

Facebook

Facebook requires that users be who they say they are, which allows the company to remove suspicious users and fake accounts, but that has not stemmed the tide of fake news, violence, and hate speech that has been one of the more controversial aspects of the site.

Facebook Controversies

Many major controversies stem from privacy and issues and concerns and scandals, where Facebook has made the supposedly private data of users available to advertisers and analysts.

Scams

- Scam ads
- Hidden statistics about people viewing your profile
- Look at this embarrassing video of you!
- Shocking news & headlines

Retaining users' deleted videos (2018)

Even if a user deleted their video, it still remained on Facebook's servers.

Data-Breaches 2018-2019

- June 2013: personal data of 6 million users (1%) exposed
- May 2018: private posts of 14 million users (1%) made public
- September 2018: attackers gained access to 50-90 million user (2-4%) accounts
- March 2019: 600 million (25%) passwords saved in plaintext
- April 2019: 540 million (22%) records found on a public server
- April 2019: Facebook harvested email contacts of 1.5 million new users
- September 2019: 419 million (17%) user ID, phone number full name, gender, location found on an exposed server
- December 2019: 309 million (12%) phone numbers, names, user IDs found on an exposed server

The percentage in parentheses is the percent of users affected of all active Facebook users at that time.

Scraping Public Profiles

At one point this data could have included: email address, phone number, location, attended events, liked pages, groups, photos, and all public comments and posts. This data can then be linked to all other kinds of public records (ie voter records) as well as behavior on other websites.

Apps Sharing Personal Data (- 2019)

- Apps shared data with FB, including private health information like women's periods and pregnancy attempts.
- Apps shared this data with FB even if the user **DID NOT** have a FB account.

Rohingya (2018-2019)

- Hate speech against the Rohingya in Sri Lanka (March 2018)
- Hate speech in India (2019)
- Incitement of Genocide against Rohingya in Myanmar (2018)

Facebook Algorithm and “Censorship”

Censorship is defined as the suppression of words, images, or ideas that are deemed offensive. Usually, censorship involves imposing personal, political, or moral values onto others. The first amendment was drafted to protect free speech from governmental interference. *It does not apply to private organizations or individuals.* (Emphasis mine)

- Community moderators are generally outsourced to other countries (Manila)
- Automatically ban pictures of things like breasts (even in historical artwork and photos)
- [Algorithm](#) populates news feed (not your interests)
- Activists are often suspended for *pointing out* hate speech and racism

Categories of speech that fall outside protection are:

- hate speech
- child pornography
- defamation / slander
- incitement to violence
- true threats of violence.

Is Facebook now a quasi-public space? Chuck Johnson lost a similar case against Twitter.

Russian Meddling

Russians created thousands of social media accounts pretending to be Americans, paid for Facebook ads during the 2016 campaign that reached 126 million FB users. These ads were not just pro-Trump and anti-Clinton, but aimed at manipulating Democratic voters as well, with campaigns to skip voting or use bogus voting methods. See also: Cambridge Analytica.

Cambridge Analytica (2014-2018)

Readers took a “personality” survey through a downloaded app, which also scraped data from their profile AND the profiles of their friends. Only 270k users took the survey and consented to data harvesting, however [Cambridge Analytica](#) collected data on over 50 MILLION users.

- 2016 US Election (Trump, Cruz)
- Brexit Vote
- 2018 Mexican General Election (IDP)

We also got access to census data. Unlike developing nations with less stringent privacy controls, the U.S. government won't provide raw data on specific individuals, but you can get information, down to the county or neighborhood level, on crime, obesity, and illnesses such as diabetes and asthma. A census block typically contains six hundred to three thousand people, which means that by combining many sources of data, we could build models that infer those attributes about individuals. For example, by referencing risk or protective factors for diabetes, such as age, race, location, income, interest in health food, restaurant preference, gym membership, and past use of weight-loss products (all of which are available in most U.S. consumer files), we could match that data against aggregated statistics about a locality's diabetes rates. We could then create a score for each person in a given neighborhood measuring the likelihood that they had a health issue like diabetes—even if the census or consumer file never directly provided that data on its own.

-- Wylie, Christopher. *Mindf*ck* (p. 72). Random House Publishing Group. Kindle Edition.

Facebook Tracking

You've probably noticed that when you shop for something on one website, ads in Facebook immediately appear for whatever it is you were just looking for. This is not a coincidence but it's not black magic either. In short, it comes down to primarily two things (there are others, but these are the important ones): unique identifiers and web cookies.

Unique Identifiers

If you want to understand how to make your online presence more secure and more private, you need to understand the basics of how companies collect and collate your data in the first place.

When you log into Facebook, your login credentials require your email address. This email address is your [unique identifier](#).

How do companies use this to collect information? Because this email address is associated only with you, every time this email address appears in an advertiser database, it can be directly linked to your Facebook account. So if you use the same email address for everything, all data you have shared with each of those companies *could* become aggregated into a single file.

Web Cookies

In electronic terms, cookies are not a delicious baked good, but are instead bits of code that hold information about what you are doing. Cookies are what allow you to place an item in your online shopping cart, browse around for other items, and then purchase all those items at one time. Without cookies, the web would not be particularly interactive, because your information could not be saved from one page view to another.

Unfortunately, cookies can be used by “third parties” to track what you are doing, and Facebook does a lot of this. If you see a Facebook “Like and Share” button on a web page, then Facebook is collecting information about what you are doing on that page.

Facebook collects this information **whether you have a Facebook account or not.**

Facebook collates and uses this information **whether you have a Facebook account or not.**

Libra Cryptocurrency

In May 2019, Facebook announced it was attempting to start a [cryptocurrency](#) with several other corporations (Visa, PayPal, eBay, MasterCard) that they hoped will be used globally instead of credit cards and bank accounts. This would be a big deal for Facebook, because they could then become the place where people go to send money online and shop.

Unlike other cryptocurrencies, which can rapidly fluctuate in value, Libra is supposed to be backed by reserves, so its value should remain relatively stable. It would also (unlike current cryptocurrencies) be built into Facebook and Whatsapp, so it should be simple to use.

There are a lot of possible issues with this, starting with the compliance systems used by banks to put a check on illegal uses, such as money laundering, tax avoidance, and terrorist financing. Another problem is that if Libra becomes part of the global economy, who would be responsible for bailing it out in the case of theft? There are also issues of national security and the flow of money across borders—how would Libra keep users from sending money to North Korea or other restricted countries? Another area which might be easily overlooked is that in the US we have a general prohibition between banking and commerce.

Imagine Facebook's subsidiary Calibra knowing your account balance and your spending, and offering to sell a retailer an algorithm that will maximize the price for what you can afford to pay for a product. Imagine this cartel having this kind of financial visibility into not only many consumers, but into businesses across the economy. Such conflicts of interest are why payments and banking are separated from the rest of the economy in the United States.

-- Launching a Global Currency Is a Bold, Bad Move for Facebook, Matt Stoller, New York Times, 2019-06-19

And Yet...

Despite these issues, Facebook does have the potential to be a force for good, allowing people to remain in contact across distances in a manner that was unimaginable a half century ago. It has also been useful in emergencies, allowing affected individuals to “check in” and let friends and family know they are safe, which could help to reduce some of the burden on phone lines and cell towers during such times.

Making Your Facebook Use More Secure

Here are the top things you can do to make using Facebook safer:

- Do **NOT** use the Facebook [app](#) on your phone. Use a [web browser](#) on your phone instead.
- Do **NOT** use the Facebook Messenger app on your phone.
- Install a browser on your computer / device that you **ONLY** use for Facebook.
- Go through all your Facebook privacy settings.
- Do **NOT** use Facebook to log into other websites; create credentials for every site.
- Regularly remove third-party apps that have permissions to your account.
- Use privacy and security [add-ons](#) to restrict access to your browsing history.
- Create and use an email account that is unique for Facebook.

Using Facebook

Facebook looks (and sometimes works) differently, depending upon whether you are using a computer or a mobile device. And the Facebook app does not look the same on [iOS](#) devices as it does on [Android](#) devices.

The rest of the document is divided into parts: Facebook on a computer, the Facebook app on an android device, and the Facebook app on an iOS (apple) device. All tables of contents in this handout are hyperlinks, so you can jump directly to the section you need.

At the end of the documents are various glossaries and references to help you translate a little bit of what you'll see online.

Facebook Tracking	3	Facebook App on iOS	27
Using Facebook	5	News Feed.....	27
Facebook Website on a Laptop (or Desktop)...	6	Emoticons	35
News Feed.....	6	Acronyms	36
Messenger.....	14	Technology Glossary.....	37
Facebook App on Android.....	17	References.....	47
News Feed.....	17	Index	50

Facebook Website on a Laptop (or Desktop)

News Feed

Your News Feed displays posts from family and friends as well as groups and businesses you have liked and/or followed. The News Feed is the main part of Facebook—it's what you see when you first log into the website.

You have two options to make minor modifications to this. One is to hide posts by specific groups or individuals, and the other is to toggle see first for specific pages or individuals.

Hiding Posts

1. Click on the ellipse (...) beside the post that offends you.
2. From the menu, select your desired option.

Hide post

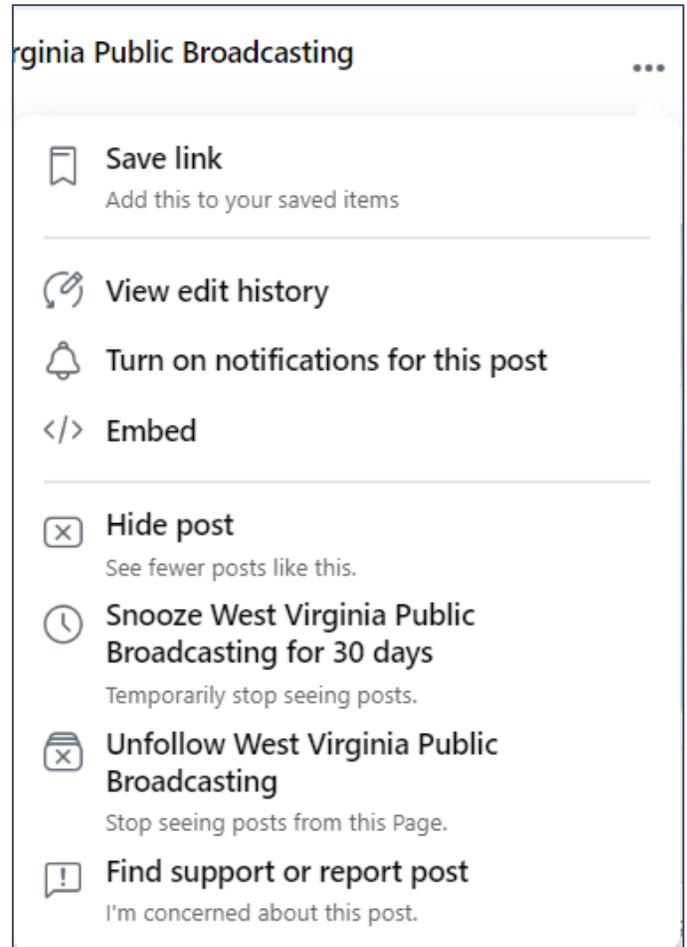
Hide this specific post from your wall / news feed. This is good if you want to ignore a single, specific post.

