 3rd party app to access your data
- Block or report suspicious account

References

Department, Published by Statista Research, and Feb 4. “Most Popular Social Media Apps in U.S.” *Statista*, 4 Feb. 2021, www.statista.com/statistics/248074/most-popular-us-social-networking-apps-ranked-by-audience/.

Identity Guard, www.identityguard.com/news/what-you-need-to-know-about-instagrams-privacy-policy.

“Instagram Help Center.” *Data Policy | Instagram Help Center*, help.instagram.com/519522125107875.

“Protecting Privacy and Security.” *About Facebook*, 16 Sept. 2020, about.fb.com/actions/protecting-privacy-and-security/.

THANK You

Safe, Secure and Social

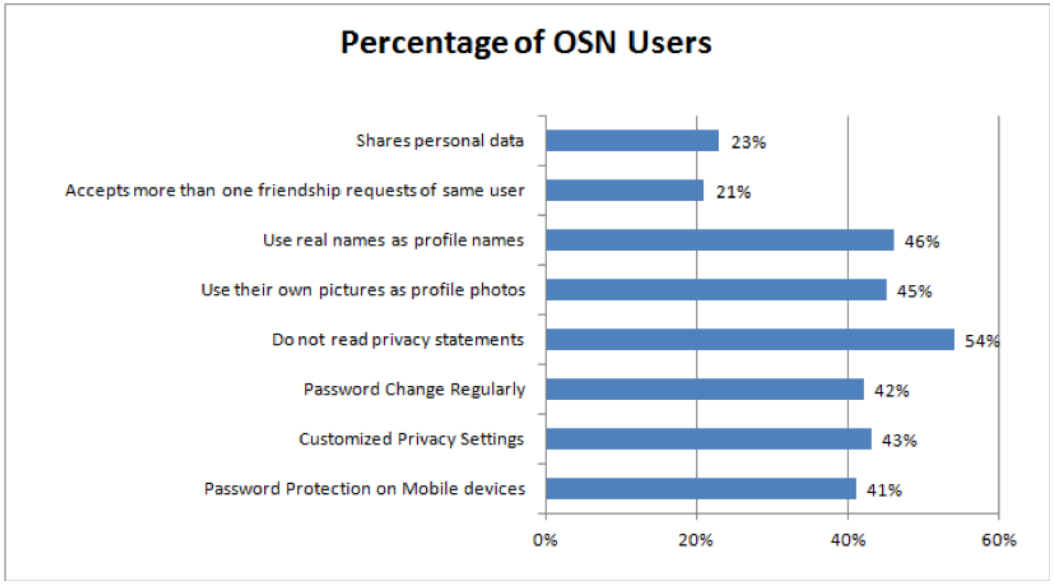
Mingliao Xu

Social Media Definition

- A web site designed to allow several users to publish content freely on any subject for use by ‘friends’ and others.
- Such a site allows users to create a personal ‘profile’ visible to the people they allow.
- First Social Network: Six degrees

What are you sharing?

