



# INF529: Security and Privacy In Informatics

Privacy and Social Networks

*Prof. Clifford Neuman*

**Lecture 8**

1 March 2018

OHE 100C



# Course Outline

- What data is out there and how is it used
- Technical means of protection
- Identification, Authentication, Audit
- The right of or expectation of privacy
- Government and Policing access to data – February 15th
- Mid-term, Then more on Government, Politics, and Privacy
- **Social Networks and the social contract – March 1st**
- Big data – Privacy Considerations – March 8th
- Criminal law, National Security, and Privacy – March 22nd
- Civil law and privacy – March 29<sup>th</sup> (also Measuring Privacy)
- International law and conflict across jurisdictions – April 5th
- The Internet of Things – April 12<sup>th</sup>
- Technology – April 19th
- The future – What can we do – April 26th

# This Week: Social Networks



---

## Class Discussion on Social Networks

Three student presentations (integrated discussion):

- Nityai Harve
- Deepti Siddagangappa
- Chloe Choe

# Next Week: Big Data & PII Monetization



---

## Big Data

- Jacqueline Dobbas - Location Data
- Kavya Sethuraman

## Monetization of PII

- Faris Almathami - Privacy vs. Marketers and Advertisers

Class discussion on Big Data and Monetization.



# New Readings

---

- [CAS] Cloak and Swagger: Understanding Data Sensitivity Through the Lens of User Anonymity.
- [Levemore] Saul Levemore, "The Offensive Internet: Speech, Privacy, and Reputation"
- [Nissenbaum] Helen Nissenbaum, "Privacy in Context: Technology, Policy, and the Integrity of Social Life"

# 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”

# FACEBOOK AND IT'S MISTAKES

NAME: NITYA MOHINI HARVE

USC ID: 7992-0968-14

March 1, 2018

# WHY PEOPLE STARTED USING FACEBOOK?

- ▶ User Friendly Nature
- ▶ Better Interface
- ▶ Source of Information
- ▶ Entertainment
- ▶ Find Old Friends
- ▶ Sharing Options
- ▶ No Competition

# EXPECTATION OF PRIVACY FROM FACEBOOK

- ▶ My private data is shared only when I give my consent via opting in rather than opting out
- ▶ My private data is stored in a “trusted” location with strong security mechanisms in place
- ▶ If my data is sent to third party companies, it shouldn’t be personally identifiable. Should be anonymized as much as possible to remove any possibility of linking.
- ▶ I should know what data has been collected, be able to access the data and use cases of the data being collected
- ▶ Facebook shouldn’t sell my PII data without consent.
- ▶ Only data relevant to supporting the functionality of Facebook is collected
- ▶ I should have the right to delete any data that has been collected about me/from me and it should be truly deleted from the data storage
- ▶ I should be informed immediately if my data has been leaked in a breach
- ▶ Only people who are my friends can view the data I post publicly
- ▶ My personal messages are not viewed by anyone apart from me and the recipient

CCPA

GDPR

# WHAT DATA IS COLLECTED BY FACEBOOK?

- ▶ Things that you and others do and provide
  - ▶ Information and content you provide
  - ▶ Networks and connections
  - ▶ Your usage
  - ▶ Information about transactions made on our Products
  - ▶ Things others do and information that they provide about you

- ▶ Device information

- ▶ Device attributes
- ▶ Device operations
- ▶ Identifiers
- ▶ Device signals
- ▶ Data from device settings
- ▶ Network and connections
- ▶ Cookie data

## Information from partners

- ▶ Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about your activities off Facebook—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have a Facebook account or are logged into Facebook.

# Facebook's Data Use Policy

2013 :

- ▶ “We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use.”

2015 :

- ▶ “Information from third-party partners - We receive information about you and your activities on and off Facebook from third party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.
- ▶ Facebook companies - We receive information about you from companies that are owned or operated by Facebook, in accordance with their terms and policies.
- ▶ Sharing With Third-Party Partners and Customers - We work with third party companies who help us provide and improve our Services or who use advertising or related products, which makes it possible to operate our companies and provide free services to people around the world.”

# MAJOR PRIVACY ISSUES ENCOUNTERED SO FAR

- ▶ CAMBRIDGE ANALYTICA - MARCH 2018
- ▶ A BUG CHANGED PRIVACY SETTINGS OF UP TO 14 MILLION USERS - JUNE 2018
- ▶ FACEBOOK INADVERTENTLY INTRODUCED THREE VULNERABILITIES IN ITS VIDEO UPLOADER - SEPTEMBER 2018
- ▶ DATA BREACH EXPOSES USER PHOTOS - DECEMBER 2018
- ▶ FACEBOOK GAVE TECHNOLOGY COMPANIES SPECIAL ACCESS TO USER'S DATA WITHOUT ANYONE ELSE KNOWING - DECEMBER 2018

# MAJOR PRIVACY ISSUES ENCOUNTERED SO FAR

- ▶ **FACEBOOK vs SIX4THREE - December 2018**
  - ▶ **Whitelisting agreements with companies to maintain access to friends' data after policy changes stopping it.**
  - ▶ **Reciprocity - "Full reciprocity means that apps are required to give any user who connects to FB a prominent option to share all of their social content within that service (i.e. all content that is visible to more than a few people but excluding 1:1 or small group messages) back to Facebook."**
  - ▶ **Facebook used Onavo to conduct global surveys of the usage of mobile apps by customers, and apparently without their knowledge.**



# FACEBOOK'S ATTEMPTED REDEMPTION

- ▶ Allowing users to take control of the ads shown to them
- ▶ Facebook no longer works with third-party data providers to offer their targeting segments directly on Facebook.
- ▶ Facebook pledged to make changes to its data policies and introduces new measures to make its privacy controls easier to find and use.
- ▶ Facebook announced an update made to its data policy to “better spell out what data we collect and how we use it in Facebook, Instagram, Messenger and other products,” as well as additional updates to restrict data access on the site. Facebook also asks users to review their privacy settings.
- ▶ Facebook announced a program called the Data Abuse Bounty to “reward people who report any misuse of data by app developers.”
- ▶ Facebook introduced plans to build a feature called “Clear History” that will allow users to have more information about and control over personal data usage from third-party applications.
- ▶ Facebook introduced a customized message onto individuals users' News Feeds with detailed explanations about their chosen privacy settings.

- Login and Password
- Your Profile and Settings
- Names on Facebook
- Keeping Your Account Secure
- Notifications
- Ad Preferences**

---

- How Ads Work on Facebook**

  - Control the Ads You See
  - Your Info and Facebook Ads

---

- Accessing & Downloading Your Information
- Deactivating or Deleting Your Account

## How does Facebook work with data providers?

Share article

This page used to contain a list of the third-party data providers that Facebook worked with to offer their targeting segments directly on Facebook, and a description of that program. After we last updated our Data Policy (in April 2018), we terminated this program. Facebook no longer works with third-party data providers to offer their targeting segments directly on Facebook.

Businesses may continue, on their own, to work with data providers. Many businesses today work with third parties to help manage and understand their marketing efforts. For example, an auto dealer may want to customize an offer to people who are likely to be interested in buying a new car. The dealer also might want to send offers, like discounts for service, to customers that have purchased a car from them. To do this, the auto dealer works with a third-party company to identify and reach those customers with the right offer.

So businesses who advertise to you may be using a list of people that they've gotten, or gotten the ability to use, from third parties that they work with for their marketing efforts. Businesses that advertise on Facebook are required to have any necessary rights and permissions to use this information, as outlined in our [Custom Audience Terms](#) that businesses must agree to.

You can learn more about what influences the ads you see and control your ads experience by visiting [Ad Preferences](#).