Snooze for 30 days

Hide posts from this person for a month. This is something that is useful in the month before an election.

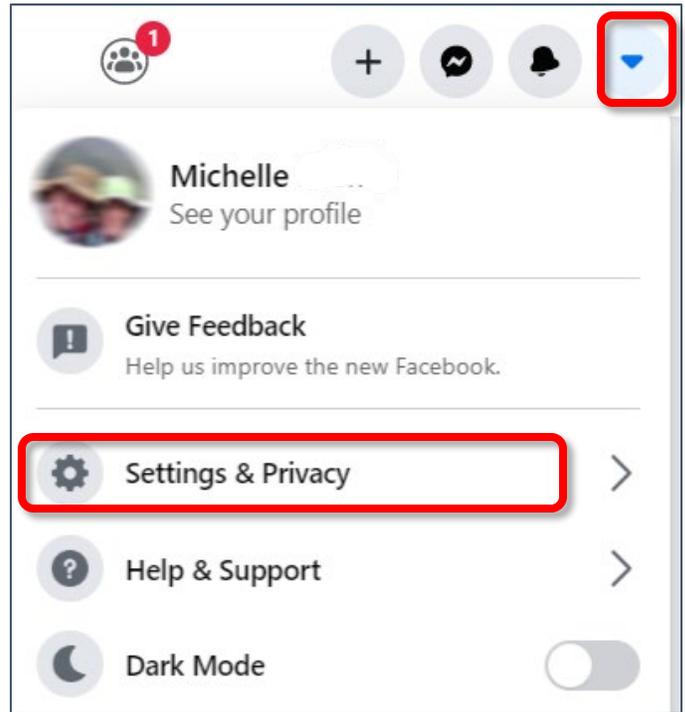
Hide all from / Unfollow

This allows you to stop seeing posts from someone, but still remain friends with them; you can see their posts by going to their wall.

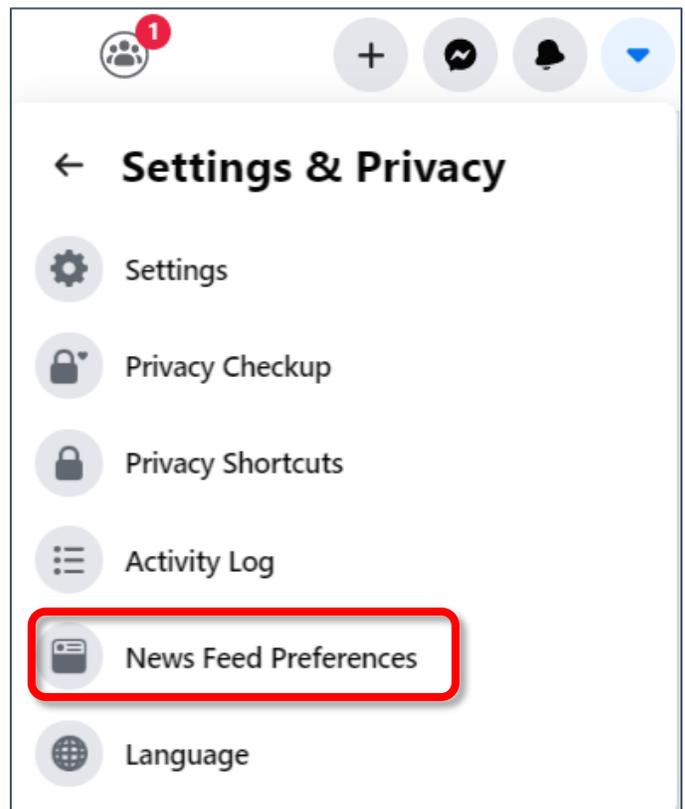


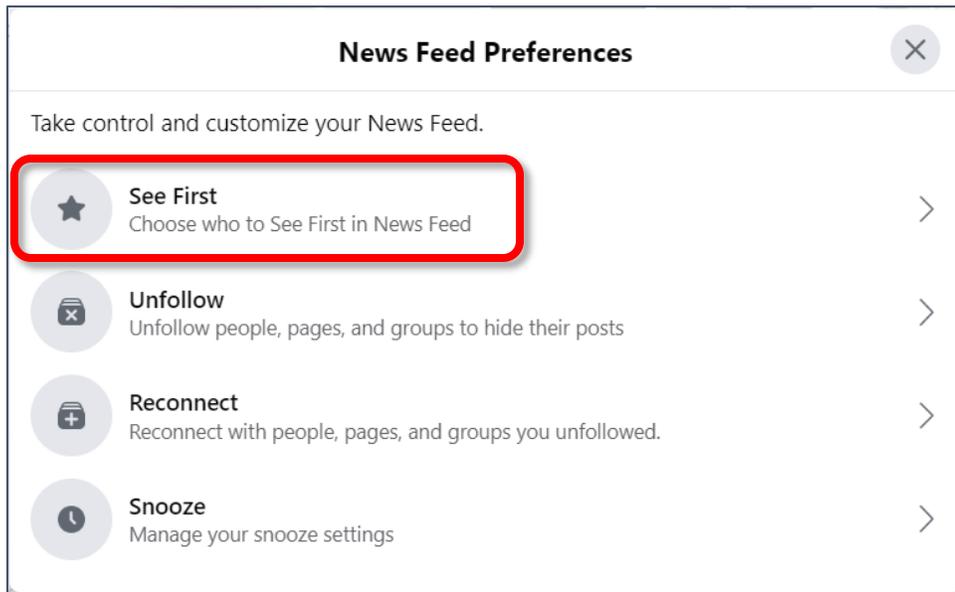
News Feed Preferences

1. In the top right corner of the Facebook window, click the triangle.
2. From the drop down menu select **Settings and Privacy**.

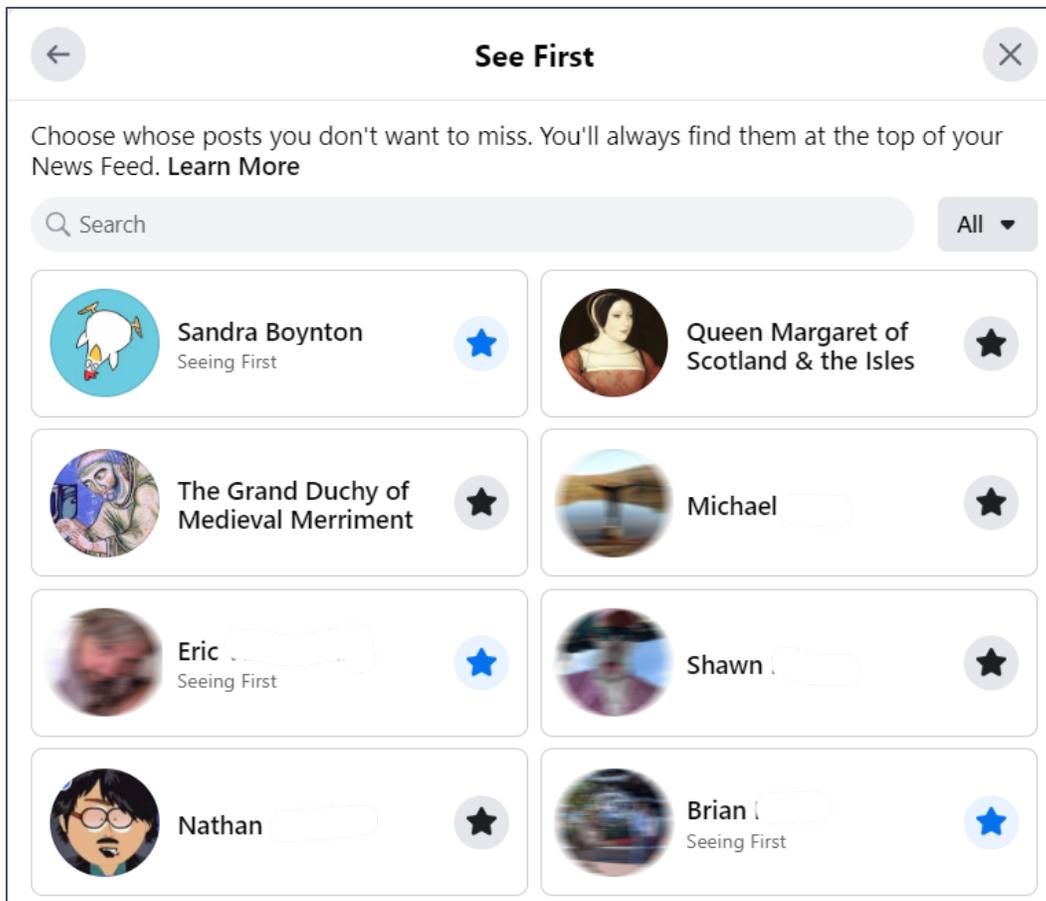


3. In the Settings & Privacy section, select **News Feed Preferences**.





4. In the News Feed Preferences dialog box, select on **See first**.



5. Click on the picture of someone whose posts you want to make sure you see. **Seeing First** appears under their name.
6. Once you're finished, click the left point arrow in the top right corner.

Posts

There are typically two ways you can post to your timeline: writing a post, or sharing a post from another person or group. When you create or share something on your timeline / wall, that post is displayed on your wall.

Anything you post on your wall—even something you are sharing from someone else’s wall, gets its own comment section on your wall. This means that comments you make on posts on other people’s walls will not appear on your wall.

Public vs Friends vs Groups

Your posts can have four levels of accessibility: public, friends, specific friends, and only me.

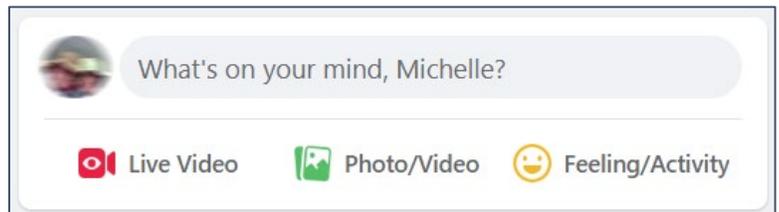


Posting something to the public means that anyone in the world who access Facebook can see what you posted. Friends means that the post will be visible to everyone in your friends list. Selected Friends posts are displayed to a group or a handful of friends. Only Me is precisely what it sounds like.

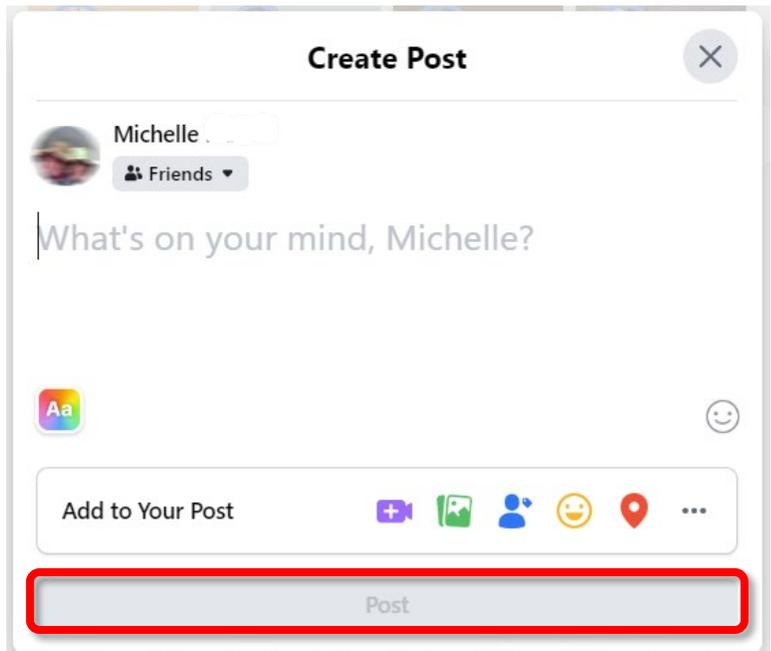
If you change the post visibility when you are creating the post, that setting will “stick” and be the setting for all posts going forward. You do have the ability to change the visibility of a post after it has been created, and in usually this is easier than trying to remember to change the visibility the next time you post.