- Your Profile
- Your Status
- Your Location
- Shared Content

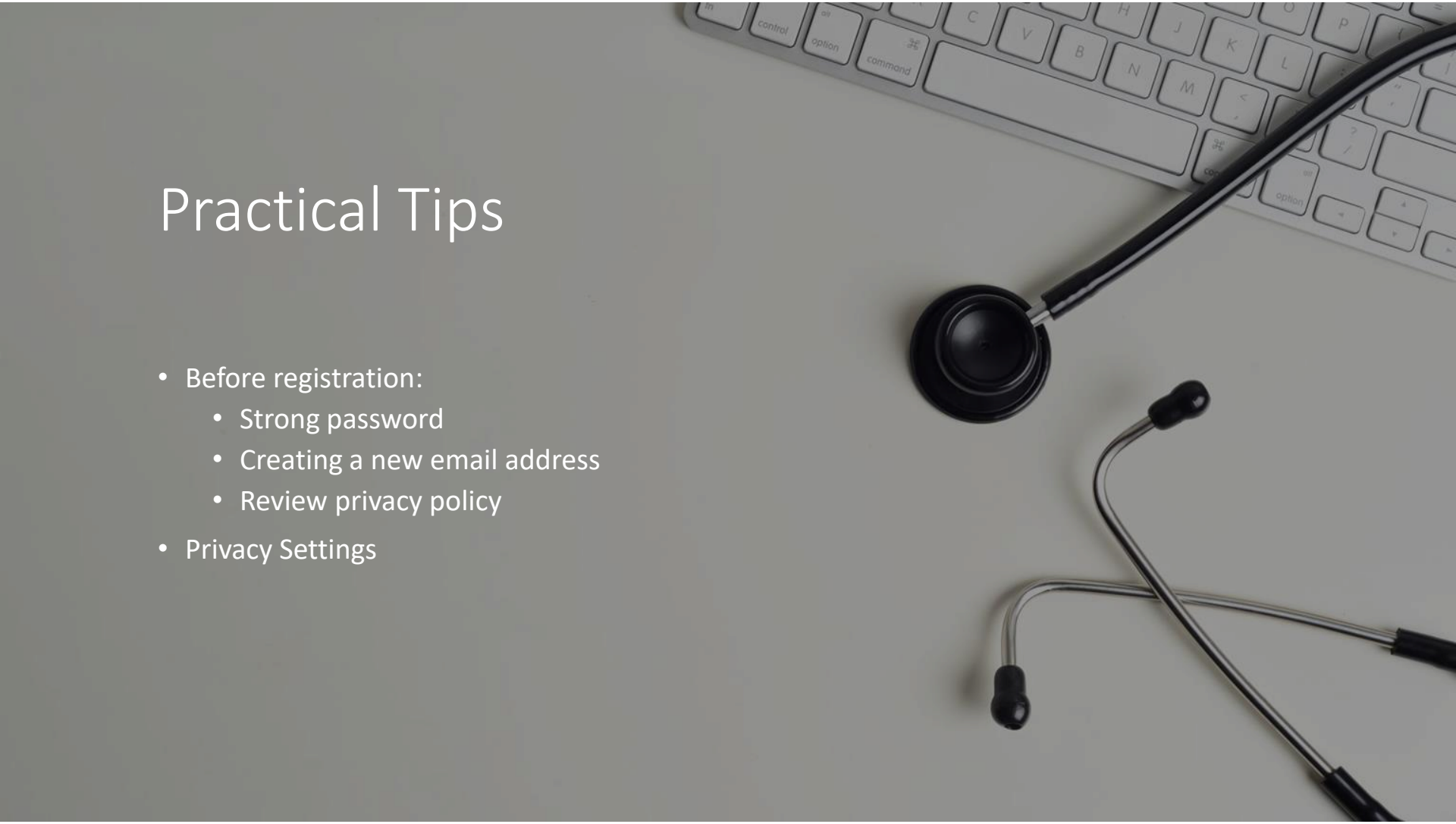


https://doi.org/10.3390/fi10120114

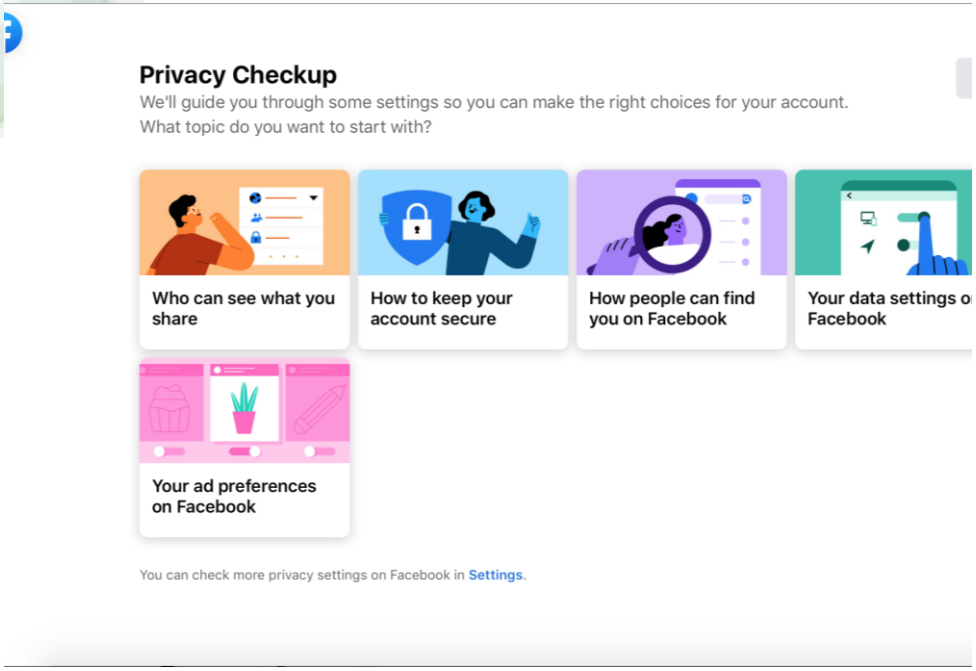
Possible Attacks

Malware	Phishing Attacks	Spam Attacks	Cross-Site Scripting
Clickjacking	De-anonymization Attacks	Fake Profiles	Identity Clone Attacks
Inference Attacks	Information Leakage	Location Leakage	Cyberstalking