facebook



### Some important updates and settings to review

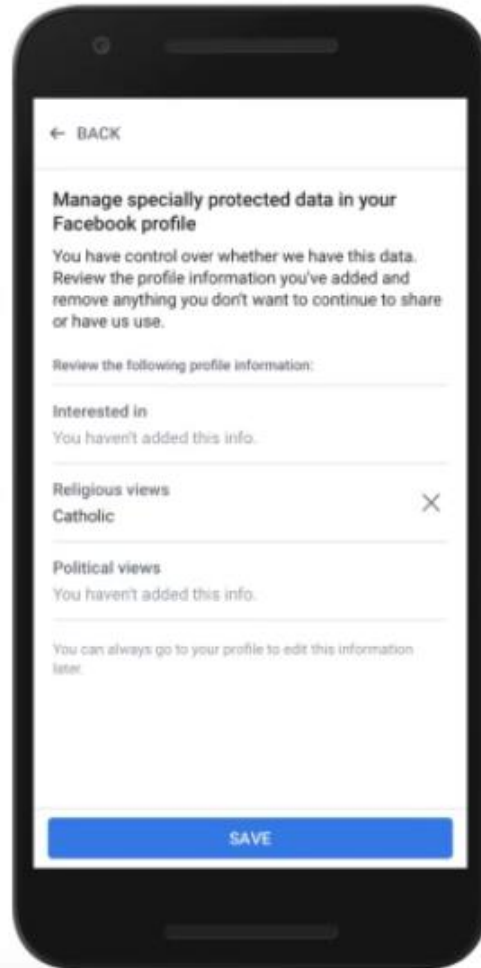
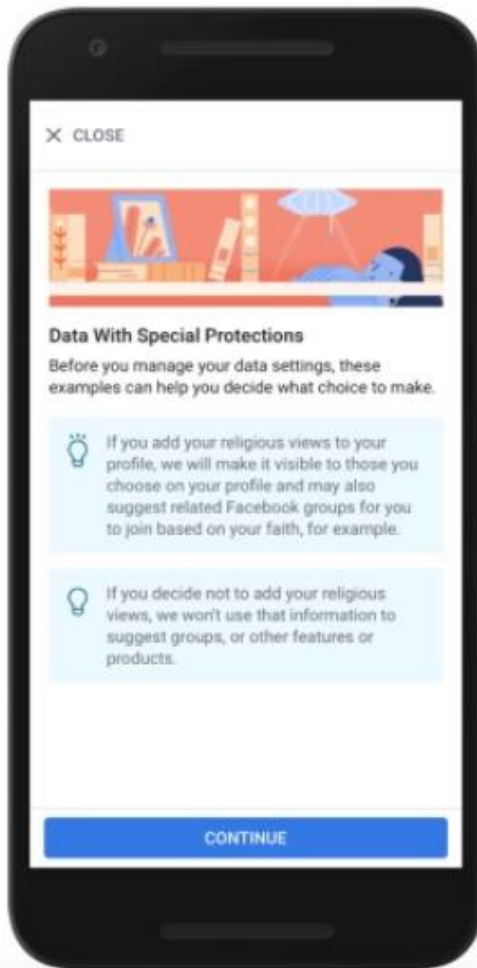
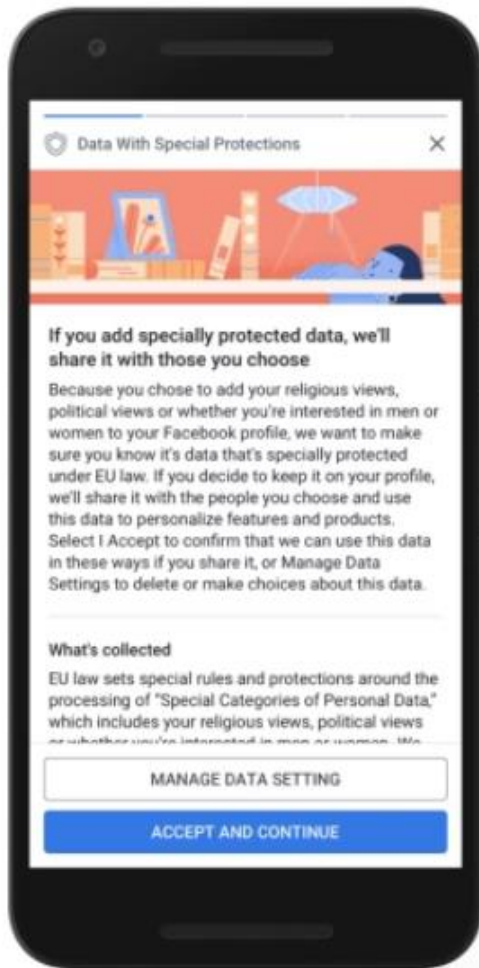
Personal data laws are changing in the European Union, and we want to make it easy for you to view some of your data settings.

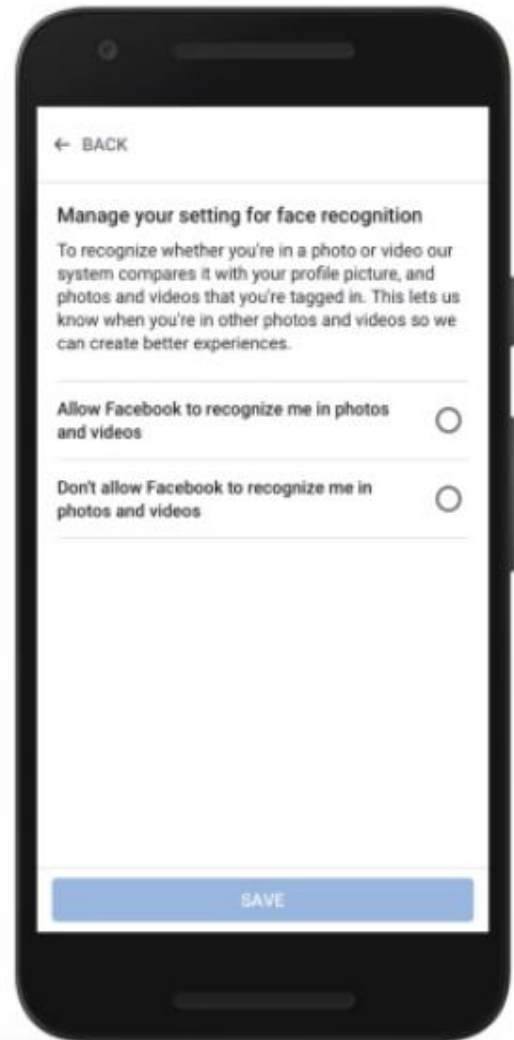
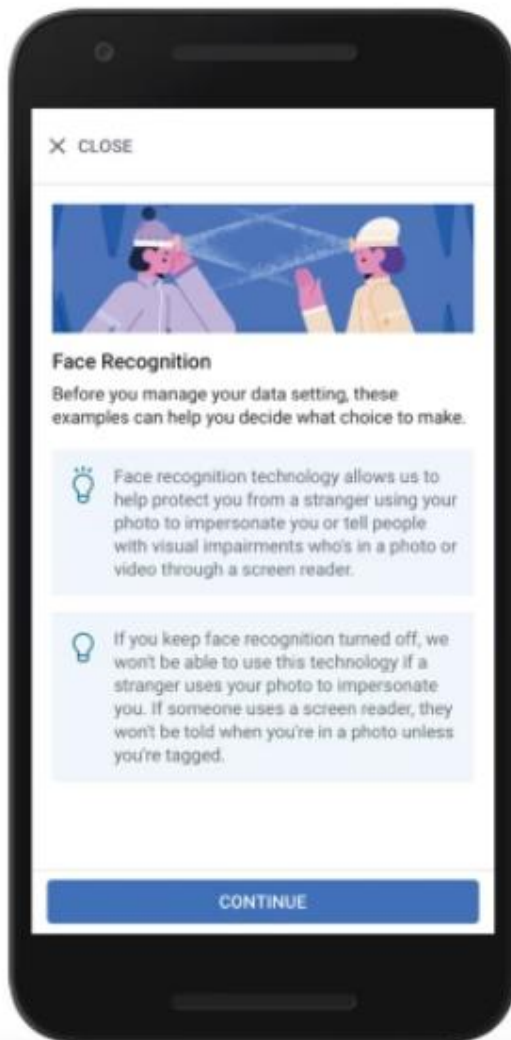
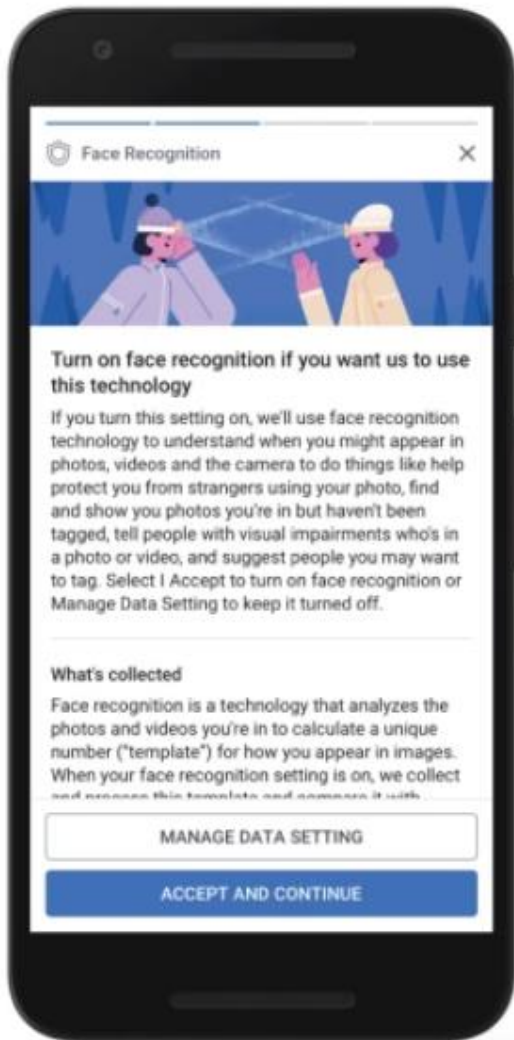
Please take a few minutes to review these updates and make choices about some specific data settings.