Writing Posts

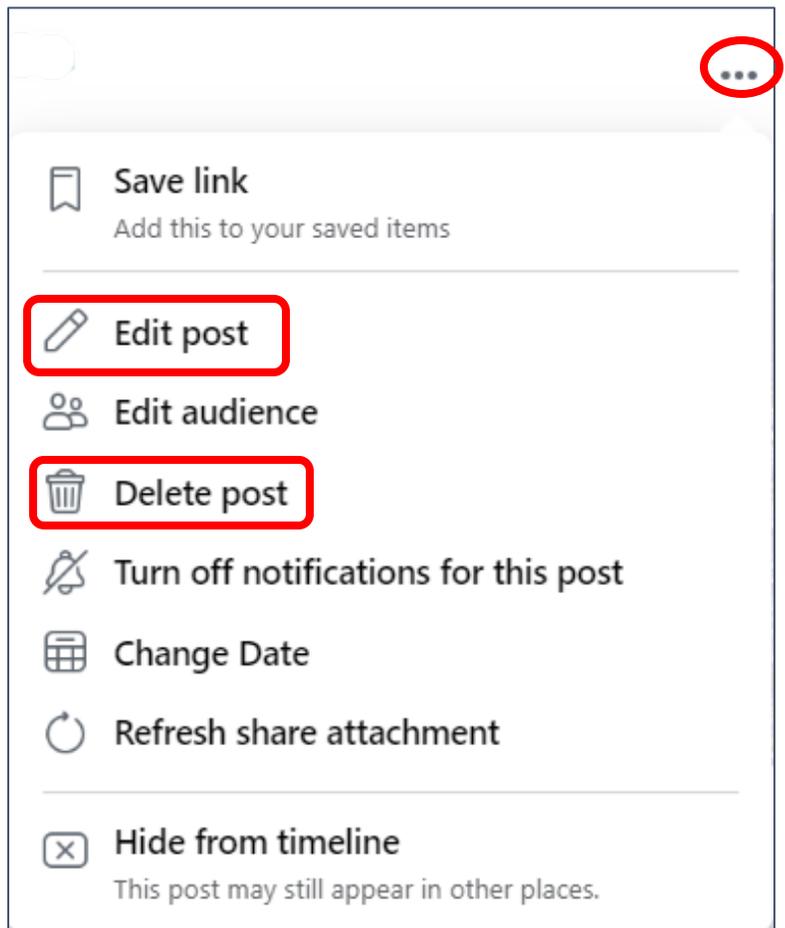
1. In your newsfeed or on your profile, click in the post area.



2. Type what you want to say. Click the links to add pictures, tag friends, or add emoticons. Once you've added everything, click **Post**.



3. Once you have created a post, you have the option to edit or delete what you posted. In the top right corner of your live post, click the **ellipse (...)**.
4. From the menu that appears, select the desired option.
5. These options are also available on comments you make to others posts.

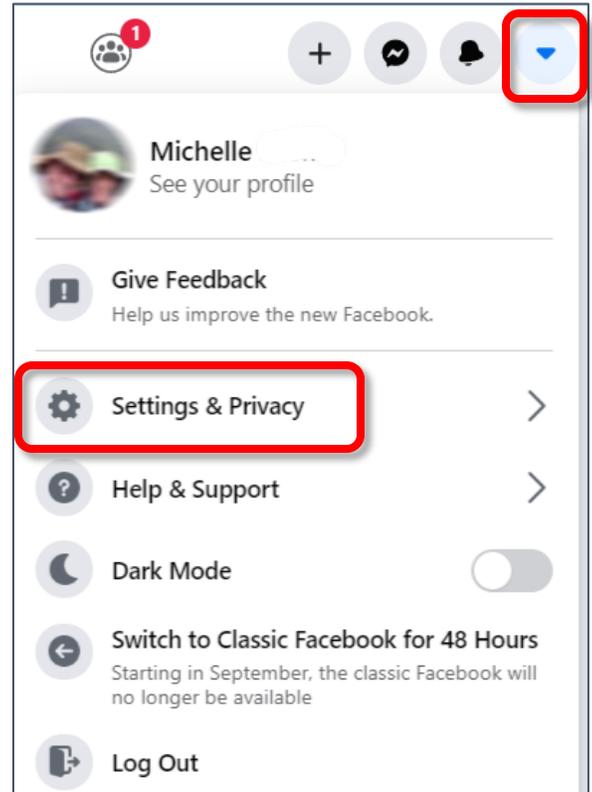


Settings

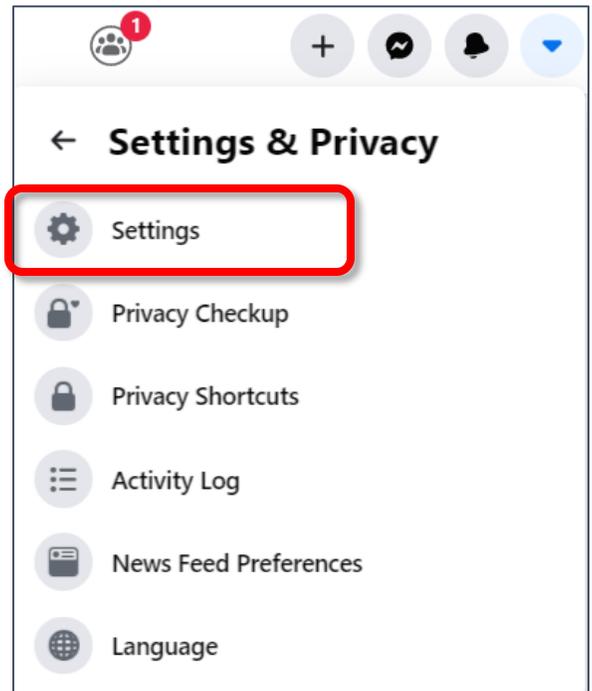
Settings are where you will go to check on your privacy and security, as well as to do things like tweak your notifications.

Accessing Your Facebook Settings

1. In the top right corner of the Facebook window, click the triangle.



2. From the menu, select **Settings**.



Privacy

1. Open your Facebook **Settings**.
2. In the left pane, select **Privacy**.

Who can send you friend requests?

Setting this to Friends of friends limits the audience of people who can make friend requests, however, it means that if you don't have friends in common, you can't receive a friend request from someone.

Who can see your friends list?

Unless you know someone famous, Friends of friends is a reasonable choice.

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

Do you want your Facebook page to come up in a google search of your name? My answer is no. You have to decide this for yourself.

Timeline and Tagging

1. Open your Facebook settings.
2. In the left pane, select **Timeline and Tagging**.
3. Change the toggles to restrict who can see your posts to your desired options.

Who can post on your timeline?

This allows you to restrict who want write on your wall / timeline. If you have family members who passive-aggressively share things on your timeline, restricting this might be useful.

Who can see posts you're tagged in on your timeline?

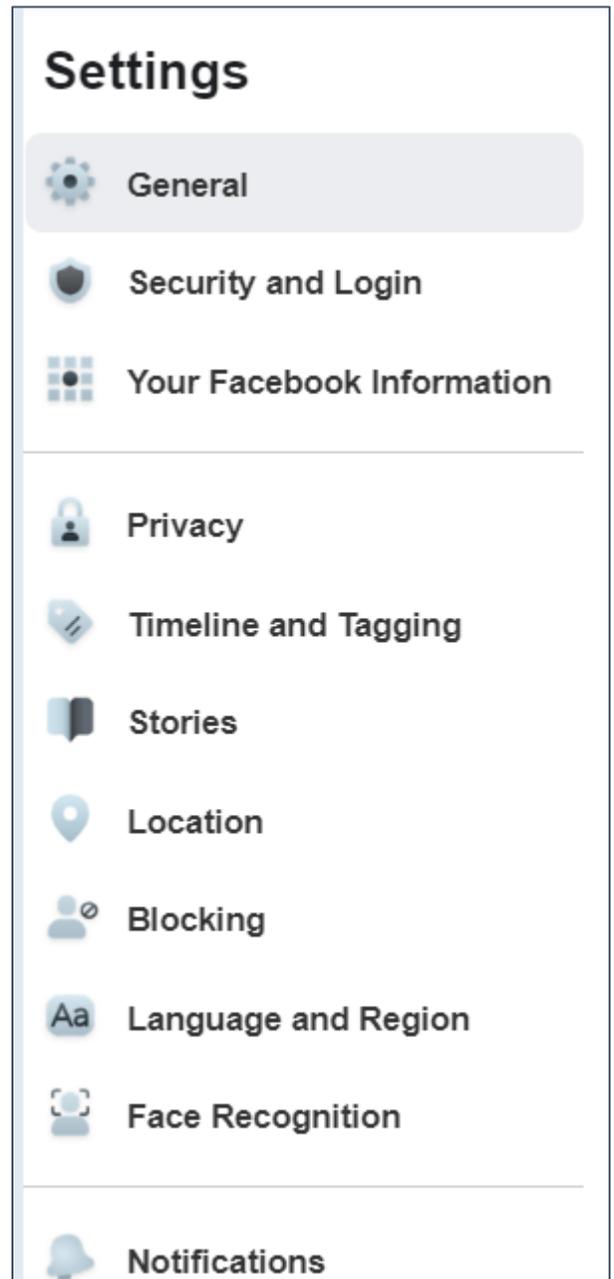
If someone tags you in a post, who do you want to see that post?

Review posts you're tagged in before the post appears on your timeline?

If someone tags you in a post, do you want to OK it before other people can see it?

Face Recognition

1. Open your Facebook settings.
2. In the left pane, select **Face Recognition**.
3. On the right side of the window, click on **Edit**.
4. Change the toggle from Yes to **No**. Click **Close**.



Off-Facebook Activity

Facebook has a privacy / security setting that allows you to see how you are being tracked by third parties when you are not actively using the Facebook site. I highly recommend you peruse and clear this list.

https://www.facebook.com/off_facebook_activity

Location History

Location history is for the Facebook app on your mobile device. Through the website you can toggle it on or off

Notifications

Notifications are updates you can receive about what has happened on Facebook. By default, Facebook wants you to know ABSOUTELY EVERYTHING ALL THE TIME. This is designed to keep you using Facebook, and can be overwhelming. You can turn these various notifications off, or allow some notifications but not others.

- **Red Alert Notifications:** Notifications that appear above the bell icon. When you have a new notification, a red bubble will appear with the number of new notifications you've received.
- **Email Notifications:** Notifications you receive via email. Facebook sends a message to your email to let you know you have been tagged in a post or something similar.
- **Push Notifications:** Notifications that appear when you're not actively using Facebook.