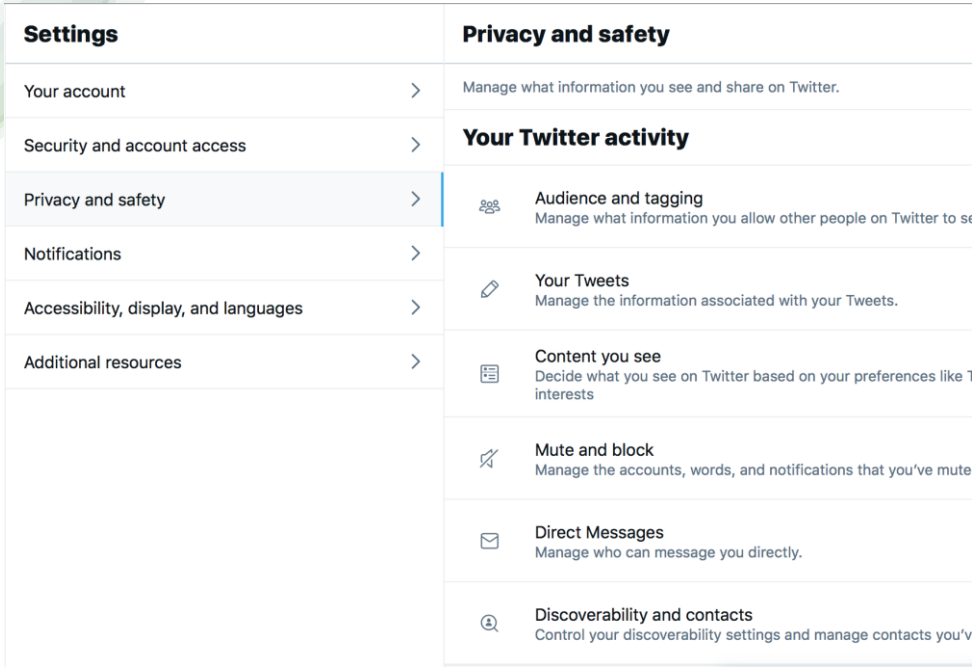
Practical Tips



- Before registration:
  - Strong password
  - Creating a new email address
  - Review privacy policy
- Privacy Settings



Facebook Privacy Checkup



Twitter Privacy and Safety

Citation

- Ali, S., Islam, N., Rauf, A., Din, I., Guizani, M., & Rodrigues, J. (2018). Privacy and Security Issues in Online Social Networks. *Future Internet*, *10*(12), 114. https://doi.org/10.3390/fi10120114
- Privacy Rights Clearinghouse. (2019, March 25). *Social Networking Privacy: How to be Safe, Secure and Social | Privacy Rights Clearinghouse*. https://privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social

Data Privacy on Social Media

Shengwang Zhang
4297788031

What is Social Media?

Social media is any digital tool that allows users to quickly create and share content with the public. Social media encompasses a wide range of websites and apps. Some, like Twitter, specialize in sharing links and short written messages. Others, like Instagram and TikTok, are built to optimize the sharing of photos and videos.

What makes social media unique is that it is both broad and relatively uncensored. While many social media companies impose some limitations—such as taking down images that display violence or nudity—there are much fewer limitations on what someone can share than there with other means of mass communication like newspapers, radio stations, and television channels.

1

Facebook is a social networking site that makes it easy for you to connect and share with family and friends online. Originally designed for college students, Facebook was created in 2004 by Mark Zuckerberg while he was enrolled at Harvard University. By 2006, anyone over the age of 13 with a valid email address could join Facebook. Today, Facebook is the world's largest social network, with more than 1 billion users worldwide.

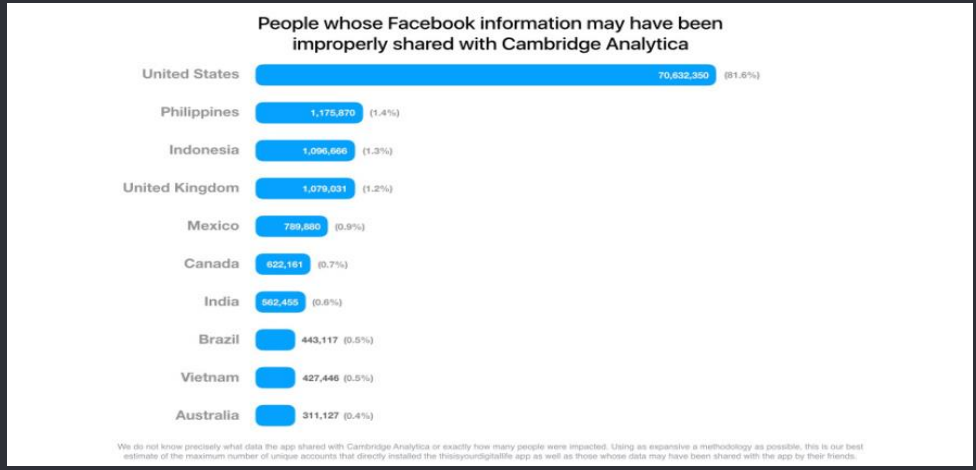
What could Facebook possibly know?

- Anything you provide them, recall it..
  - Name, Date of birth, City of residence, Phone, Email, Relationship, Birthday, Family members, Friends, Favorite movies, etc…
- More than that…
  - The links you have clicked on, the image you just liked, the videos you just watched, the comments you have left with companies, what you have searched before, etc..