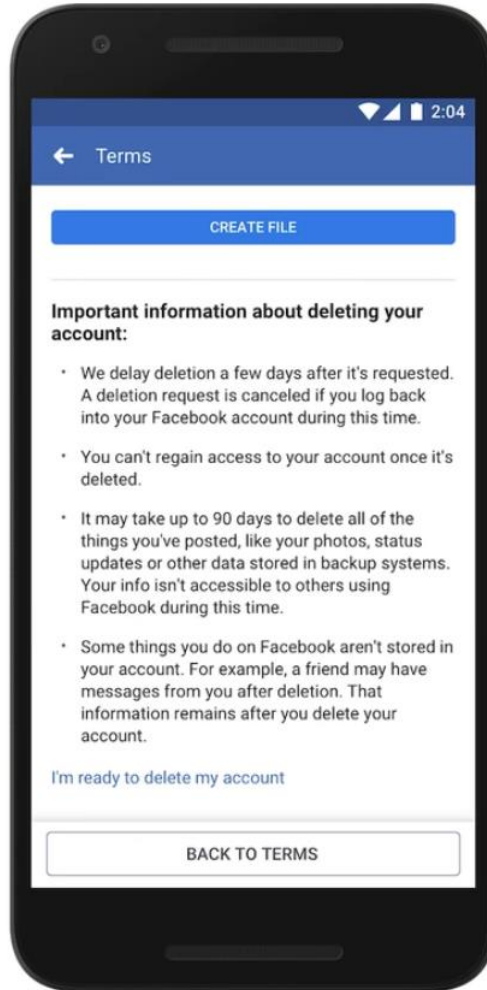
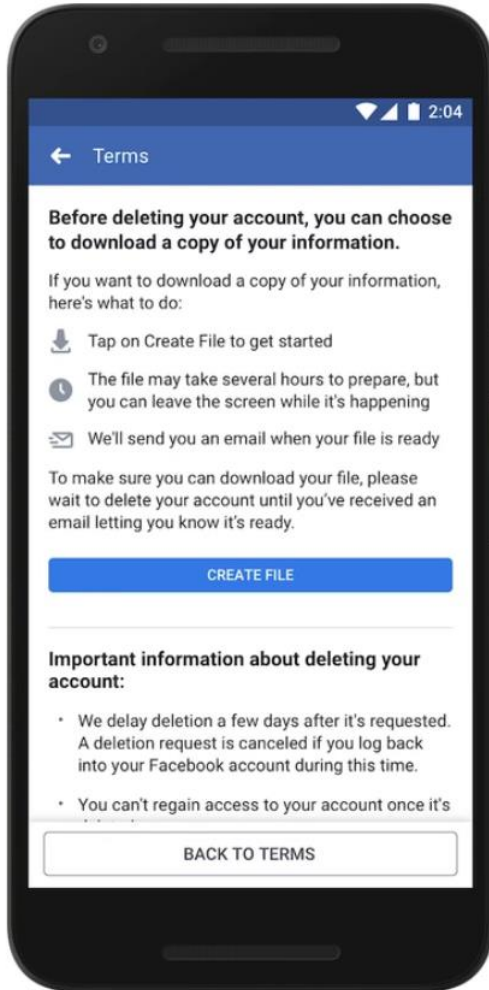
#### Here's what we'll have you review:

- How we use personal data from partners to show you relevant ads
- How we use the specially protected personal data you choose to add on your profile
- An option to turn on face recognition
- Our updated Terms, Data Policy and Cookies Policy

GET STARTED









Search



Nitya

Home

Create



- General
- Security and login

**Your Facebook information**

- Privacy
- Timeline and tagging
- Location
- Blocking
- Language
- Face recognition

- Notifications
- Mobile
- Public posts

- Apps and websites
- Instant Games
- Business integrations
- Ads
- Payments
- Support Inbox
- Videos

## Your Facebook information

You can view or download your information and delete your account at any time.

<b>Access your information</b>	View your information by category.	<a href="#">View</a>
<b>Download your information</b>	Download a copy of your information to keep or to transfer to another service.	<a href="#">View</a>
<b>Activity log</b>	View and manage your information and some settings.	<a href="#">View</a>
<b>Managing your information</b>	Learn more about how you can manage your information.	<a href="#">View</a>
<b>Delete your account and information</b>	Permanently delete your Facebook account and information.	<a href="#">View</a>

## Download Your Information

You can download a copy of your Facebook information at any time. You can download all of it at once, or you can select only the types of information and date ranges you want. You can choose to receive your information in an HTML format that is easy to view, or a JSON format, which could allow another service to more easily import it.

Downloading your information is a password-protected process that only you will have access to. Once you've created a file, it will be available for download for a few days.

If you'd like to view your information without downloading it, you can [Access Your Information](#) at any time.

**New File**

Available Files **1**

Date:

Format:

Quality:

Create File

**Your Information** ⓘ

Select All



**Posts**

Posts you've shared on Facebook, posts that are hidden from your timeline, and polls you have created



**Photos**

Photos you've uploaded and shared



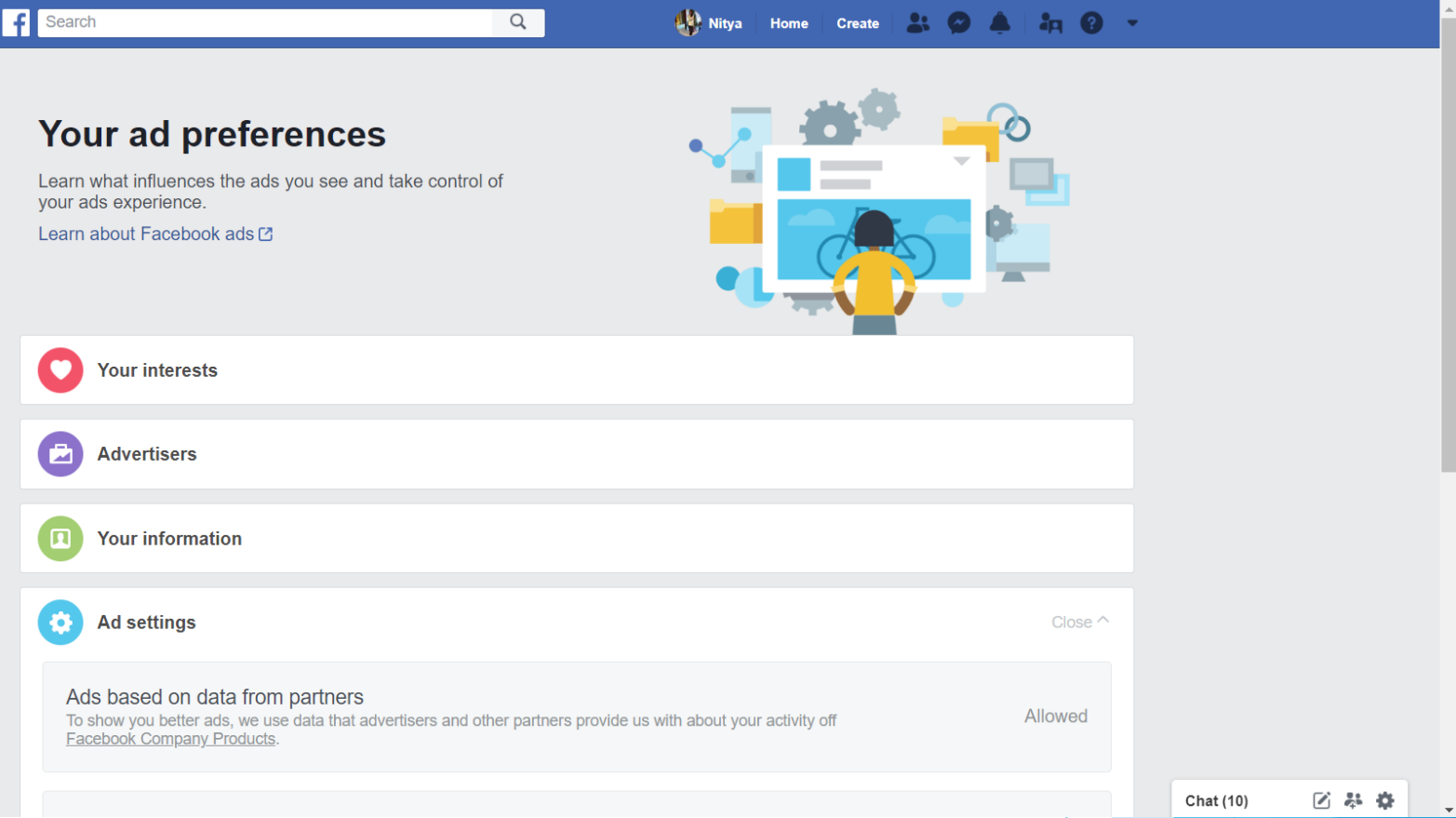
**Videos**

Videos you've uploaded and shared





# HOW USER'S CAN MANAGE WHAT DATA HAS BEEN STORED ABOUT THEM



The image shows a screenshot of the Facebook 'Your ad preferences' page. At the top, there is a search bar with the Facebook logo and a search icon. To the right of the search bar, the user's name 'Nitya' is displayed, along with navigation links for 'Home' and 'Create', and icons for friends, messages, notifications, and a help/question mark. The main heading is 'Your ad preferences' in bold black text. Below the heading, there is a sub-heading 'Learn what influences the ads you see and take control of your ads experience.' followed by a link 'Learn about Facebook ads'. To the right of the text is an illustration of a person in a yellow shirt looking at a computer screen, surrounded by various icons representing data, settings, and user interests. Below the text and illustration are four main sections: 'Your interests' (with a red heart icon), 'Advertisers' (with a purple briefcase icon), 'Your information' (with a green person icon), and 'Ad settings' (with a blue gear icon). The 'Ad settings' section is expanded, showing a toggle for 'Ads based on data from partners' which is currently set to 'Allowed'. Below this, there is a partially visible section for 'Ads based on your activity off Facebook Company Products'. At the bottom right of the page, there is a chat notification that says 'Chat (10)' with icons for chat, a group, and settings.



Search



Nitya

Home

Create



## Advertisers



### Your information

Close ^

About you

Your categories

The categories in this section help advertisers reach people who are most likely to be interested in their products, services and causes. We've added you to these categories based on information you've provided on Facebook and other activity.

Birthday in September

Early technology adopters

**About Facebook access (browser): Chrome**

People who primarily access Facebook using Google Chrome.