Notifications Settings

What Notifications You Receive

 **Comments**
Push only ▲

These are notifications for comments on your posts and replies to your comments.

Where you receive these notifications

	Push	On <input checked="" type="checkbox"/>
	Email	Off <input type="checkbox"/>
	SMS	Off <input type="checkbox"/>

 **Tags**
Push only ▼

Pruning Facebook Notifications

1. Open your Facebook settings.
2. In the left pane, select **Notifications**.
3. Go through all your notification settings and turn off various notifications.

Apps within Facebook

As we saw with the Cambridge Analytica scandal, Facebook apps have disseminated your data in ways you probably are not comfortable with. It's important to see what apps have access to your information, and to remove apps that are not integral to your Facebook experience.

Seeing Your Facebook Apps

1. Open your **Settings**.
2. Along the left side of the page, select **Apps and Websites**.
3. The display shows you all the apps you have given permission to view your profile.
4. To view the permissions an app has to your profile, click **View and edit**.
5. The permissions for the selected app appear in a menu. You will see there are some options you can toggle off, and some you cannot.
6. Once you are finished making any changes, click the **Save** button.

Removing Apps

1. In the list of active apps, find the app you want to remove.
2. To the right of the app is a very faint check box. Click inside that box to select the app (or apps) to be deleted.
3. Click the **Remove** button.
4. A dialog box opens making sure you want to remove the app. Place a **check** in the box beside the text asking if you want to delete all posts, photos and videos.

Click **Remove**.

Messenger

Using Facebook Messenger generally gives people the ability to see if you are online. I do not recommend using the Facebook Messenger App on your mobile device, for privacy and security reasons, so we're going to look at FB messenger in the web browser.

Facebook Chat Options

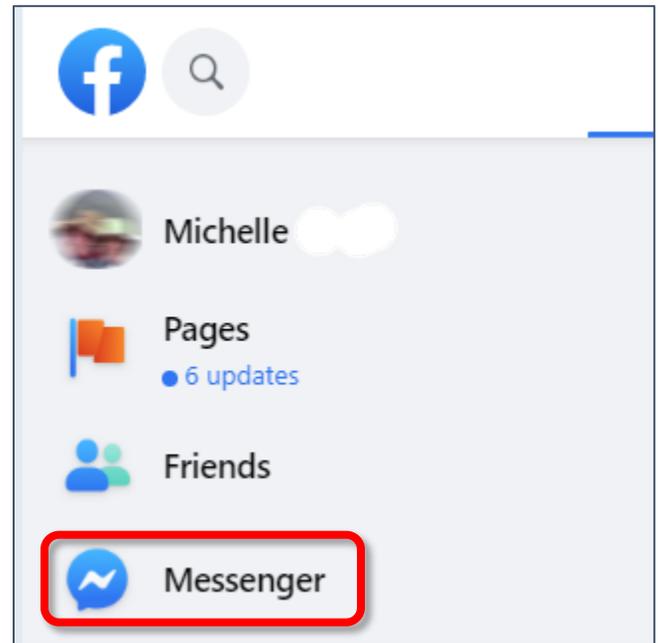
One of the ways Facebook pushes you to use Facebook Chat / Messenger is by putting it right in your face. Luckily, you can close your chat box and turn off your active status. This will keep people from knowing when you are online.

Using Facebook Messenger in Your Browser

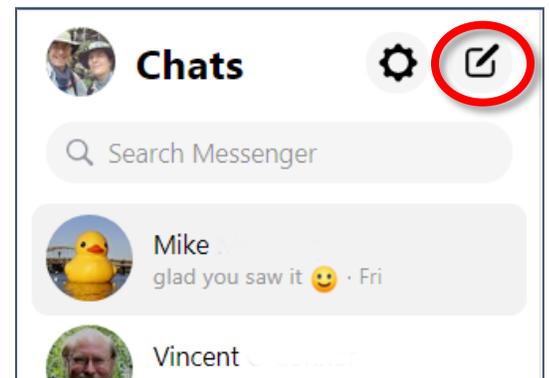
If you are not using the Messenger app or the chat box, Facebook is going to make it more annoying for you by forcing you to go to a separate page. Just keep in mind that Facebook is making things less easy precisely so you will use the app. Although it is not as convenient, I recommend having private conversations through a messaging app, such as Skype or Signal.

Using Messenger in Your Browser

1. In the top left corner of the Facebook window, beneath your news feed, click on the **Messenger** link.

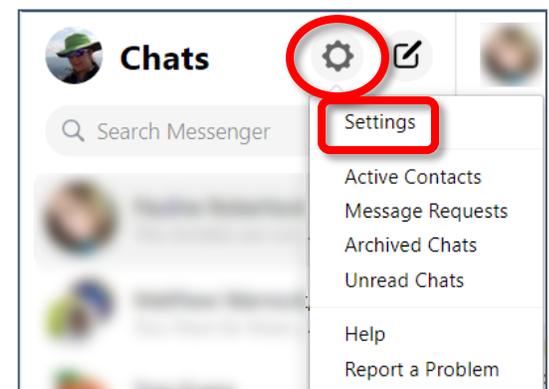


2. A list of ongoing chats appears in the left pane. Click on any chat to add to the message thread.
OR
Click the **New Message** icon to create being a new chat.

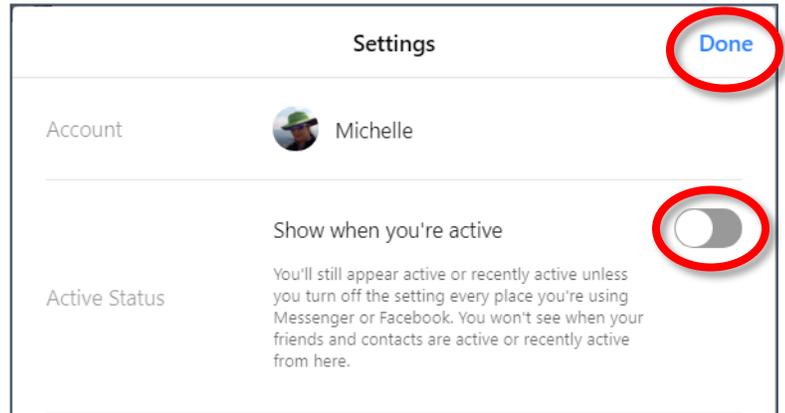


Turning off Active Status

1. Open Messenger.
2. Click the **Options** (gear) icon
3. From the drop down menu, select **Settings**.

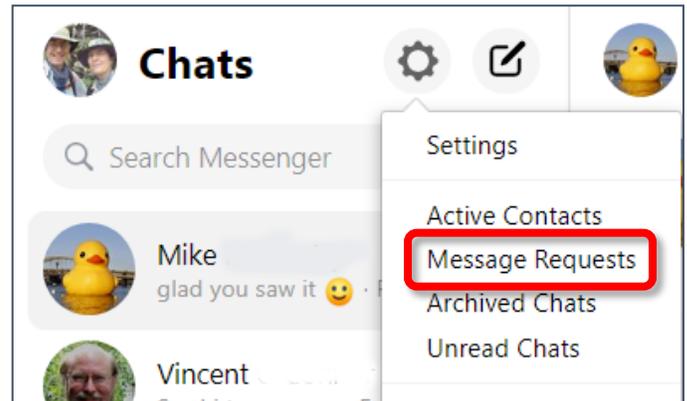


4. Toggle **Show when you're active**.
5. Click **Done**.

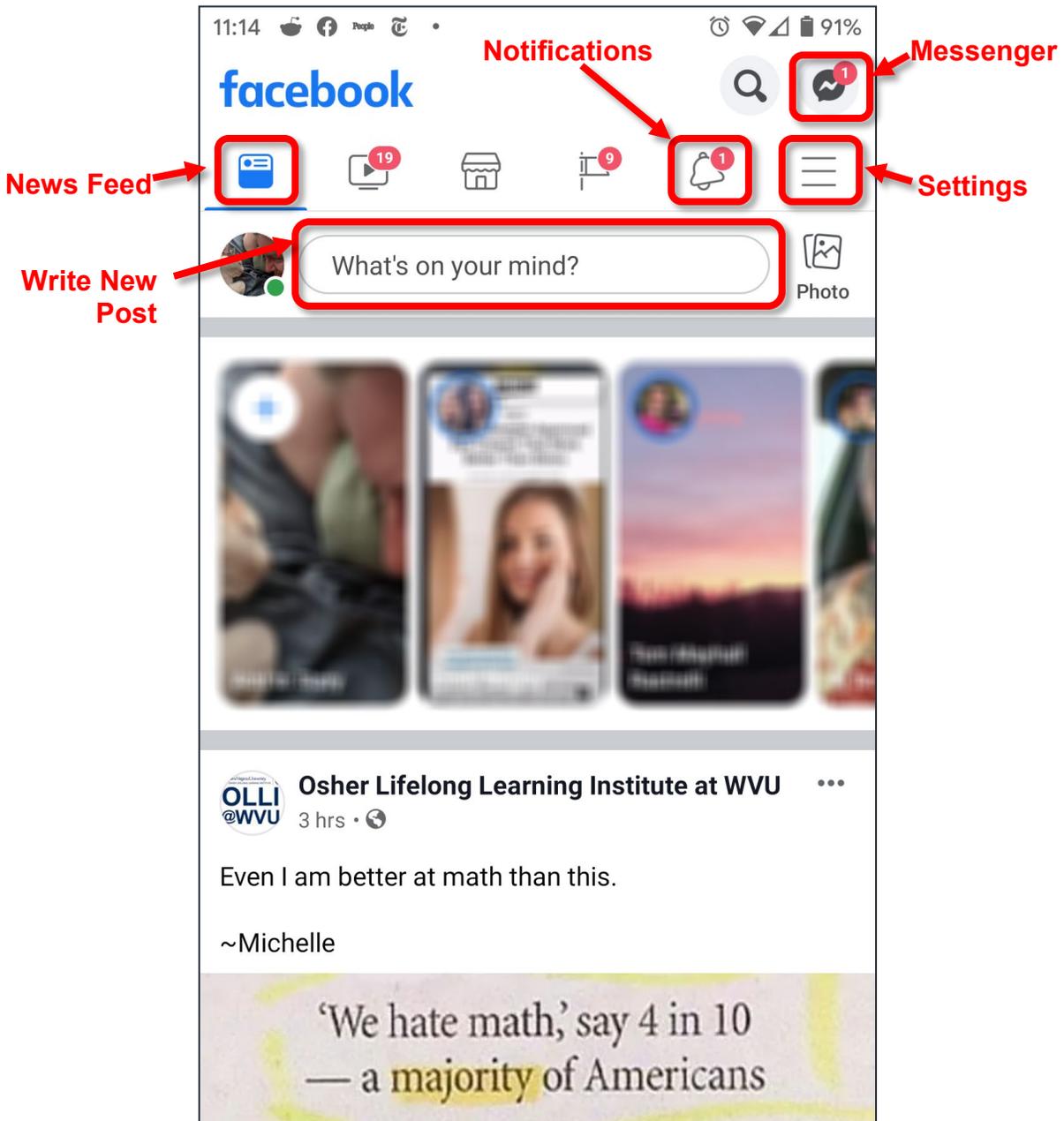


Finding Missed Chat Messages

1. If you are not already a friend with someone, Facebook hides those conversations in a folder called **Message Requests**.
2. Check this folder occasionally to see if anyone has tried to contact you.