Facebook data privacy scandal

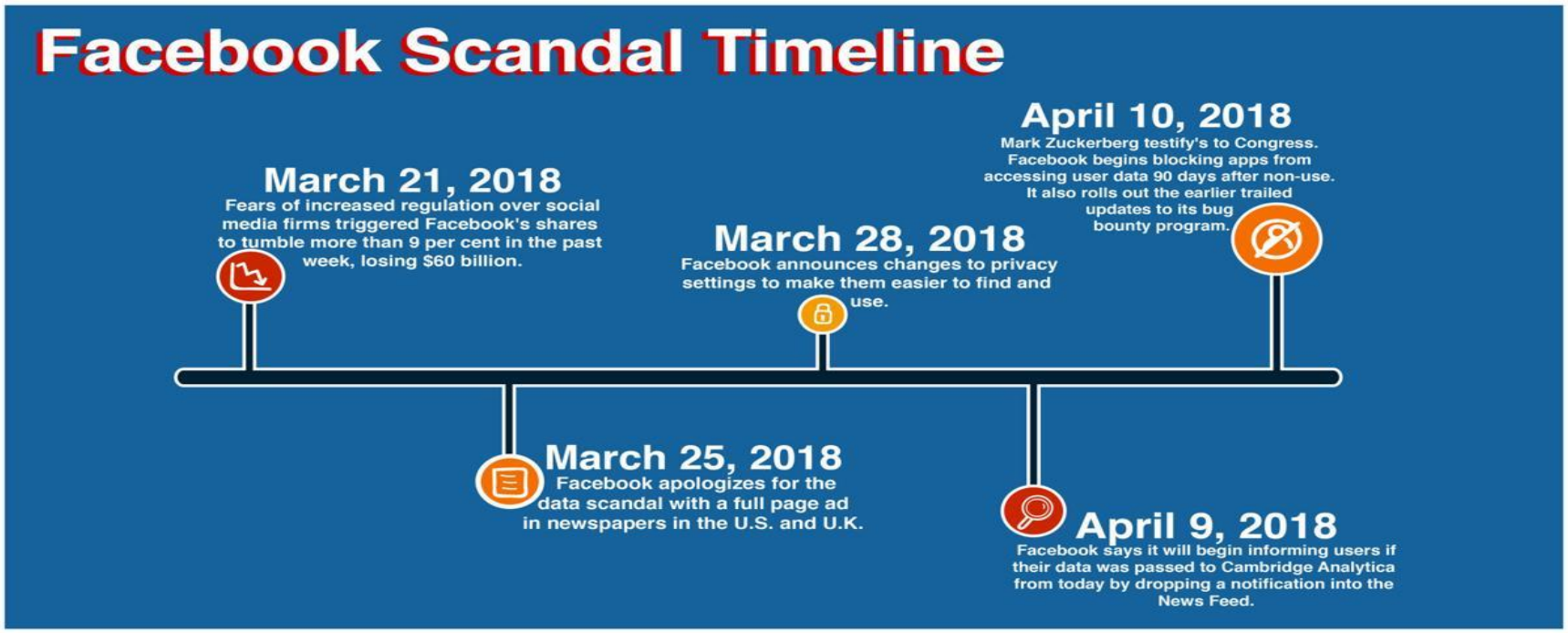
The Facebook data privacy scandal centers around the collection of personally identifiable information of "up to 87 million people" by the political consulting and strategic communication firm Cambridge Analytica. That company--and others--were able to gain access to personal data of Facebook users due to the confluence of a variety of factors, broadly including inadequate safeguards against companies engaging in data harvesting, little to no oversight of developers by Facebook, developer abuse of the Facebook API, and users agreeing to overly broad terms and conditions.

Researchers associated with Cambridge University claimed in a paper that it "can be used to automatically and accurately predict a range of highly sensitive personal attributes including sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender," with a model developed by the researchers that uses a combination of dimensionality reduction and logistic/linear regression to infer this information about users.



Timeline

In 2015, Aleksandr Kogan starts to collect Data through APP under contract from Cambridge Analytics. By accepting the App *Terms and Conditions,* users allowed the collections of data about themselves and their friends. In 2018, Facebook app grow about 300k active users + 87 million friends information and the scandal is revealed.



What are the possible implications for enterprises?

Business users and business accounts should be aware that they are as vulnerable as consumers to data exposure. Because Facebook harvests and shares metadata--including SMS and voice call records--between the company's mobile applications, business users should be aware that their risk profile is the same as a consumer's. The stakes for businesses and employees could be higher, given that incidental or accidental data exposure could expose the company to liability, IP theft, extortion attempts, and cybercriminals.

Though deleting or deactivating Facebook applications won't prevent the company from creating so-called advertising "shadow profiles," it will prevent the company from capturing geolocation and other sensitive data. For actional best practices, contact your company's legal counsel.

How can I change my Facebook privacy settings?

According to Facebook, in 2014 the company removed the ability for apps that friends use to collect information about an individual user. If you wish to disable third-party use of Facebook altogether--including Login With Facebook and apps that rely on Facebook profiles such as Tinder--this can be done in the Settings menu under Apps And Websites. The Apps, Websites And Games field has an Edit button--click that, and then click Turn Off.

Facebook is also developing a Clear History button, which the company indicates is "their database record of you." CNET and CBS News Senior Producer Dan Patterson noted on CBSN that "there aren't a lot of specifics on what that clearing of the database will do, and of course, as soon as you log back in and start creating data again, you set a new cookie and you start the process again."