Gmail users

Facebook access (browser): Chrome



Owns: Galaxy S8+

Uses a mobile device (25 months+)

Family of those who live abroad

Facebook access (mobile): Samsung Android mobile... devices

Facebook access (OS): Windows 10

Facebook access (mobile): all mobile devices

Frequent international travellers

See more

Was the **information about your categories** section helpful to you? Yes No

Chat (11)



### Advertisers

Close ^

Who use a contact list added to Facebook Whose website or app you've used Who you've visited More

Review advertisers whose ads you may currently be seeing because you've visited their website or app that uses

Whose ads you've clicked  
Who you've hidden



Keurig



Today Show



KLM Finland



KLM Norge



Runner's World



BuzzFeed México



Women's Health



AirHelp



BuzzFeed Canada



Vogue



KLM Polska



Nifty Brasil

See more

Was the **advertisers** section helpful to you? Yes No

### Your information

- General
- Security and login
- Your Facebook information
- Privacy**
- Timeline and tagging
- Location
- Blocking
- Language
- Face recognition
- Notifications
- Mobile
- Public posts
- Apps and websites
- Instant Games
- Business integrations
- Ads
- Payments
- Support Inbox
- Videos

### Privacy Settings and Tools

<b>Your activity</b>	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
<b>How people can find and contact you</b>	Who can send you friend requests?	Friends of friends	Edit
	Who can see your friends list?	Friends	Edit
	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your Profile?	No	Edit



Search



Nitya

Home

Create



### Filters

Activity log

Timeline review

Photo review

Posts

Posts you're tagged in

Other people's posts to your timeline

Hidden from timeline

Photos and videos

Likes and reactions

Comments



## Activity log

Activity Search



February 2019

### TODAY

Nitya Mohini Harve was tagged in Adventure Gurus's photo.



Best way to see the sign is when you can hike to it!

2019

2018

2017

2016

2015

2014

2013

2012

2011

2010

2009

2008

2007

- General
- Security and login
- Your Facebook information

- Privacy**
- Timeline and tagging
- Location
- Blocking
- Language
- Face recognition

- Notifications
- Mobile
- Public posts

- Apps and websites
- Instant Games
- Business integrations
- Ads
- Payments
- Support Inbox
- Videos

## Privacy Settings and Tools

### Your activity

Who can see your future posts?

Friends

Edit

Review all your posts and things you're tagged in

[Use Activity Log](#)

#### Limit The Audience for Old Posts on Your Timeline

Close

If you choose to limit your past posts, posts on your timeline that you've shared with Friends of friends, and Public posts, will only be shared with Friends. Anyone tagged in these posts, and their friends, may also still see these posts.

If you want to change who can see a specific post, you can go to that post and choose a different audience. [Learn about changing old posts](#)

[Limit Past Posts](#)

### How people can find and contact you

Who can send you friend requests?

Friends of friends

Edit

Who can see your friends list?

Friends

Edit

Who can look you up using the email address you provided?

Friends

Edit

Who can look you up using the phone number you provided?




Friends

Edit







Do you want search engines outside of Facebook to link to your Profile?

No




Edit

-  General
-  Security and login
-  Your Facebook information








---

-  Privacy
-  Timeline and tagging
-  Location**
-  Blocking
-  Language
-  Face recognition


---

-  Notifications
-  Mobile
-  Public posts

---

-  Apps and websites
-  Instant Games
-  Business integrations
-  Ads
-  Payments
-  Support Inbox
-  Videos

### Location settings

 You can change your location settings in the app on your device. If you haven't got the app installed, locations cannot be received from the device.

**Location history**

**Your location history is off**  
 Facebook builds a history of precise locations received through location services on your device. Only you can see this information and you can delete it by viewing your location history. [Learn more.](#)

[View your location history](#)

- General
- Security and login
- Your Facebook information

---

- Privacy
- Timeline and tagging
- Location
- Blocking
- Language
- Face recognition

---

- Notifications
- Mobile
- Public posts**

---

- Apps and websites
- Instant Games
- Business integrations
- Ads
- Payments
- Support Inbox
- Videos

### Public Post Filters and Tools

**Who Can Follow Me** Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your public posts. Use this setting to choose who can follow you. Friends ▾

Each time you post, you choose which audience you want to share with.

This setting doesn't apply to people who follow you on Marketplace and in buy-and-sell groups. You can manage those settings on Marketplace.

[Learn more.](#)

<b>Public Post Comments</b>	Who can comment on your public posts? <b>Public</b>	<a href="#">Edit</a>
<b>Public Post Notifications</b>	Get notifications from <b>Public</b>	<a href="#">Edit</a>
<b>Public Profile Info</b>	Who can like or comment on your public profile pictures and other profile info? <b>Friends</b>	<a href="#">Edit</a>



- General
- Security and Login
- Your Facebook Information
- Privacy
- Timeline and Tagging
- Location
- Blocking
- Language
- Notifications
- Mobile
- Public Posts
- Apps and Websites**
- Instant Games
- Business Integrations
- Ads
- Payments
- Support Inbox
- Videos

### Apps and Websites

Logged in With Facebook

Active 4 Expired Removed

Search Apps and Websites

#### Data Access: Active





These are apps and websites you've used Facebook to log into and have recently used. They can request info you chose to share with them. [Learn More](#)

Use this list to:

- View and update the info they can request
- Remove the apps and websites you no longer want

#### Active Apps and Websites

Remove

	<b>Quora</b> <a href="#">View and edit</a>	<input type="checkbox"/>
	<b>Goodreads</b> <a href="#">View and edit</a>	<input type="checkbox"/>
	<b>Academia.edu</b> <a href="#">View and edit</a>	<input type="checkbox"/>
	<b>UPS My Choice</b> <a href="#">View and edit</a>	<input type="checkbox"/>

#### Preferences

# WHY PEOPLE STILL USE FACEBOOK?

- ▶ “Because everyone else uses it”
- ▶ “It's an easy and convenient way to keep in touch with my friends and family and share photos and videos with people.”
- ▶ “First, I have a number of acquaintances whose lives I like to be updated about but do not want to “chat on the phone” with to find that information. Secondly, Facebook is the way I login to a lot of other places I don't want to give up.”
- ▶ “I have always assumed that every service I use is trying to store and analyse my information, and unless they're stalking me or somehow stealing from my bank account... I don't care. It's free and I can keep in touch with my relatives overseas.”
- ▶ “I don't even have an email or phone number for my old college roommate but can contact her via Facebook.”

# REFERENCES

- ▶ <https://www.technotification.com/2015/01/why-facebook-is-so-popular.html>
- ▶ <https://www.nytimes.com/2018/06/07/technology/facebook-privacy-bug.html>
- ▶ <https://www.facebook.com/privacy/explanation>
- ▶ [https://www.wired.com/story/facebook-security-breach-50-million-accounts/?fbclid=IwAR1wjL5U93G4uScl1AqvXXWHU\\_Wli07ovqovhZ4mvBM6riP8-D3uC8p-54](https://www.wired.com/story/facebook-security-breach-50-million-accounts/?fbclid=IwAR1wjL5U93G4uScl1AqvXXWHU_Wli07ovqovhZ4mvBM6riP8-D3uC8p-54)
- ▶ <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>
- ▶ <https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/>
- ▶ <https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf>
- ▶ <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- ▶ <https://www.businessinsider.com/facebook-documents-six4three-case-published-british-parliament-2018-12>
- ▶ <https://www.facebook.com/help/494750870625830?ref=dp>
- ▶ [https://www.kctv5.com/news/more-privacy-problems-for-facebook/article\\_37e3c1a8-03d7-11e9-9e64-f3e82585864d.html?fbclid=IwAR1LDC-kSwcEnHDBUDdpZGOLidrpL8JsY-yeV6XwbDTTgcbnKldfXotSCNs](https://www.kctv5.com/news/more-privacy-problems-for-facebook/article_37e3c1a8-03d7-11e9-9e64-f3e82585864d.html?fbclid=IwAR1LDC-kSwcEnHDBUDdpZGOLidrpL8JsY-yeV6XwbDTTgcbnKldfXotSCNs)
- ▶ [https://www.theverge.com/2019/2/26/18241985/facebook-clear-history-launch-2019-ad-targeting-privacy-tool?fbclid=IwAR0SksVj3Yaww\\_lb4T5lNAdZHi9xfVO43LuIFJe6bWZu0pGbpXvAgwS2UWA](https://www.theverge.com/2019/2/26/18241985/facebook-clear-history-launch-2019-ad-targeting-privacy-tool?fbclid=IwAR0SksVj3Yaww_lb4T5lNAdZHi9xfVO43LuIFJe6bWZu0pGbpXvAgwS2UWA)
- ▶ <https://www.chicagotribune.com/business/national/ct-facebook-privacy-policy-20180325-story.html?fbclid=IwAR2jsa1cS0tQbtJfyudlhmArlzeenOnFbi40ScLrbQn9pq-jivR5TjAt4Mg>
- ▶ <https://www.theverge.com/2018/12/5/18127230/facebook-data-documents-parliament-deals-zuckerberg>
- ▶ <https://tech.co/news/facebook-data-breach-exposes-user-photos-2018-12>
- ▶ <https://techcrunch.com/2018/04/17/facebook-gdpr-changes/>
- ▶ <https://www.digitaltrends.com/social-media/terms-conditions-facebooks-data-use-policy-explained/>
- ▶ <https://www.counterextremism.com/blog/updated-tracking-facebook%E2%80%99s-policy-changes>
- ▶ <https://www.cbsnews.com/news/facebook-promises-for-protecting-your-information-after-data-breach-scandal/>