Facebook App on Android



News Feed

Your News Feed displays posts from family and friends as well as groups and businesses you have liked and/or followed. The News Feed is the main part of Facebook—it's what you see when you first log into the website.

You have two options to make minor modifications to this. One is to hide posts by specific groups or individuals, and the other is to toggle see first for specific pages or individuals.

Hiding Posts

1. Click on the ellipse (...) beside the post that offends you.
2. From the menu, select your desired option.

Hide post

Hide this specific post from your wall / news feed. This is good if you want to ignore a single, specific post.

Snooze for 30 days

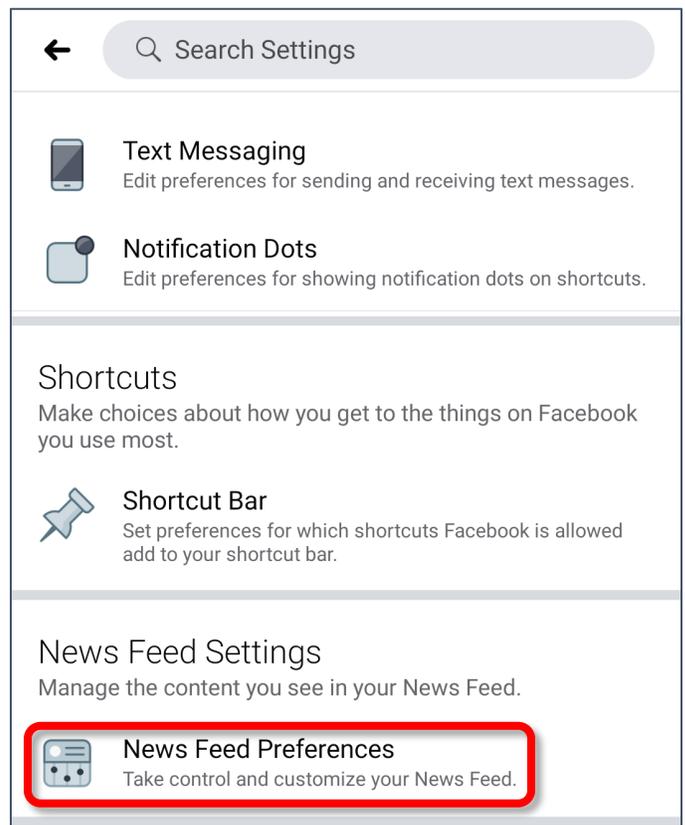
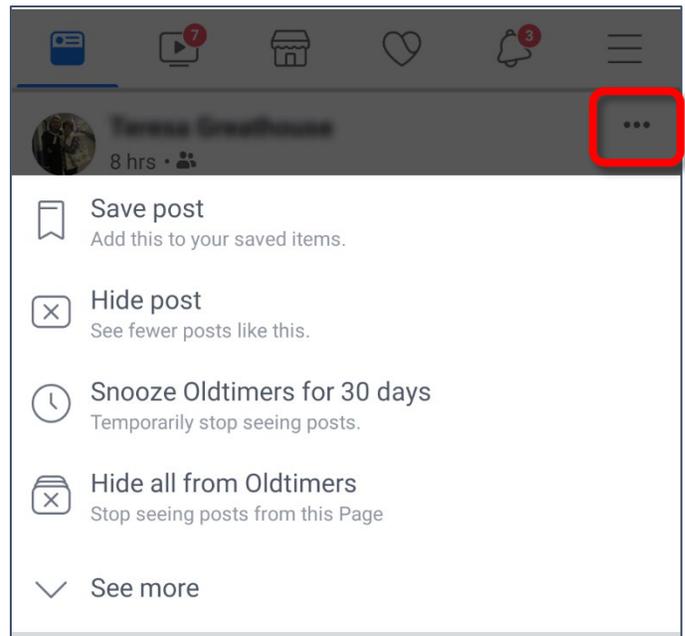
Hide posts from this person for a month. This is something that is useful in the month before an election.

Hide all from / Unfollow

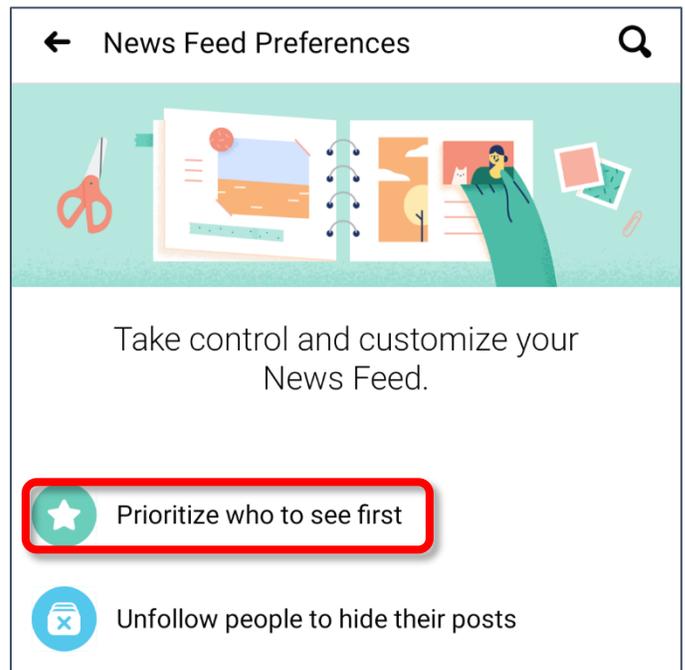
This allows you to stop seeing posts from someone, but still remain friends with them; you can see their posts by going to their wall.

News Feed Preferences

1. In the upper right corner of the Facebook window, tap the three parallel lines for **Settings**.
2. From the menu tap **Settings & Privacy**.
3. Tap **Settings**.
4. Scroll down until you see **News Feed Preferences**.

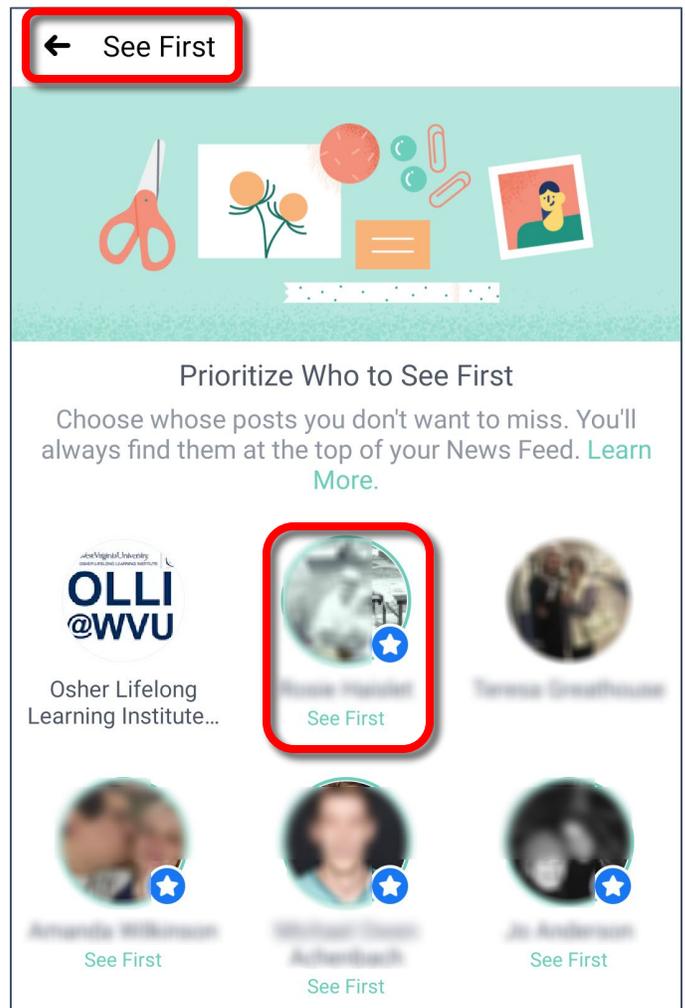


5. Tap **Prioritize who to see first.**



6. Tap on the picture of someone whose posts you want to see first. A blue **See First** is displayed under their name and a star appears on the profile picture.

7. Once you're finished, tap **See First** at the top of the screen or tap Android's **Back** button.



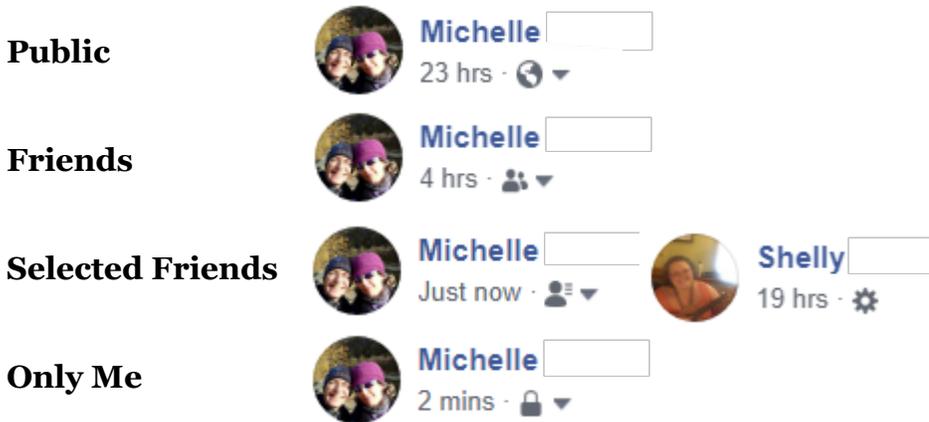
Posts

There are typically two ways you can post to your timeline: writing a post, or sharing a post from another person or group. When you create or share something on your timeline / wall, that post is displayed on your wall.

Anything you post on your wall—even something you are sharing from someone else’s wall, gets its own comment section on your wall. This means that comments you make on posts on other people’s walls will not appear on your wall.

Public vs Friends vs Groups

Your posts can have four levels of accessibility: public, friends, specific friends, and only me.

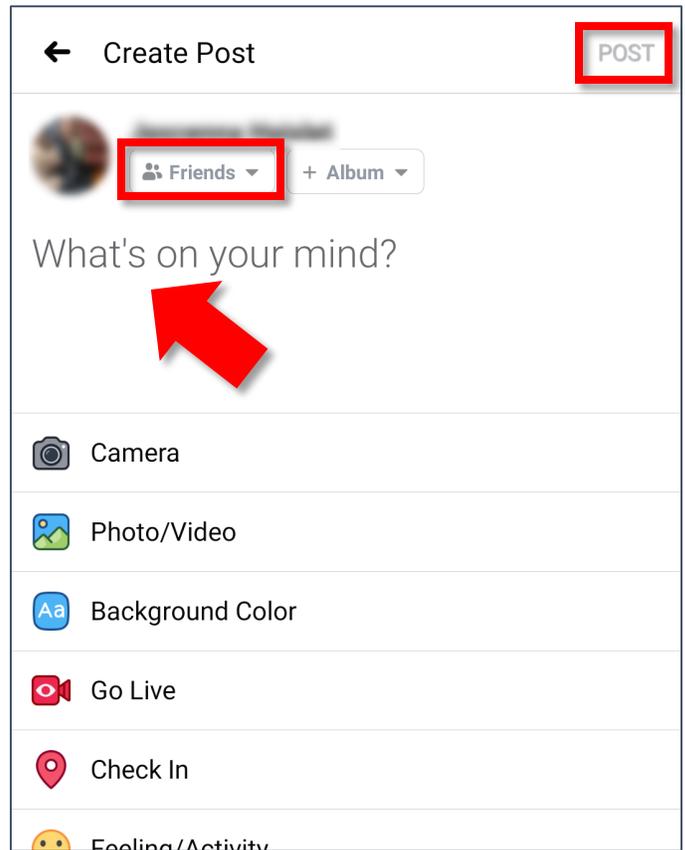


Posting something to the public means that anyone in the world who access Facebook can see what you posted. Friends means that the post will be visible to everyone in your friends list. Selected Friends posts are displayed to a group or a handful of friends. Only Me is precisely what it sounds like.