THANK YOU!

Social Networking Privacy — How to be Safe, Secure and Social

Hehan Xie

Content

- What is Social Networking
- What information we are sharing when using social networks
- How may our social network information will be used and shared
- Privacy policies
- Tips

What is Social Networking ?

Social networking is the use of Internet-based social media sites to stay connected with friends, family, colleagues, customers, or clients. Social networking can have a social purpose, a business purpose, or both, through sites like Facebook, Twitter, Linkedin, and WeChat.

What information are we sharing when using social network ?

- Your profile
  - Gender, age, familiar information, interests, educational background and employment
- Your status
  - Social networks allow users to past status updates in order to communicate with others
- Your location
  - Real-time location or past location
- Shared content
  - Music, photographs, videos and links to other webpages

How may our social networking information be used and shared ?

- Publicly available information: there may be some data that you share publicly without realizing it, here are some less obvious ways:
  - Certain information may be publicly visible by default
  - A social network (application) can change its privacy policy at any time without a user's permission
  - Approved contacts may copy and repost information(your personal information or pics)
  - Granted Third-party applications view information
  - Social networks do not guarantee the security of the information that has been uploaded to a profile, even when those posts are set to be private

How may your social networking information be used and shared ?

- Advertising
  - Tracking which websites were viewed
  - Storing information associate with specific websites
  - Analyzing aggregate data for marketing purpose
- Third-party applications
  - Take many forms but some typical and popular forms include games , online polls or quizzes
- Employment
  - Potential employers are generally permitted to use whatever information they can gather about an applicant in making hiring decisions
- Policy
  - Advertise some policy related news then affect voter’s choice

Example

- Facebook data misuse and voter manipulation in 2016 U.S. election [1]
  - Cambridge Analytica used stolen Facebook data to target voters for President campaign in the 2016 U.S. election
  - Psychographic profiling — derived from CA's modelling of Facebook user data — was used to segment US voters into targetable groups, including for serving microtargeted online ads.
- Sina Weibo was reported about 172 millions data leak in March 2020 [2]
  - Data was obtained by matching contacts against its address book API (not include pwd)
  - Data Including real names, gender, location, and phone number were post for sale on dark web markets
  - The risk of phishing was amplified due to the large accumulation of personal sensitive data exposed

[1]https://techcrunch.com/2020/01/06/facebook-data-misuse-and-voter-manipulation-back-in-the-frame-with-latest-cambridge-analytica-leaks/
[2]https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Privacy policies

Most people skip over the privacy policy when joining a social network. However, users can learn a lot of useful information by reviewing a privacy policy before signing up for service. A social network's privacy policy will explain how the social network will collect and use information about people who visit the site.

Remember:

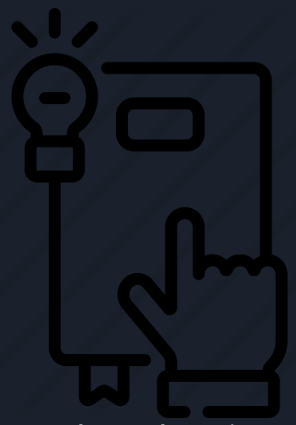
- Privacy policies can change – sometimes dramatically-- after a user creates an account.
- Terms of service may have information just as important as the privacy policy, so always review those as well.
- The privacy policy only covers the social network. It does not cover third-party applications that interact with the website.

Tips

When registering an account

- Use a strong password different from you use to access other sites
- If you are asked to provide security questions, use information that others would not know about
- Consider creating a new email address to use only with our social media profile
- Provide the minimum amount of personal information necessary
- Review the privacy policy and terms of service
- During the registration process, social networks often solicit you to provide an email account password so that they can access your address book or your contact list

Tips



General privacy tips for using social networks

- Become familiar with privacy setting available on any social network and review your privacy settings
- Be careful sharing your birthday, age, or place of birth on social media
- Try to stay aware of changes to a social networks' terms of service and privacy policy
- If receive a connecting request from a stranger, the safest thing to do is reject
- Consider pruning your "friends" list on a regular basis
- Log off from social networking sites when you no longer need

Thanks


SECURITY & PRIVACY ISSUES OF SOCIAL NETWORKS
- CHENGYUAN ZHOU

What are social networks?

Definitions are from Oxford Languages

1. A network of social interactions and personal relationships.
2. A dedicated website or other application which enables users to communicate with each other by posting information, comments, messages, images, etc.

Common examples are Facebook, Instagram, Twitter, WeChat, etc.

What data is out there?

Depends on the type of social network, there could be multiple kinds of data that are collected by them, including but not limited to:

1. Personal Identifiable Information
2. Location data
3. Payment information
4. Biometric data
5. Social media data

Social media data

- All the raw insights and information collected from individual's social media activity such as engagement to some contents or preference to some topics.
- Actionable insights concerning the social media strategy.
- Shares, Likes, Mentions, Impressions, Hashtag usage, URL clicks, Keyword analysis, New followers, Comments.