Deepti Siddagangappa

# **Social Network- Privacy Concerns and Potential dangers**

---

# Agenda

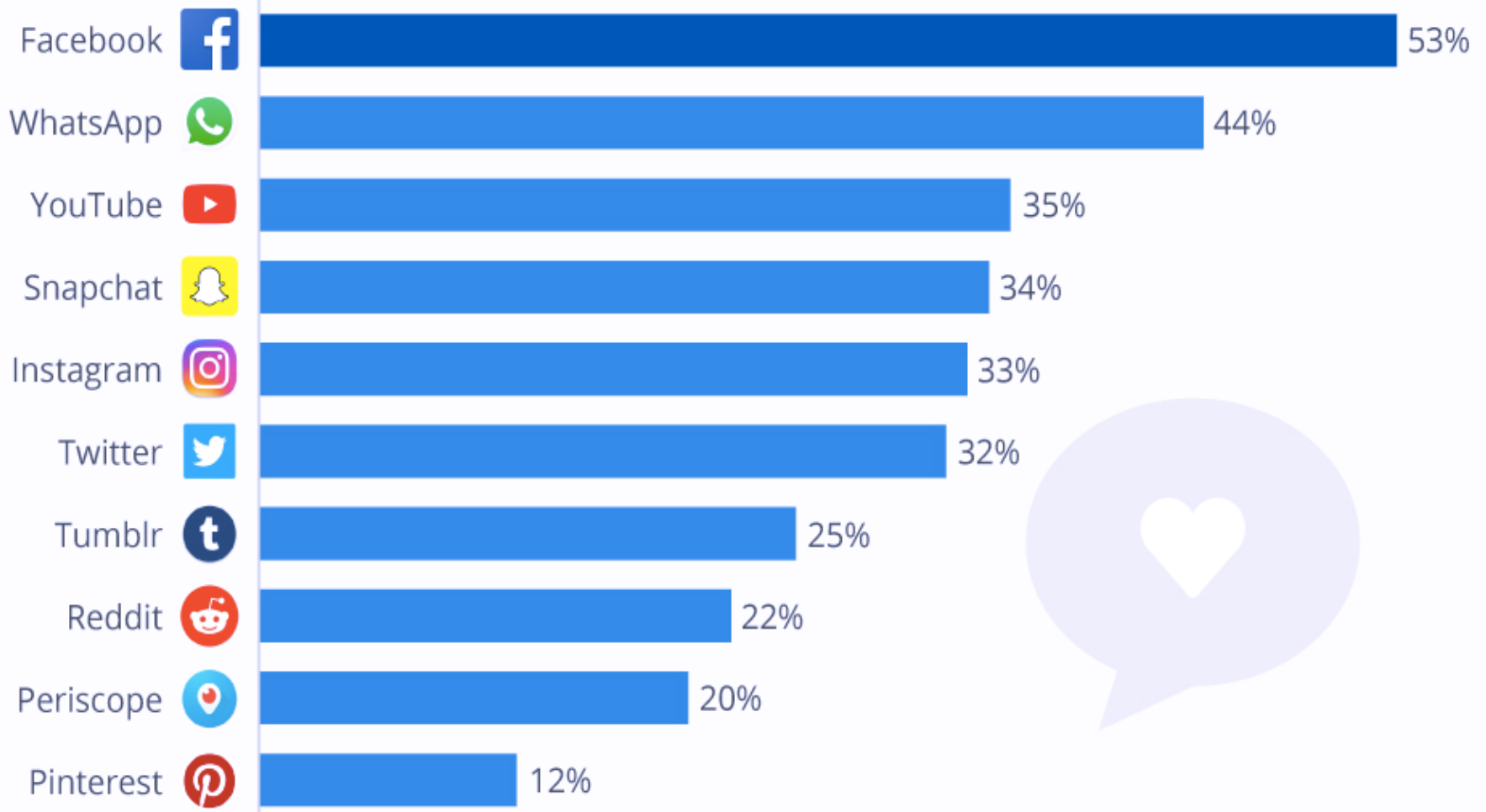
- Privacy Concerns
- Potential Threats
- Case Study
  - United States v. Drew
  - Arizona Spammers
  - F1 driver robbed
  - 30 years jail for Facebook post
  - Mind reader reveals his secret



- Social networking is the practice of expanding the number of one's business and/or social contacts by making connections through individuals, often through social media sites such as Facebook, Twitter, LinkedIn and Google+.

# Always on...Facebook

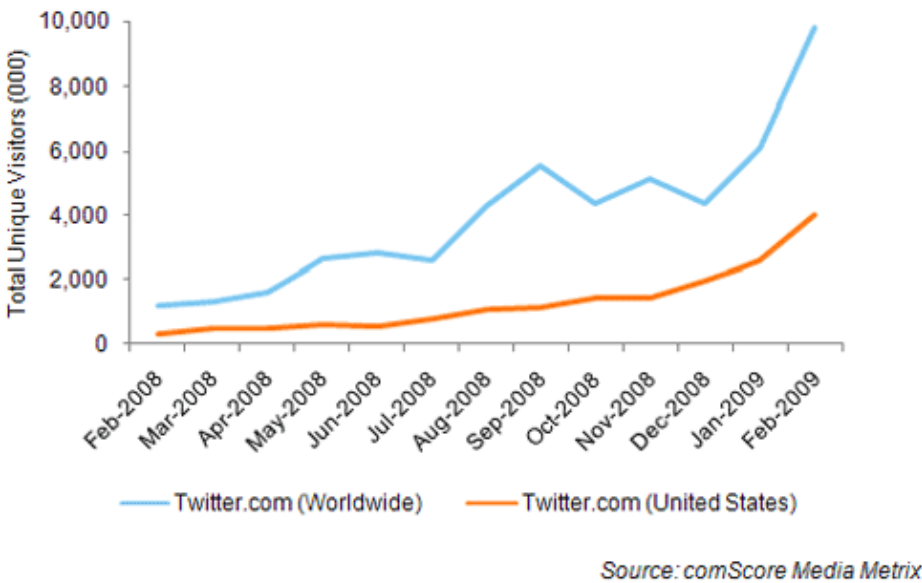
Share that use the following social media apps "several times a day" in the U.S.\*



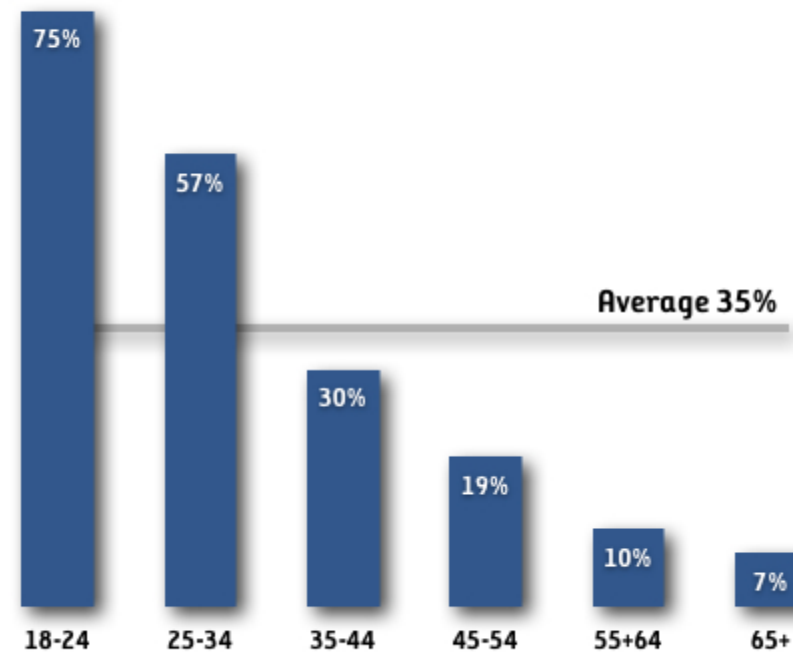
\* mobile only



# Explosion of Social Network



Have a profile on a social network site  
Percentage of Internet Users, By Age



- Rapid growth of social network sites spawns a new area of network security and privacy issues



# Privacy Concerns

## **1. The Privacy Act of 1974 (a United States federal law) states:**

- "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains [subject to 12 exceptions]."

# Exceptions in the privacy law

- Freedom of information Act
- Information disclosed is compatible with the purpose
- For members of an agency.
- Statistical research
- Law Enforcement Agency
- Health or safety of individual
- requested by House of Congress
- Court order
- Government Accountability office
- Debt Collection Act
- National Archives and Records
- Third party if it is meant for statistical research and not “individually identifiable”.

## **2. Companies**

- Privacy settings page
- Instagram, Twitter and Facebook

# Potential Threats

- Identity Theft
- Pre Teens and Early teens
- Sexual Predators
- Stalking
- Unintentional fame
- Employment
- Online Victimization
- Surveillance

# Social Network – Privacy Issues

- United States v. Drew
- Arizona Spammers
- F1 driver robbed
- 30 years jail for Facebook post
- Mind reader reveals his secret

# United States v. Drew

- The Communications Decency Act of 1996 currently exempts websites and internet service providers from liability relating to information posted by third party users, even if it is used for criminal purposes. It also protects them from liability for refusing to disclose the identities of anonymous posters who use the websites for criminal or fraudulent activities.
- Jury convicted a Missouri woman who had created a false MySpace entry of violating the Computer Fraud and Abuse Act (CFAA)
- Defendant, Drew, had created a fake MySpace profile of a teenage boy, "Josh," and used it to "friend" and develop an online relationship with one of her daughter's friends, teenager Megan Meier.
- After several months of online correspondence, "Josh" lashed out at Meier. Shortly after receiving a message from "Josh" that the world would be a better place without her, Meier committed suicide.

# Arizona Facebook Scammers

- Scammers look for targets on facebook.
- Scammers then contact targets as government officials.
- Then push some more information and claim tax on their behalf.
- Targets- unemployed
- Data Retrieved- sensitive information

# F1 Driver Robbed

UK Formula one driver Jenson Button had his house robbed at St Tropez, France.

- How could the robbers have found their location ?
- Key lesson- Ensure social media privacy settings are set to your personal requirements.



# 30 Years of Jail for FB post

- 48 year old Man sentenced for 30 years of jail for insulting Thailand Monarchy through facebook posts.
- Sentenced in Bangkok Military court under a rule known as *injured majesty* .Anyone who insulted the King, Queen, or heir would face imprisonment for 15 year each.
- Man admitted to defaming the monarchy in 6 different posts.
- Original sentence was 60 years but on admission of guilt reduced to 30 years.
- Lesson - Take a moment to consider everything that you are posting to your social media accounts.