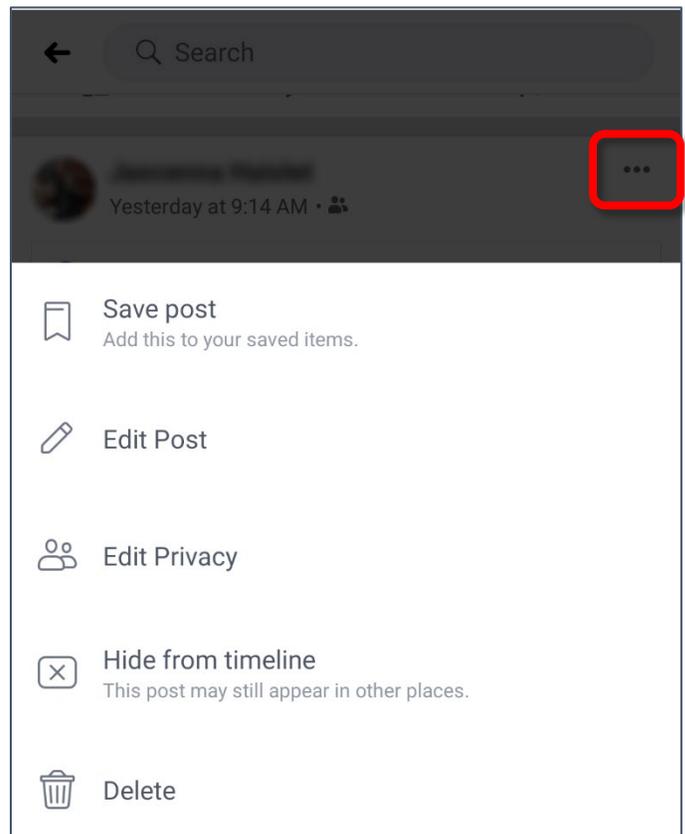
If you change the post visibility when you are creating the post, that setting will “stick” and be the setting for all posts going forward. You do have the ability to change the visibility of a post after it has been created, and in usually this is easier than trying to remember to change the visibility the next time you post.

Writing Posts

1. In your newsfeed or on your profile, tap in the post area.
2. Type whatever you want to say. Tap the links to add pictures, tag friends, or add emoticons. Once you've added everything, tap **Post** in the top right corner.



3. Once you have created a post, you have the option to edit or delete what you posted. In the top right corner of your live post, click the **ellipse (...)**.
4. From the menu that appears, select the desired option.
5. The ellipse is also available to edit or delete comments you make to others' posts.

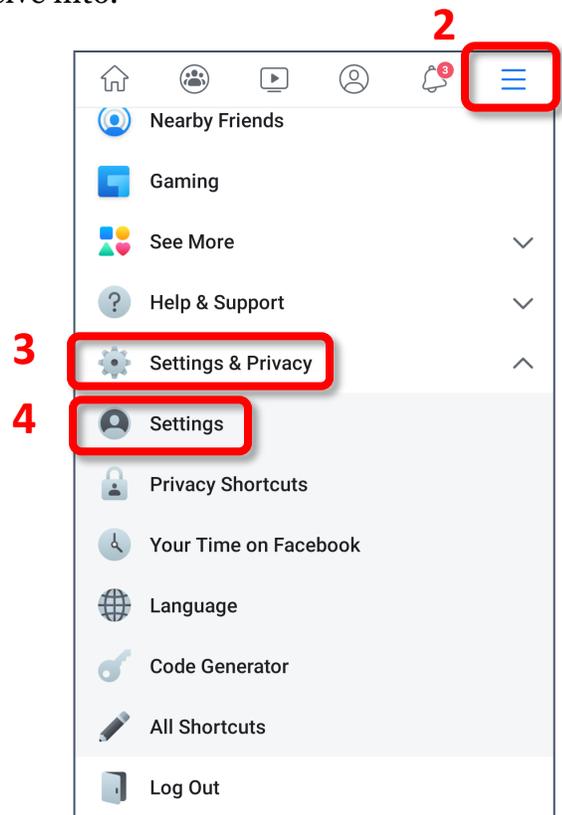


Facebook Settings

Obviously, my first recommendation is to NOT use the Facebook app on your phone, but if you are going to use the app, there are definitely settings you should delve into.

Accessing Facebook Settings

1. Open the Facebook app.
2. In the upper right corner, click the three parallel lines to access the available menu options.
3. Scroll down through the list until you see **Settings & Privacy**.
4. The menu expands out, select **Settings**.



Privacy Settings

1. Open your **Settings**.
2. Scroll down to the **Privacy** section.
3. Tap on **Privacy Settings**.
4. Make changes to your settings as desired.

Who can send you friend requests?

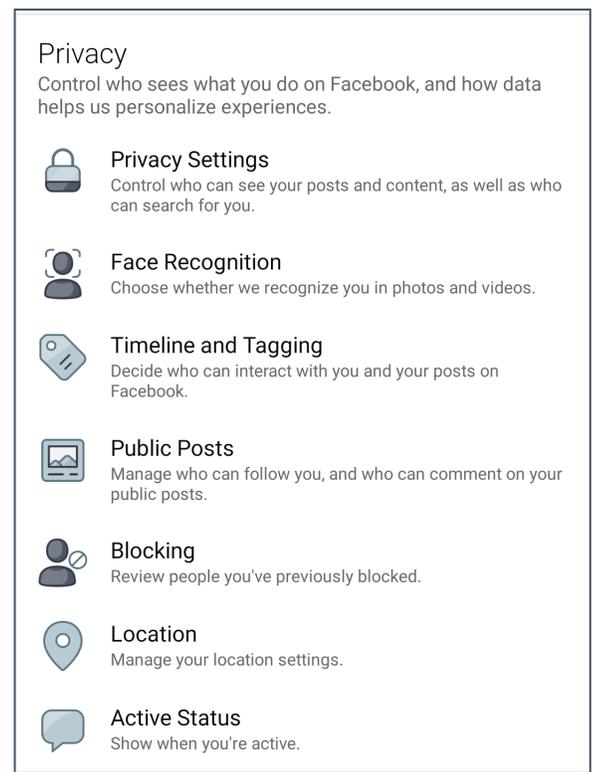
Setting this to Friends of friends limits the audience of people who can make friend requests, however, it means that if you don't have friends in common, you can't receive a friend request from someone.

Who can see your friends list?

Unless you know someone famous, Friends of friends is a reasonable choice.

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

Do you want your Facebook page to come up in a google search of your name? My answer is no. You have to decide this for yourself.



Timeline and Tagging

1. Open **Settings**.
2. Scroll down to the **Privacy** section.
3. Tap on **Timeline and Tagging**.
4. Make changes to your settings as desired.

Who can post on your timeline?

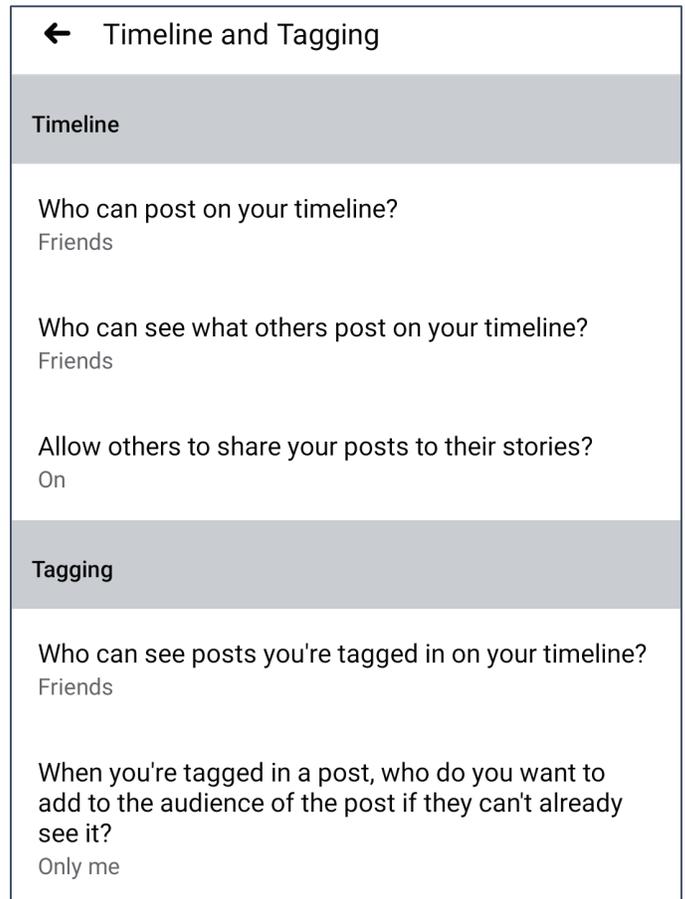
This allows you to restrict who want write on your wall / timeline. If you have family members who passive-aggressively share things on your timeline, restricting this might be useful.

Who can see posts you're tagged in on your timeline?

If someone tags you in a post, who do you want to see that post?

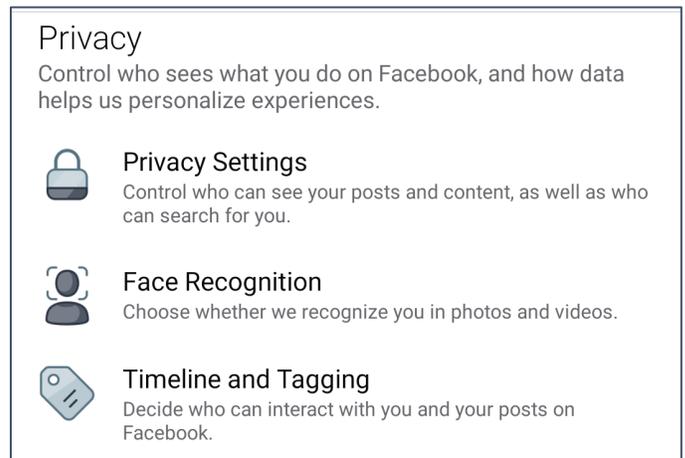
Review posts you're tagged in before the post appears on your timeline?

If someone tags you in a post, do you want to OK it before other people can see it?



Face Recognition

1. Open your **Settings**.
2. Scroll down to the **Privacy** section.
3. Tap on **Face Recognition**.
4. Toggle on or off.



Off-Facebook Activity

Facebook has rolled out a new privacy / security setting that allows you to see how you are being tracked by third parties when you are not actively using the Facebook site. I highly recommend you peruse and clear this list.