What do they do with the data?

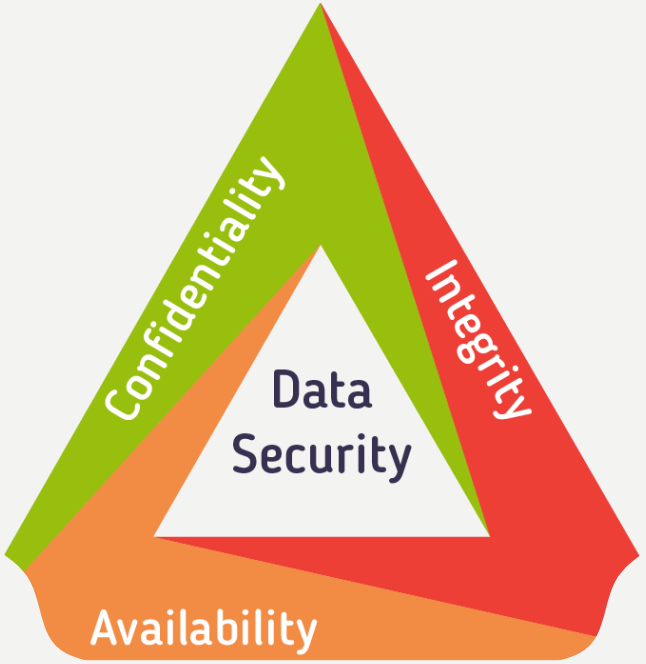
- Thanks to the advancing world of big data, social media platforms now can apply data mining on the collected data. These processed data can help to determine the "hidden attributes about you that you didn't even know you were sharing information about".
- Targeted marketing & advertising
- Political advertisements & propagations

Facebook–Cambridge Analytica data scandal

- Obtaining of the personal data of millions of Facebook users without their consent by consulting firm Cambridge Analytica
- Psychological profiles on users based on their answers to a series of questions
- Personal data of the users via Facebook's Open Graph platform
- The Open Graph platform of Facebook leaked the user profile.
- The data is used in Donald Trump campaign and Ted Cruz campaign in 2016

Security Analysis in FB-CA Scandal

- The data scandal happened because of the defective security policy that it allows the access to Facebook user data for app developers
- The security mechanisms of the Open Graph platform also failed in enforcing app developers like CA to delete misused user data.



Privacy issue of social networks

- Identity theft
- Sexual predators
- Stalking/Cyberstalking
- Unintentional fame
- Online victimization
- Surveillance
- Law enforcement prowling the networks
- ……

Reference – Thanks for watching!

- https://www.oktopost.com/blog/social-media-data/
- https://www.investopedia.com/terms/s/social-data.asp
- https://www.loyola.edu/academics/emerging-media/blog/2017/3-ways-that-social-media-knows-you-better-than-your-friends-and-family-do
- https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/
- https://techcrunch.com/2020/01/06/facebook-data-misuse-and-voter-manipulation-back-in-the-frame-with-latest-cambridge-analytica-leaks/
- https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html
- https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal#cite_note-:8-2
- https://sproutsocial.com/insights/social-media-data/

The Privacy Paradox and Social Media

•••

DSCI 529

Brianna Heffernen

What is the “Privacy Paradox?”

Self Disclosure

Privacy

The link between self disclosure and privacy

What motivates privacy?

- Autonomy
  - Self
  - Relationships
  - Democracy
- Self evaluation
- Protected communication

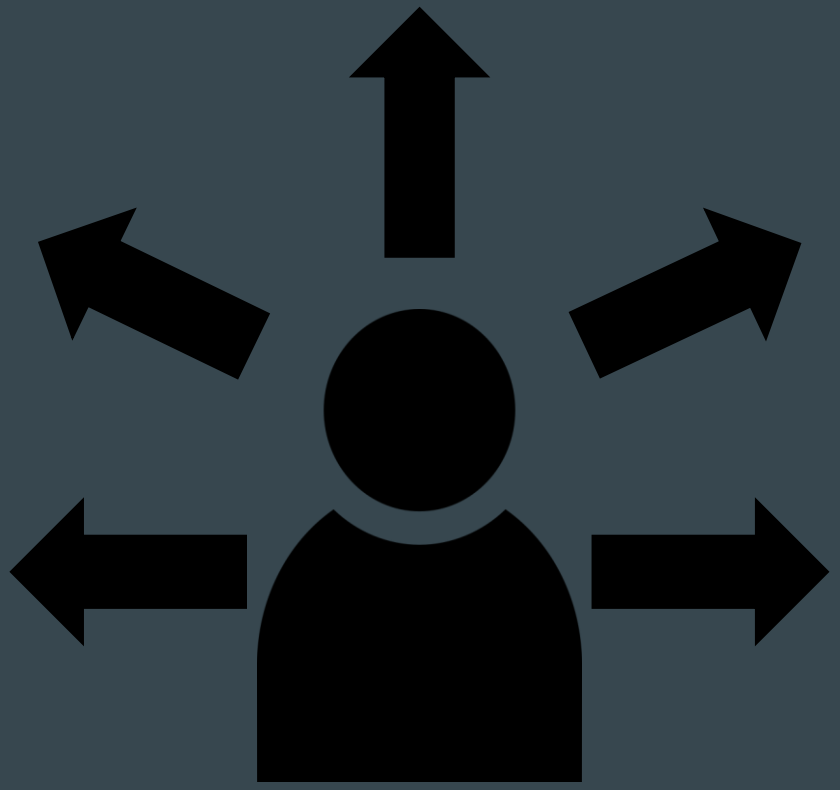
What motivates self-disclosure?