# Amazing mind reader reveals his secret

- Dave is an extremely gifted psychic who finds out specific financial information. This [video](#) reveals the magic behind the magic, making people aware of the fact that their entire life can be found online. And by doing so urging everybody to be vigilant.
- Tips for using online banking more safely can be found at <http://safeinternetbanking.be>

# References

- <https://www.youtube.com/watch?v=F7pYHN9jC9I&feature=youtu.be>
- <https://www.hongkiat.com/blog/bizarre-facebook-crimes/>
- <https://www.socialmediatoday.com/news/social-media-privacy-and-scams-3-recent-cases-that-highlight-the-need-to/454720/>
- <https://nakedsecurity.sophos.com/2015/08/07/facebook-tax-refund-scam-earns-arizona-woman-6-years-in-jail/>
- [https://en.wikipedia.org/wiki/Privacy\\_concerns\\_with\\_social\\_networking\\_services](https://en.wikipedia.org/wiki/Privacy_concerns_with_social_networking_services)
- [https://www.reddit.com/r/IAmA/comments/1ndvop/im\\_joe\\_lipari\\_the\\_nyc\\_comedian\\_turned\\_terror/](https://www.reddit.com/r/IAmA/comments/1ndvop/im_joe_lipari_the_nyc_comedian_turned_terror/)



# Cambridge Analytica and Facebook— A Case Study


Chloe Choe

INF 529

March 1, 2019



# Agenda

- ▶ History of Facebook and Data Collection
  - ▶ 2016 Election and Cambridge Analytica
  - ▶ Aftermath
  - ▶ Policies, Issues, and Implications
  - ▶ What can you do?
- 



# History of Facebook

- ▶ 2003: Mark Zuckerberg started FaceMash at Harvard University.
- ▶ 2006: Opened registration broadly.
- ▶ 2007: Facebook ad platform and Pages. Advertising partnership with Microsoft. Beacon program that launches user Facebook activity on other sites.
- ▶ 2009: Surpasses MySpace as largest social network.
- ▶ 2010: Open Graph API.
- ▶ 2011: Federal Trade Commission (FTC) settlement for deceiving and violating privacy policies.



# 2011 FTC Violation

- ▶ December 2009: Facebook changed website so certain information that was private turned public (i.e. Friends List) without consent or warning.
- ▶ Third-party apps had access to unnecessary amounts of personal data.
  - ▶ PII is toxic waste!
- ▶ “Friends Only” did not prevent data from being shared to third-party apps.
- ▶ “Verified Apps” didn’t actually certify these apps.
- ▶ Broke privacy policy of not sharing information with advertisers.
- ▶ Deleted accounts’ data still accessible.
- ▶ Did not comply with U.S. – EU Safe Harbor Framework when claiming it did.



# Facebook Settlement with FTC

- ▶ No misrepresentations about privacy or security of consumers.
- ▶ Required consent before changing privacy preferences.
- ▶ No access to data 30 days after deleting account.
- ▶ Comprehensive privacy program to address risks and protect consumers' information.
- ▶ Obtain independent, third-party audits certifying it has privacy program in place that meets FTC order every two years.





# Cambridge Analytica and the 2016 Election

- ▶ Kogan sold 50 million user data (users and friends) to Cambridge Analytica.
- ▶ Ted Cruz, Ben Carson, and other Republicans hired Cambridge Analytica for data.
- ▶ “When you think about the fact that Donald Trump lost the popular vote by 3m votes but won the electoral college vote, that's down to the data and the research.” – Alexander Tayler, Cambridge Analytica data head.
  - ▶ Targeted users with bespoke messages.



# How did Facebook get involved?

- ▶ 2010: Facebook launched OpenGraph to third party applications, which allowed the third party applications to access large amounts of user data and friend data.
- ▶ 2013: Aleksandr Kogan launched “thisisyourdigitallife” which was an application which prompted users to answer questions about their psychological profile.
  - ▶ 300,000 users participated.
- ▶ 2014: Facebook changed its rules so that friend data cannot be accessed without their permission. Aleksandr Kogan of Cambridge Analytica did not comply and delete previously acquired data.
- ▶ December 2015: Facebook told Cambridge Analytica to delete all data.
  - ▶ Did not follow up to confirm.



# Aftermath of Cambridge Analytica

- ▶ Kogan claimed he was doing everything in accordance to Facebook policy, according to Cambridge Analytica staffer Christopher Wylie [4].
- ▶ Facebook fined \$650k over scandal [6].
  - ▶ Cutting off applications' access to your data after three months if inactive [7].
  - ▶ Disclose information of advertisers and what is an ad [7].
  - ▶ New initiative to conduct "independent, credible research about the role of social media in elections, as well as democracy more generally" [7].



# Policies, Issues, and Implications

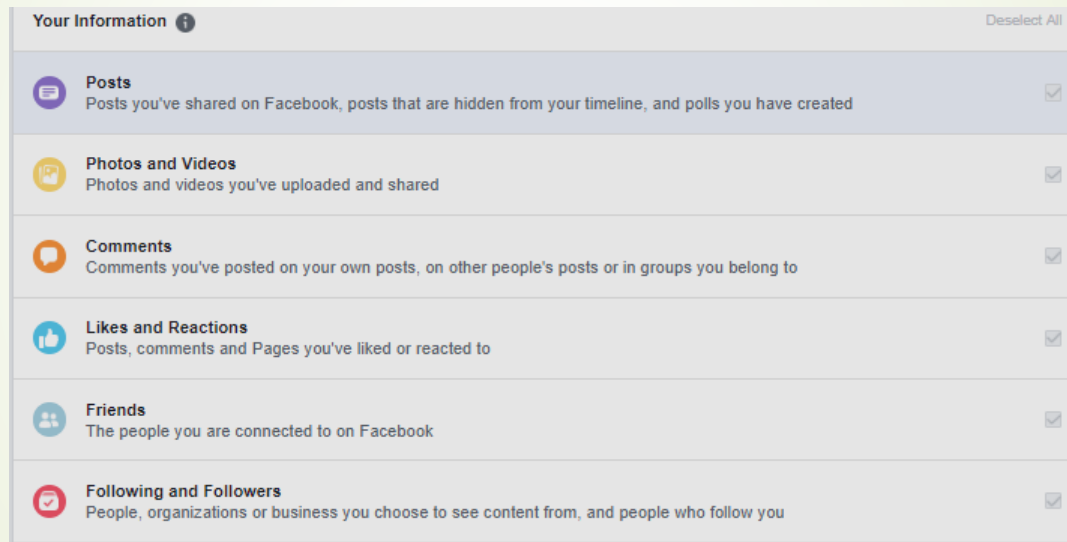
- ▶ The ethics of research.
  - ▶ Data being used way beyond how it is expected.
    - ▶ Deep neural networks being more accurate at detecting sexual orientation than humans [9].
- ▶ General Data Protection Regulation (GDPR): A policy enacted by the EU.
  - ▶ Ensures that an individual consumer's data is stored and managed in a regulated manner.
- ▶ Asking for data often not practical for millions of users.
  - ▶ Researchers should put good of users first.









# What can you do? (Facebook)

- ▶ Shared settings
  - ▶ Myself, friends, public, etc.
- ▶ Check which applications you are currently sharing data to and what exactly you are sharing.
  - ▶ Millions of applications that you may have shared with even in middle school!
- ▶ Search engine settings
- ▶ Delocalize Facebook from all other applications
  - ▶ “Log In with Facebook”
- ▶ Encrypt messages







# Information Facebook Has About You



The screenshot displays the 'Your Information' page on Facebook, which lists various types of data collected about the user. Each item includes an icon, a title, a brief description, and a checkbox indicating whether the information is selected. A 'Deselect All' link is visible in the top right corner of the list.

Category	Description	Selected
 <b>Posts</b>	Posts you've shared on Facebook, posts that are hidden from your timeline, and polls you have created	<input checked="" type="checkbox"/>
 <b>Photos and Videos</b>	Photos and videos you've uploaded and shared	<input checked="" type="checkbox"/>
 <b>Comments</b>	Comments you've posted on your own posts, on other people's posts or in groups you belong to	<input checked="" type="checkbox"/>
 <b>Likes and Reactions</b>	Posts, comments and Pages you've liked or reacted to	<input checked="" type="checkbox"/>
 <b>Friends</b>	The people you are connected to on Facebook	<input checked="" type="checkbox"/>
 <b>Following and Followers</b>	People, organizations or business you choose to see content from, and people who follow you	<input checked="" type="checkbox"/>

# Information Facebook Has About You

Information About You ⓘ		
	<b>Ads</b> Ads topics that are most relevant to you, advertisers who have collected information directly from you and information you've submitted to advertisers	<input checked="" type="checkbox"/>
	<b>Search History</b> A history of your searches on Facebook	<input checked="" type="checkbox"/>
	<b>Location</b> Information related to your location	<input checked="" type="checkbox"/>
	<b>Calls and Messages</b> Logs of your calls and messages that you've chosen to share in your device settings	<input checked="" type="checkbox"/>
	<b>About You</b> Information associated with your Facebook account	<input checked="" type="checkbox"/>
	<b>Security and Login Information</b> A history of your logins, logouts, periods of time that you've been active on Facebook and the devices you use to access Facebook.	<input checked="" type="checkbox"/>




# What can you do? (General)

- ▶ Always ask: Why do they need this information? What will this be used for? Do you really need to sign up for this application?
  - ▶ Release as little information as possible.
- ▶ As a future potential employee in the tech sector: protect users!
  - ▶ Don't gather information if you don't absolutely need it.