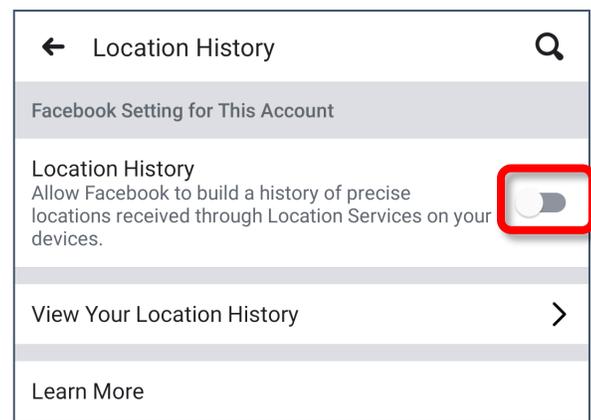
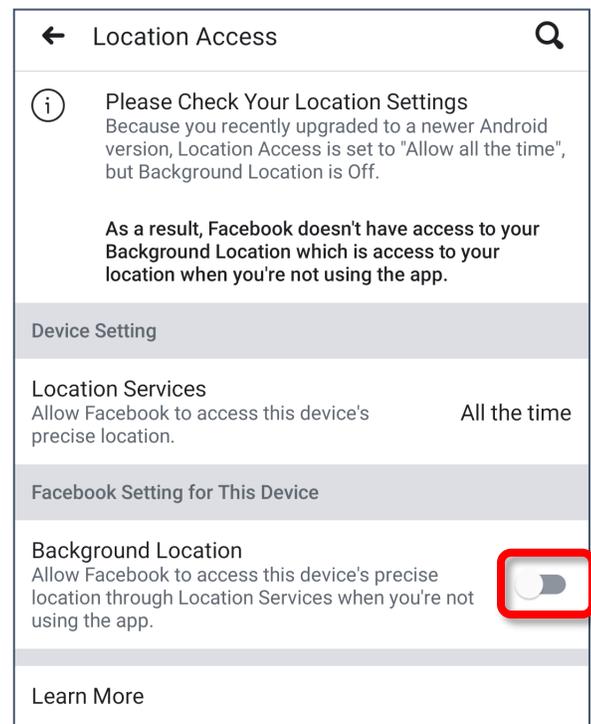
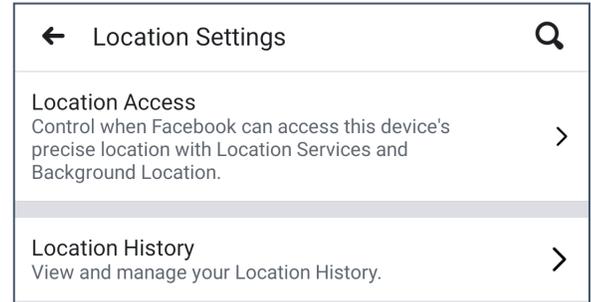
https://www.facebook.com/off_facebook_activity

Location Settings

In general, unless you use Check-in, there is no reason to allow Facebook to know your location. I recommend turning all location settings off. If this setting has been on, assume that Facebook knows precisely where you live, and all the places you frequently visit, including the homes and family members and your favorite stores.

Accessing Your Location Settings

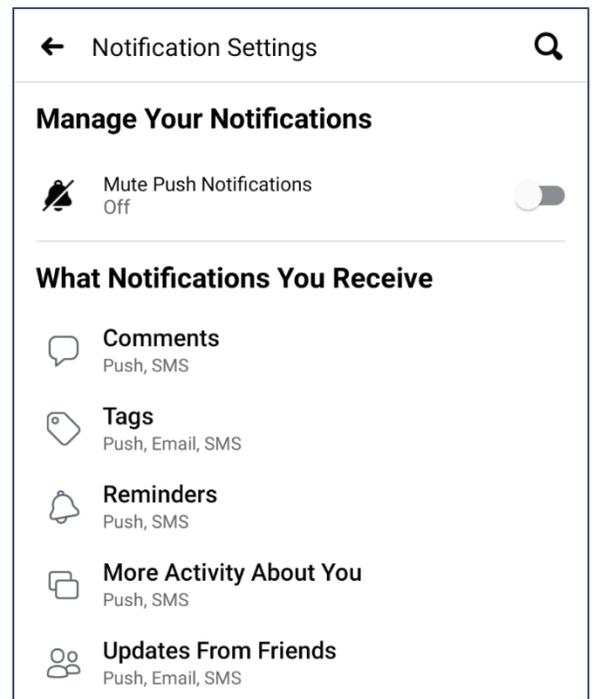
1. Open your **Settings**.
2. Scroll down to the **Privacy** section.
3. Select **Location**.
4. Open **Location Access**.
5. Facebook will act like it is vitally important it knows where you are at all times. It is **NOT**.
6. Toggle **OFF** the setting to give Facebook **Background Location**. Facebook definitely does NOT need to know where you are when you are not using the app.
7. Select **Location Services** (under Device Setting) and change this setting to **Never**. Or if you use Check-in, you can set it to when you are actively using the app. But I highly recommend **Never**.
8. You should also clear your location history and tell Facebook is cannot build a location history. This won't change what information Facebook has used in the past, but it will keep Facebook from using your location going forward.



Notifications

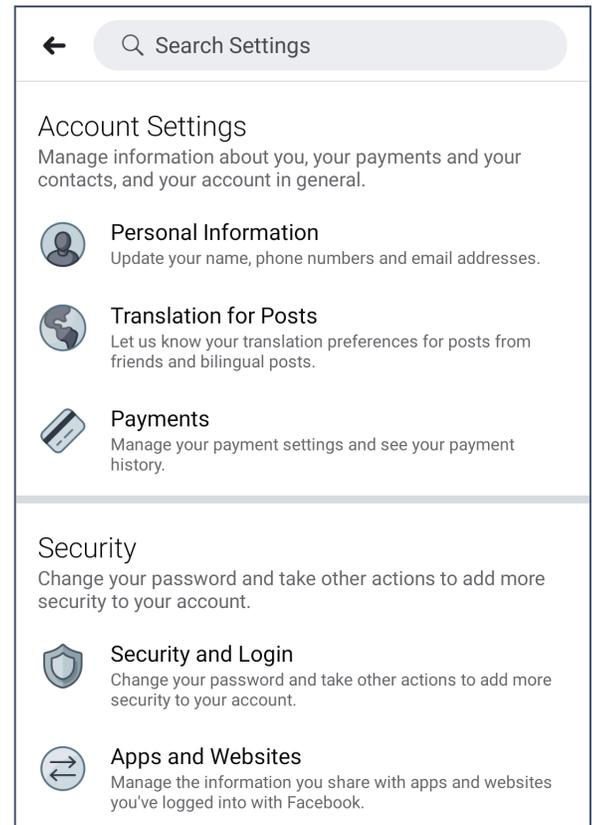
Notifications are updates you can receive about what has happened on Facebook. By default, Facebook wants you to know ABSOUTELY EVERYTHING ALL THE TIME. This is designed to keep you using Facebook, and can be overwhelming. You can turn these various notifications off, or allow some notifications but not others.

- **Red Alert Notifications:** Notifications that appear above the bell icon. When you have a new notification, a red bubble will appear with the number of new notifications you've received.
- **Email Notifications:** Notifications you receive via email. Learn more about email notifications.
- **Push Notifications:** Notifications that appear when you're not actively using Facebook. Learn more about mobile and desktop push notifications.

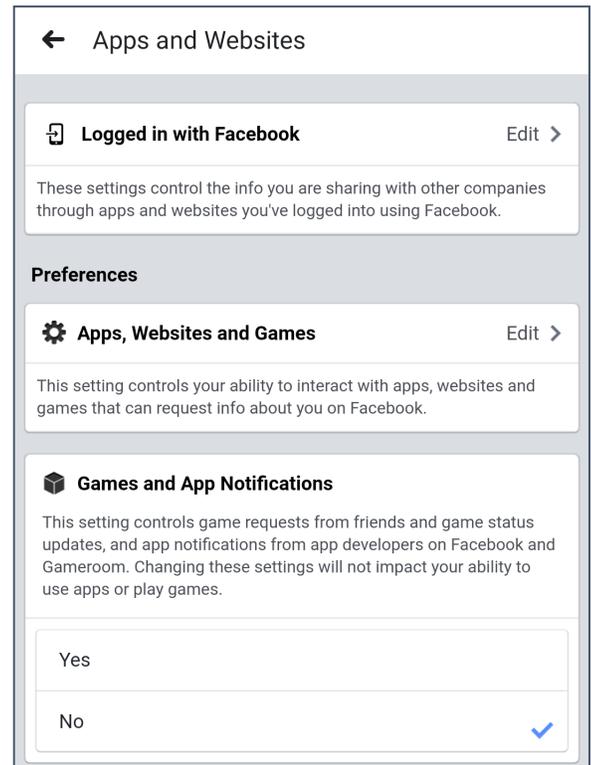


Apps within Facebook

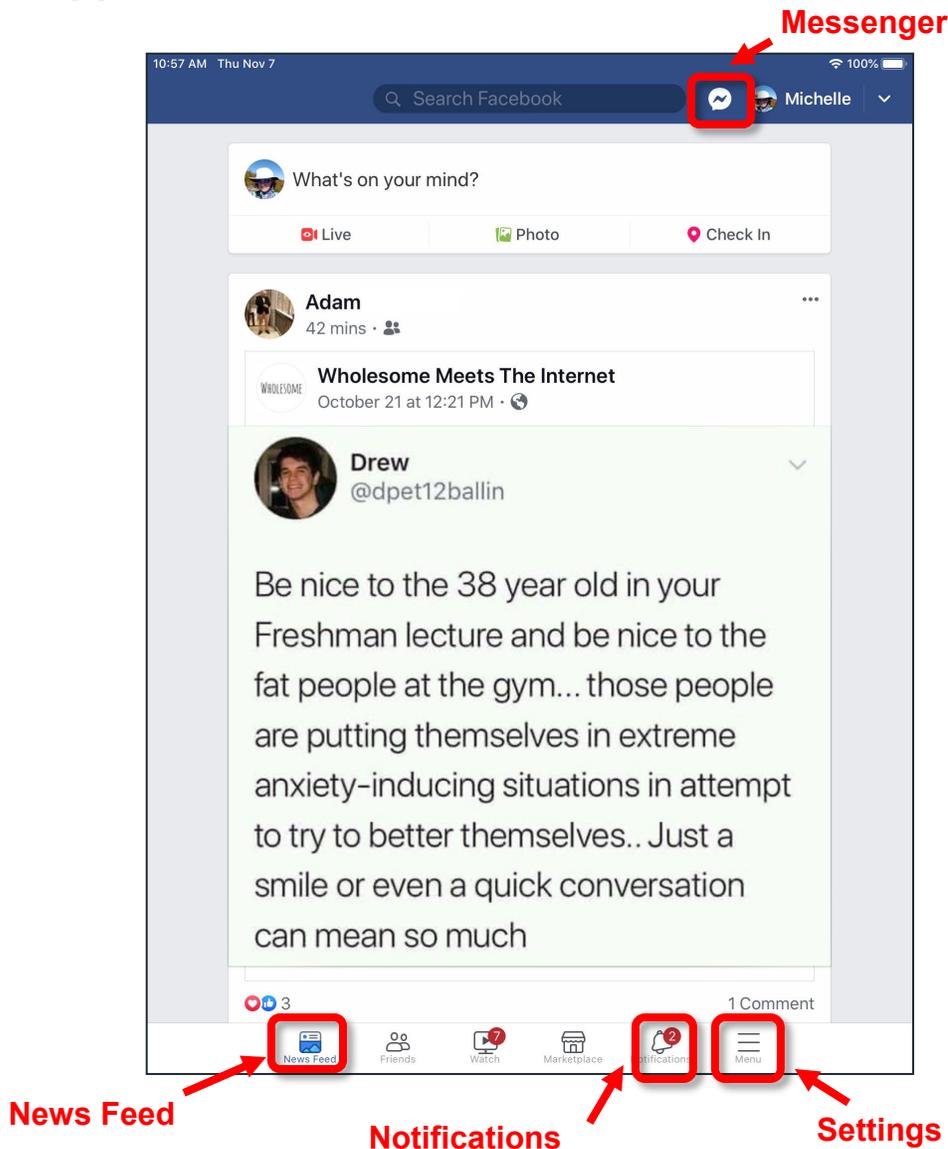
1. Open your **Settings**.
2. Scroll down and then select **Apps and Websites**.