- Self expression
- Extrinsic rewards
- Intrinsic rewards

Why is the Social Web different?

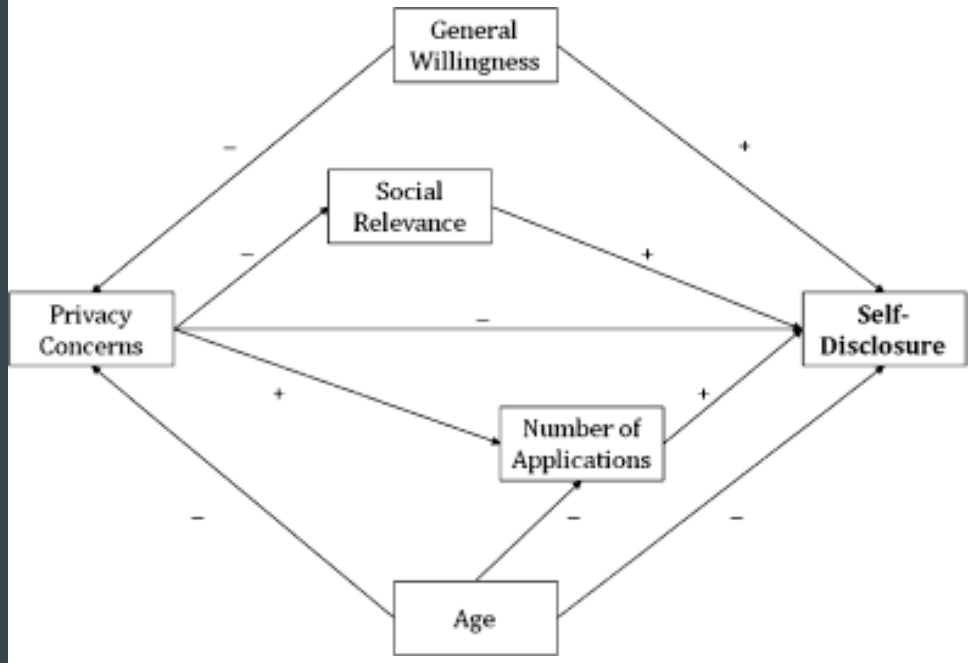
- Persistence
- Replicability
- Scalability
- Searchability
- Shareability

(Papacharissi and Gibson)



How likely are social media users to self-disclose?

(Taddiken)



	Self-Disclosure on the Social Web*				Self-Disclosure on the Social Web by Accessibility‡		
	N	More Frequently	Once	Never	N‡	Open Access§	Restricted Access§
Basic Information							
First Name	2739	72.0%	21.1%	7.0%	2548 (2739)	56.6% (52.6%)	46.4% (43.2%)
E-mail Address	2739	59.4%	28.7%	11.9%	2413 (2739)	23.0% (20.3%)	78.6% (69.3%)
Factual Information							
Last Name	2739	54.7%	30.0%	15.3%	2320 (2739)	38.5% (32.6%)	63.0% (53.4%)
Birth Date	2739	59.8%	28.9%	11.3%	2429 (2739)	37.8% (33.5%)	63.5% (56.3%)
Profession	2739	38.3%	38.3%	23.5%	2096 (2739)	37.8% (29.0%)	63.1% (48.3%)
Postal Address	2739	20.5%	31.4%	45.3%	1497 (2739)	9.7% (5.3%)	88.6% (48.4%)
Sensitive Information							
Photos	2739	31.7%	35.8%	32.5%	1848 (2739)	45.0% (30.4%)	58.5% (39.5%)
Experiences	2739	20.4%	32.0%	47.5%	1437 (2739)	32.8% (17.2%)	68.6% (36.0%)
Thoughts	2739	23.4%	31.3%	45.3%	1498 (2739)	32.6% (17.8%)	68.6% (37.5%)
Feelings	2739	17.8%	24.4%	57.8%	1155 (2739)	30.1% (12.7%)	70.1% (29.6%)
Concerns and Fears	2739	13.1%	21.3%	65.6%	942 (2739)	30.5% (10.5%)	69.3% (23.8%)

(Taddiken)

Future implications

“Privacy, the *right* to be let alone, must not be confused with a *desire* to be let alone.”