# Bibliography

- ▶ [1] <https://www.theatlantic.com/business/archive/2012/02/the-history-of-facebook-as-a-facebook-timeline/252390/>
- ▶ [2] <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>
- ▶ [3] <https://home.bt.com/tech-gadgets/internet/social-media/how-to-set-up-facebook-privacy-settings-11363802641202>
- ▶ [4] <https://money.cnn.com/2018/03/20/technology/aleksandr-kogan-interview/index.html>
- ▶ [5] <https://www.entrepreneur.com/article/313110>
- ▶ [6] <https://www.forbes.com/sites/emmawoollacott/2018/10/25/facebook-fined-645150-over-cambridge-analytica-scandal-and-is-told-its-getting-off-lightly/#1a39888c2c34>
- ▶ [7] <https://www.cbsnews.com/news/facebooks-promises-for-protecting-your-information-after-data-breach-scandal/>
- ▶ [8] <https://www.nature.com/articles/d41586-018-03856-4>
- ▶ [9] <https://psycnet.apa.org/doiLanding?doi=10.1037%2Fpspa0000098>
- ▶ [10] <https://www.npr.org/2018/03/21/595535935/cambridge-analyticas-role-in-trump-s-2016-campaign-raises-potential-legal-flags>
- ▶ [11] <https://www.theguardian.com/commentisfree/2018/mar/22/us-politics-data-cambridge-analytica-russia-trump>



Thank you! Questions?



# SOCIAL NETWORKS

- ADVERTISEMENTS, COOKIES AND USER SAFETY  
(SELECTED SLIDES FROM LAST YEAR)

---

Kirthana Ramesh Selvam

# Advertisements and Cookies

## First-Party Cookies

- Cookies are small files that travel back and forth between the browser and the server
- They are stored in our hard disks and will be accessed by the servers of the websites that we are return to
- In short, it makes it easy for the server to recognize that its us returning to the same site again
- Mainly used to provide a 'tailored' online experience for the user
- No Personally Identifiable Information

# Advertisement and Cookies

## **Third Party Cookies**

- These are the problematic ones
- These cookies directly flow to the Ad displaying companies
- These Ad serving companies can know what ads you have seen through your browser
- This will make sure that the user doesn't see repeated ads and will try to improve effectiveness of the campaign

# Tinder

- Formally, Tinder is a location-based social search app, according to Wikipedia
- You can swipe right or left to like or dislike a person
- Users are allowed to communicate with each other only if both parties swipe right
- This sounds safe... right?

# Tinder's Privacy Policy

- Even tinder collects cookies for targeted advertisement
- Your information from Tinder's sister companies, which are a part of the Match Group that owns Tinder is taken and used by Tinder
- As stated in the policy, data will be retained as long as Tinder needs it for legitimate business purposes

# How much data does Tinder have about a single user?

- Any guesses?

Just 800 pages!





# 800 pages of data

- Personal data
- All conversations and their locations
- General interests, like, dislikes, etc.
- Facebook likes
- Links to instagram photos
- Age ranks of partners we are interested in
- Complete Facebook friend list
- Education information
- The percentage of white/black men you have matched
- Which words you use the most
- How much time someone spends looking at your profile

# Exodus Privacy Report for Tinder

- The following trackers' signatures have been found in Snapchat:
  - Google Ads
  - Facebook Ads
  - Flurry, LeanPlum
- Out of all the Android permissions, a few things that caught my eye:
  - android.permission.GET\_TASKS
  - android.permission.BLUETOOTH
- <https://reports.exodus-privacy.eu.org/reports/54>

# Things to learn

- All those 800 pages were because of voluntary disclosure of information
- On social networking platforms, especially on something like Tinder, users are lured to disclose information, without realizing its consequences
- As discussed in this class, the best way to keep our data safe is to not provide it in the first place!
- What would happen if Tinder gets hacked?
- Just imagine the amount of data that would be exposed. Tinder now has approx. 50 million users

# Tinder's Security flaw

- Checkmarx, an application security company found out that Tinder doesn't use HTTPS to transmit pictures
- This enables hackers in the same network as the user to sniff it and even replace it with some other picture
- The adversary can also know if you swiped right or left for a particular profile and also if there is a match, by examining the lengths of the data chunk (374 bytes/ 278 bytes/ 581 bytes)
- Proof of concept video:  
<https://www.youtube.com/watch?v=ZBTL1bmJ9o8&feature=youtu.be>

# Linkability and Targeted Surveillance

- Disclosing too much information about ourselves in the social media can make it easy for adversaries to spy on us
- If we don't take care about how we expose our location information, our phone numbers, e-mail addresses, there are chances that we could become victims to targeted surveillance
- This can only be avoided when people become more aware about the entire concept of privacy!

# Social Media as Evidence

---



- Profiles
- Lists of friends, group memberships
- Chat logs
- Photos, videos
- Tags, GPS locations
- Check-ins, login timetables
- Tweets/re-tweets, direct messages, status updates, wall comments, activity streams, blog entries, etc.

# False information in Social Media

---



- Tweets from hacked accounts can affect markets, cause panic, or instigate conflict.
  - [False Tweet on AP News Feed](#)
  - [Pro-Gun Russian Bots Flood Twitter After Parkland Shooting](#)
- Cyber Bullying includes
  - the electronic posting of mean-spirited messages about a person (as a student) often done anonymously

# Reputation in Social Media

---



- Industry around managing social
  - [Article 5 Tools](#) to monitor your online
  - Reputation.com
  - Search result manipulation
  - False product and business reviews
- How to improve accuracy
  - ?





# Implications

---

## EFF Discussion

Must balance privacy and free expression rights.

# Impersonation in Social Media

---



## Catfishing

lure (someone) into a relationship by means of a fictional online persona.

Terms of Service of Social Media Sites

[Is violation a criminal act](#) – MySpace

Can one choose who they are:

[Rushdie Runs Afoul of Web's Real-Name Police](#)

Similar issues for Online Investigations

# The Social Network

---



Friend graphs disclose information about social structure  
Used for investigation of criminal activities  
Used in organizational research

[How The NSA Uses Social Network Analysis To Map Terrorist Networks](#)



# Social Engineering via Social Media

---

## Assumption – Your Friends are Your Friends

Social media can be used to gather information enabling someone else to pose as your friend

- To get you to satisfy a request

- To get you to open an attachment

Malicious code will often spread through Social Media.  
(dorkbot)

[Cyber security sleuths warn about a new malware circulating in social media](#)



## How Does Information Become Public?

- A user Posts the information himself.
- Certain Information may be publicly visible by default.
- A social network can change its privacy policy at any time without a user's permission.
- Approved contacts may copy and repost information – including photos – without a user's permission, potentially bypassing privacy settings.



## Who Can Access Information?

- Third Party Applications may access the information without your knowledge.
- Behavioral Advertising.
- Government and Law Enforcement for investigations, data collection and surveillance.





# What Laws Protect the User's Information Online?

- **Electronic Communications Privacy Act:** This Law, if updated would strengthen the requirements needed for governmental access to the data stored on a server by necessitating a search warrant
- **Children's Online Privacy Protection Act :** This Law requires that websites directed at children under 13 must limit their data collection and usage in certain ways. There are also limitations on the information that can be sent to advertisers.
- **California Online Privacy Act :** This Law requires any website that collects personally identifiable information on California consumers to conspicuously post an online privacy policy.



## So, What about

- [Confide](#)

Wired, February  
15, 2017

WIRED

Encryption Apps Help White House Staffers Leak—and Maybe Break

BUSINESS

CULTURE

DESIGN

GEAR

SCIEN

SHARE

f SHARE  
1210

TWEET

COMMENT  
18

EMAIL

# ENCRYPTION APPS HELP WHITE HOUSE STAFFERS LEAK—AND MAYBE BREAK THE LAW



CONFIDE

IN THE FOUR tumultuous weeks since President Donald Trump's inauguration, the White House has provided a steady stream of leaks. Some are mostly innocuous, like how Trump spends his solitary hours. Others, including reports of national security adviser Michael Flynn's unauthorized talks with Russia, have proven devastating. In response, Trump has launched an investigation, and expressed his displeasure in a tweet: "Why are there so many illegal leaks coming out of Washington?"





# Current Events - Facebook

---

[TECH & MEDIA A European data privacy office has 15 open investigations. Ten are about Facebook](#) -NBC News 2/27/19

The Ireland Data Protection Commission has 15 ongoing investigations of multinational tech companies, 10 being related to Facebook and its subsidiaries, WhatsApp and Instagram. These cases stem from consumer complaints that seek to determine the privacy implications of how Facebook uses its customer data for behavior analysis and targeted advertising. Overall, total consumer complaints related to privacy have increased 56% from 2018, demonstrating a new mobilization from consumers to tackle data transparency and understand how big companies are using their data. -Jacqueline Dobbas

[Facebook's promised Clear History privacy tool to launch later this year following delay](#) 2-26-2019 - Verge

This article speaks about Facebook's new privacy tool, allowing user to clear browser history. This could be a way to clear off the cookies and history collected by Facebook for its third party applications like ads. This tool would be included by this year end. -- Deepti

[Facebook's promised Clear History privacy tool to launch later this year following delay](#) - The Verge 02/26/2019

Facebook plans to release a Clear History tool that was promised in May of last year. The tool, which is to be made available later this year, is considered by Zuckerberg as a move to win back users trust after the Cambridge Analytica data leak. Releasing such a tool will undoubtedly leave a huge impact on Facebook ad business and how they generate revenue. -Abdulla Alshabanah