- (Papacharissi & Gibson)

Future implications

- Privacy as a commodity
- Consumer protections

(Papacharissi & Gibson)

Works Cited

Monika Taddicken, The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure, *Journal of Computer-Mediated Communication*, Volume 19, Issue 2, 1 January 2014, Pages 248–273, https://doi.org/10.1111/jcc4.12052

Papacharissi, Z., & Gibson, P. L. (2011). 15 minutes of privacy: Privacy, sociality, and publicity on social network sites. In S. Trepte, & L. Reinecke (Eds.): *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 75–89). Heidelberg and New York: Springer.

Nicole C Krämer, Johanna Schäwel (2020). Mastering the challenge of balancing self-disclosure and privacy in social media. Current Opinion in Psychology, Volume 31, 2020, Pages 67-71, https://doi.org/10.1016/j.copsyc.2019.08.003.

M.H. Millham, D. Atkin. Managing the virtual boundaries: online social networks, disclosure, and privacy behaviors, New Media Soc, 20 (2018), pp. 50-67, 10.1177/1461444816654465

Social Networks and Social Media

Services that Enable us to:

- Share our thoughts and experiences
- Record intricate details of our lives
- Create communities of like minded individuals
- Manage our relationships with others online.

The intersections of technology with social interaction.

Bulletin Boards, AOL, Myspace, Facebook, Twitter, Instagram, SnapChat, and many related services. But also includes email and the rest of the web.

Threat Vectors – Social Media

Our use of social media – dissemination
Others use of social media – retrieval
Monitoring and surveillance of Social Media
False information in social media
Reputation and permanence
Many forms of impersonation
Inferences from network analysis
Social Engineering through Social media

What we Post

Pay careful attention to what you post through social media.

- We include much information we might otherwise think of as private.
- We think it is going to only our friends
- We think it is ephemeral

Remember what information is out there:

- Fortune Teller

How Our Data is Used

Surveillance through Social Media

Social Media Surveillance Could Have a Devastating Impact on Free Speech. Here's Why.

Surveillance through Social Media – Good or Bad

- **FBI's near-brush with suspect in Florida school shooting draws scrutiny**

What is "actionable".

Is this prosecuting "pre-crime"

Discussion in Forum

Additional Readings:

- Your view of the Social Dilema on NetFlix
- Privacy in Context
- Restrictions on Content
  - Lots of readings, perhaps more relevant in later lectures.

Discussion of Mid-term Exam

- It has been taking longer than I wanted to complete grading, but you all should have your submitted versions on disk, and grades will be posted by Sunday.

- I will discuss the individual questions and what I was looking for now. You are welcome to ask questions now, and again through email or office hours after you have received your grades.

- But please review this discussion first, before contacting me with individual questions. I am happy to provide more detailed discussions, but start with this overview.

2021 Mid-Term Q1

- In our first assignment you discovered the extent to which the services we use daily collect and use out data. These services included mapping applications, social media, email services, banking and even basic web surfing. What makes this collection of data particularly intrusive is the ability to link data from one datapoint (e.g. transaction, location, query) to another.

- Discuss some of the approaches used to link these datapoints. In many cases, the data is linked through an identifier, and each type of identifier could be a different approach. In your discussion of the approaches, tell me some of the steps end users can take to prevent linkage through that means, and how effective those steps are to preserve privacy.

- Guidance for answering provide at least five approaches but be sure to cover the most-used approaches and cover approaches that span the types used (i.e. don't list five that are all substantially the same). You may list more than 5 to make sure you include a good set. So that you don't get confused, there should be at least 5 three-part answers to this question. At least one for each approach, and the three parts are to (a) describe the approach (including the identifier if relevant), (b) describe some steps that limit this collection, and (c) how effective those steps are.

2021 Mid-Term Q2 – Technical Means of Protection

(15 points) Using cryptographic techniques (i.e. encryption, decryption, and a few other operations) explain the steps necessary to create a message and subsequently verify that the message has not been modified.

Hint: Note that in performing the steps in your answer, you will end up verifying the identity of the individual that created the message. If the message is modified, then the creator of the modified message is different than the original sender, and you will detect that.

(15 points) Forms of Authentication – Why might we want to use a device that we have in our possession as a second factor of authentication in addition to using a password?
List some of the common attacks on password-based authentication that are made more difficult when we use a second factor?

(20 points) Malicious code takes several forms in our computer systems. It includes software that we download to our devices (e.g. Apps) that are "trojan-horses" because they embed actions that are not in our best interest. It includes worm's that subvert servers by exploiting bugs to rewrite the server code itself. It includes viruses which self-replicate to infect other programs on our systems.

How might a malicious app (the first of the examples given in the preceding paragraph) impact our privacy? What are a few steps can you take to prevent such malicious apps from accessing sensitive data on your devices?

2021 Mid-Term Q3

- **(20 points) Big Data –** In lecture 6 we discussed some things that were different about processing of “big data” when compared with the processing of data collected and stored in a database for a traditional application. What is it about these differences that enables data to be used in ways that might not have been planned when the original data was collected (and thus, in ways that might not have been spelled out in the privacy policy of the original application). What other problems might arise from the way data is used/mined in such systems?

Current Event Discussion

- http://csclass.info/USC/INF529/s21-lec9-ce.html