# Current Events - Facebook

---

## [Popular Apps Cease Sharing Data with Facebook](#) - Wall Street Journal 2/24/19

Last week, the WSJ shared that several health apps were sharing personal user information with Facebook by utilizing Facebook's SDK. Since that report was released, health apps such as Flo Period and Instant Heart Rate: HR Monitor have updated their apps to stop sharing their user's personal data and have requested that Facebook delete that data. -- Brianna Tu

## [Facebook planned to spy on Android phone users, internal emails reveal](#) - ComputerWeekly 2/22/19

Leaked documents revealed that Facebook was planning to use its Android app to target potentially single individuals (through their relationship status on FB) with dating services ads. Facebook was also planning to target its users with political advertisements and use its Android app to retrieve competitive data about how rival apps used its Facebook functions. Other revealed discussions involved how Facebook could extract user data from independently developed applications by incentivizing the developers with access to their users' Facebook data. -- Aaron Howland

## [Facebook reportedly gets deeply personal info, such as ovulation times and heart rate, from some apps](#) CNBC(Originally WSJ) 2/22/2019

Facebook receives personal sensitive data from other famous apps on the user phone. Facebook used "custom app events" to send data like ovulation times and homes that users had marked as favorites on some apps. -- Fumiiko Uehara



# Current Events - Google

---

[Senate demands Google CEO answer for hidden Nest microphone](#) - CNET 2/27/2019

The article discusses about how Google had failed to mention that there was a microphone in their Nest security devices in any of their specifications for the device. Google says this was an error and also that they never turned the microphone on. The article further talks about the dangers of this, highlighting the fact that consumers should know exactly what kind of hardware is in their devices so they can take measures to maintain personal privacy.

~Ahmed Qureshi

[Google sets April 2 closing date for Google+, download your photos and content before then](#) USA TODAY – 2/2/2019

Google+, which was launched as a competitor to Facebook in 2011, will be shut down and deleted its service on April 2 of this year. A few months after Facebook's Cambridge Analytica incident, Google+'s customer information was leaked due to a security bug. Google's reputation suggests that the reason for Google+'s service shut down is due to a decrease in usage. – Sophia Choi



# Current Events

---

## [TokTok fined for children privacy violation](#)

Federal Trade Commission (FTC) announced that the famous app/service TikTok is fined about 5.7M USD for violating children's privacy laws. TikTok allegedly illegally collected personal information from children by not obtaining their parents' permission before they signed up. 13 years or below shouldn't ideally be on a social media platform. Yet a large percentage of Musical.ly users were under the age of 13. This \$5.7 million fine is the largest civil penalty ever in a children's privacy case. The violation is glaring because TikTok is a social media popular among teens and it ended up breaching children's privacy laws. Further actions are expected on this if things escalate. -- Kavya Sethuraman

## <https://techcrunch.com/2019/02/27/musical-ly-tiktok-fined-5-7m-by-ftc-for-violating-childrens-privacy-laws-will-update-app-with-age-gate/>

The TikTok video-creating and sharing application is facing a hefty fine for its violation of U.S. Children's Privacy Laws. The app requires users to enter personal information upon the creation of an account and collects this data for users under the age of 13, this is not permitted without parental consent. As a result, the app is making changes to provide a more restricted experience for younger users. -- Ann Bailleul

## [Instagram is leading social media platform for child grooming](#) 03/01/19

Instagram's platform use accounts for a third of the cases of child grooming. A fifth of the victims were 11 years old and younger. Numerous groups have called out various social media platforms for failures of child safety, data protection, and spread of misinformation. - Chloe Choe



# Current Events

---

## [Fake LinkedIn Job Offers used for Backdoors](#) – Security Intelligence 2/27/19

This article explains how users are being tricked into downloading the “More\_eggs” backdoor. User’s in industries that take online payments are the primary targets. Users are tricked into downloading Word documents that will begin to download the malware as soon as macros are enabled. This malware can then be used to download malware of different variety. -Jairo Hernandez

## [Could hackers 'brainjack' your memories in future?](#) - 2/19/2019 BBC

The US Defence Advance Research Projects Agency (DARPA) is attempting to work on "wireless and fully implantable neural interface" to restore memory loss in soldiers caused by traumatic brain injury. The article explains that this effort can lead to future threats of hackers "brainjacking" someone's brain by erasing or overwriting memories or controlling neurostimulators of patients with Parkinson's disease and altering the configurations. It would also be possible for them to steal credit card information and PIN numbers as these information can be obtained by analyzing someone's brainwaves. -- Yulie Felice

## [The Australian Parliament's Anti –Encryption Law Opening Doors to Potential Cyber Attacks](#) eHackingNews 02/28/2019

This article discusses a recent law that been approve by Australian Parliament giving national intelligence and law enforcement agencies access to end-to-end encrypted communication. It was vocally opposed by many cyber and technology organizations; however, the bill still passed. -- Joseph Mehlretter

## [Thailand passes controversial cybersecurity law that could enable government surveillance](#)

The bill was criticized for vagueness and the potential to enable sweeping access to internet user data. One clause to search and seize data and equipment in cases that are deemed issues of national emergency. The citizens fear that the law could be weaponized by the government to silence critics. – Louis Uuh



# Current Events

---

[Can Social Media Be Saved?](#) - Kevin Roose – New York Times 3/28/18

Our growing discomfort with our largest social platforms is reflected in polls. One recently conducted by Axios and SurveyMonkey found that all three of the major social media companies — Facebook, Twitter and Google, which shares a parent company with YouTube — are significantly less popular with Americans than they were five months ago. The primary problem with today's social networks is that they're already too big, and are trapped inside a market-based system that forces them to keep growing. Facebook can't stop monetizing our personal data for the same reason that Starbucks can't stop selling coffee — it's the heart of the enterprise. -- Gene Zakrzewski

Four in 10 people have deleted a social media account in the past year due to privacy worries - CNBC Lucy Handley 6/18/18

Privacy concerns and the circulation of fake news are contributing to people's distrust of content on social platforms, said the study by public relations consultancy Edelman. Context was also seen as important by people surveyed, with 48 percent saying it's a brand's fault if its advertising appears next to hate speech or violent content. The Cambridge Analytica data leak and Russian-produced fake news that undermined the 2016 U.S. Presidential Election have contributed to people's concerns. -- Gene Zakrzewski

[Apple fixes Group FaceTime privacy issue with iOS 12.1.4, macOS Mojave supplemental update](#)

Feb 7, 2019 · Apple has released an update to iOS bringing it up to 12.1.4, and a supplemental update to macOS Mojave with both updates re-enabling Group FaceTime by fixing a security hole that potentially allowed others to listen in to private conversations without the user's permission.- Helena Salimi



# Current Events

---

## [Social Media Post Revealing NATO Activities](#) - New York Times 2/21/2019

In a NATO training exercise, researchers were able to discover and gain key information about NATO soldiers via Instagram, and Facebook, giving them timely information on the dates of the exercises, and the movements of battalions. They used both publicly posted pictures and posts on social media by soldiers along with fake accounts/pages to get this information from their targets. The article also states that Russia has recently voted to block troops from using smartphones and posting about their military service. Would this be a beneficial stance for NATO to take as well? - Lance Aaron See

## [Nato Group Catfished Soldiers To Prove A Point About Privacy](#) - WIRED 02/18/19

A NATO research group, the Strategic Communications Center of Excellence (StratCom), conducted a catfishing operation to see how much information they could tease out of US military personnel. The researchers set up phony Facebook pages and invited military personnel to join closed Facebook groups. In addition to social engineering, this study looked at fraudulent page, profile and group detection and removal by Facebook. - Sevanti Nag

## [TWITTER IS SECRETLY HOLDING ONTO DELETED DIRECT MESSAGES](#) - Independent 02/18/19

A researcher accidentally found out that Twitter keeps direct messages between users after they are deleted. Twitter's privacy policy states that when an account is deactivated, the data will be deleted after 30 days. However, it is possible to restore the account after that period which indicates that Twitter indeed keeps the messages and data. Log data that Twitter collects like IP address and browser type is kept for a maximum of 18 months, the policy states. Abdullah Altokhais



# Current Events

---

## [A New Data Protection Bill Aims to Tackle Racial Ad Targeting](#) - Fortune 2/28/2019

Known as the DATA Privacy Act, a bill introduced by a senator in Nevada, Catherine Cortez Masto, authorizes the Federal Trade Commission to outline specific definitions of discriminatory practices in online advertising and data collection. The bill is especially relevant as investigations have found that advertisers are able to exclude racial groups from viewing specific ads. The practices of discrimination against people are based on race, gender, sexuality, etc. The DATA Privacy Act will require businesses to provide users with opt-in and opt-out consent options, according to a press release obtained by Fortune. – Mindy Huang

## [Nevada senator takes on racial ad targeting in new privacy bill](#) - The Verge 02/28/2019

Senator Catherine Cortez Masto is introducing a bill that would explicitly bar platforms like Google and Facebook from serving targeted ads that discriminate against protected groups, particularly by race, sexual orientation or gender. This Act will put in specific definitions for discriminatory behavior in targeted ads and increase FTC's civil penalty authority for violation of these rules. Facebook was found to allow discriminatory targeting in 2016 and removed several ad categories in response. A year later, it was found that it is still possible to have discriminatory ads on Facebook. --Anupama

## [What the U.S. Can Learn From the EU's Privacy Laws](#) - Adweek 3/1/2019

Considering GDPR being the biggest privacy topic of 2018. The California Consumer Privacy Act (CCPA) has been taking similar GDPR steps in its roadmap, but the important concern is if it will be as successful as GDPR. Many US publishers have taken the shortcut and blocked EU traffic, and their websites are unavailable for EU citizens. If similar restrictions in the US are officially published and require such enforcement, what will those publishers do? - Faris Almathami