3. Check each of these settings to see what (if any sites) you have logged into with using your Facebook credentials.
4. Check and see what (if any) apps have been given permission to your profile.



Facebook App on iOS



News Feed

Your News Feed displays posts from family and friends as well as groups and businesses you have liked and/or followed. The News Feed is the main part of Facebook—it's what you see when you first log into the website.

You have two options to make minor modifications to this. One is to hide posts by specific groups or individuals, and the other is to toggle see first for specific pages or individuals.

Hiding Posts

1. Click on the ellipse (...) beside the post that offends you.
2. From the menu, select your desired option.

Hide post

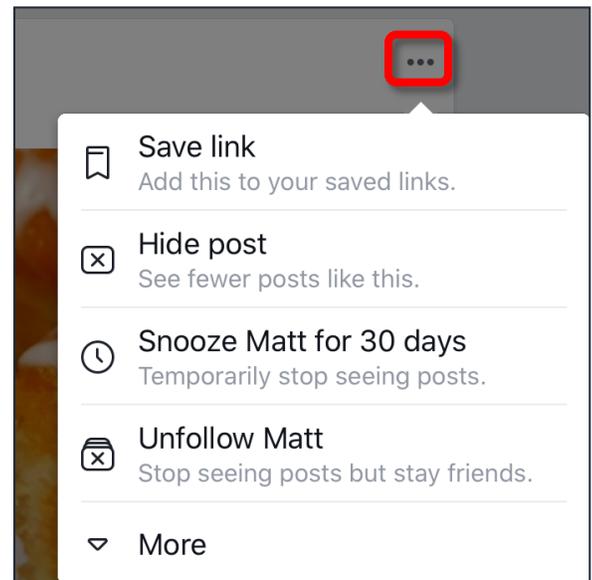
Hide this specific post from your wall / news feed. This is good if you want to ignore a single, specific post.

Snooze for 30 days

Hide posts from this person for a month. This is something that is useful in the month before an election.

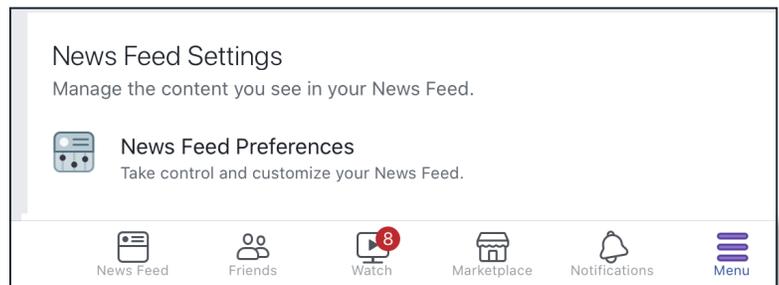
Hide all from / Unfollow

This allows you to stop seeing posts from someone, but still remain friends with them; you can see their posts by going to their wall.

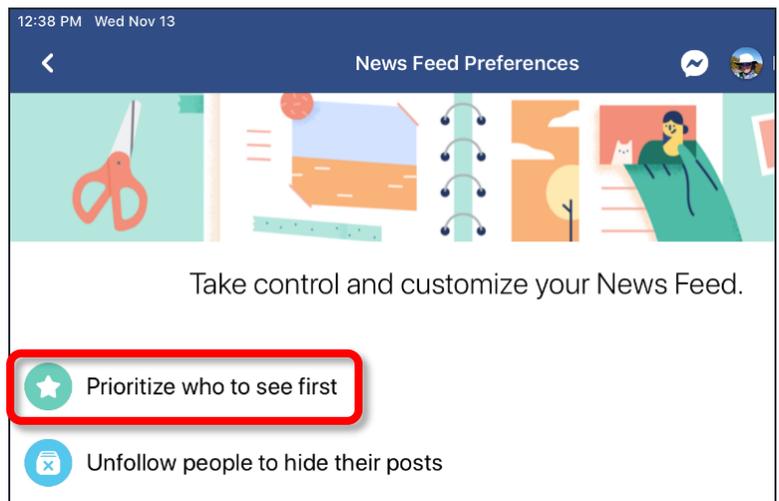


News Feed Preferences

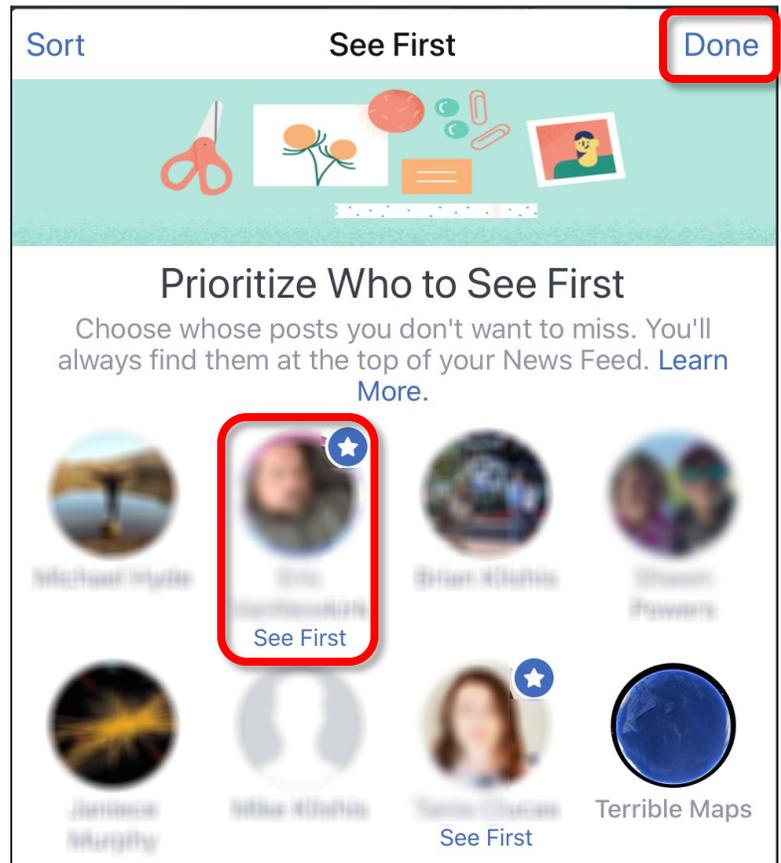
1. In the lower right corner of the Facebook window, click Menu (the three parallel lines).
2. From the menu select **News Feed Preferences**.



3. Tap **Prioritize who to see first**.



4. Tap on the picture of someone whose posts you want to see first. A blue **See First** is displayed under their name.
5. Once you're finished, click **Done**.



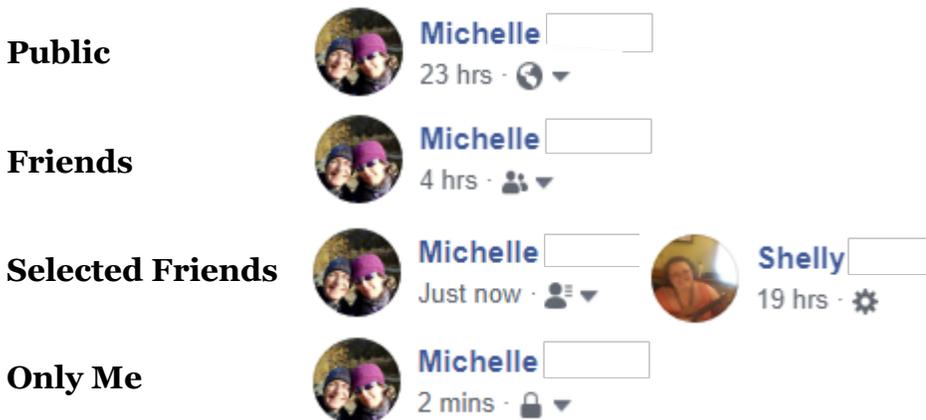
Posts

There are typically two ways you can post to your timeline: writing a post, or sharing a post from another person or group. When you create or share something on your timeline / wall, that post is displayed on your wall.

Anything you post on your wall—even something you are sharing from someone else's wall, gets its own comment section on your wall. This means that comments you make on posts on other people's walls will not appear on your wall.

Public vs Friends vs Groups

Your posts can have four levels of accessibility: public, friends, specific friends, and only me.

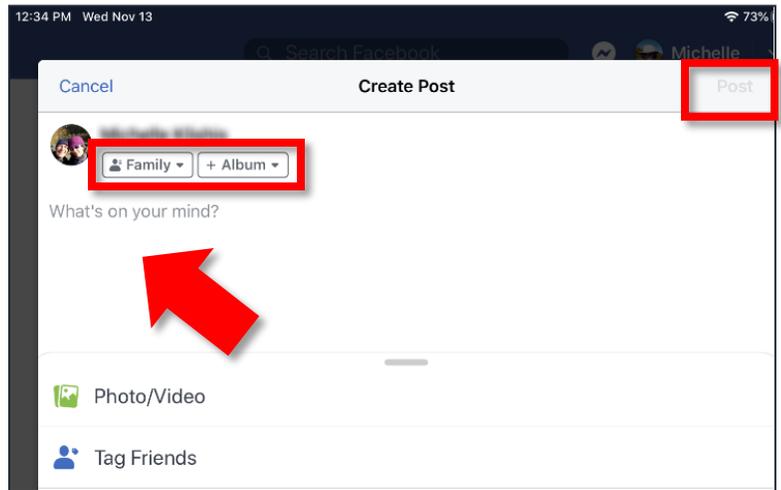


Posting something to the public means that anyone in the world who access Facebook can see what you posted. Friends means that the post will be visible to everyone in your friends list. Selected Friends posts are displayed to a group or a handful of friends. Only Me is precisely what it sounds like.

If you change the post visibility when you are creating the post, that setting will “stick” and be the setting for all posts going forward. You do have the ability to change the visibility of a post after it has been created, and in usually this is easier than trying to remember to change the visibility the next time you post.

Writing Posts

1. In your newsfeed or on your profile, tap in the post area.
2. Type whatever you want to say. Click the links to add pictures, tag friends, or add emoticons. Once you’ve added everything, click **Post**.



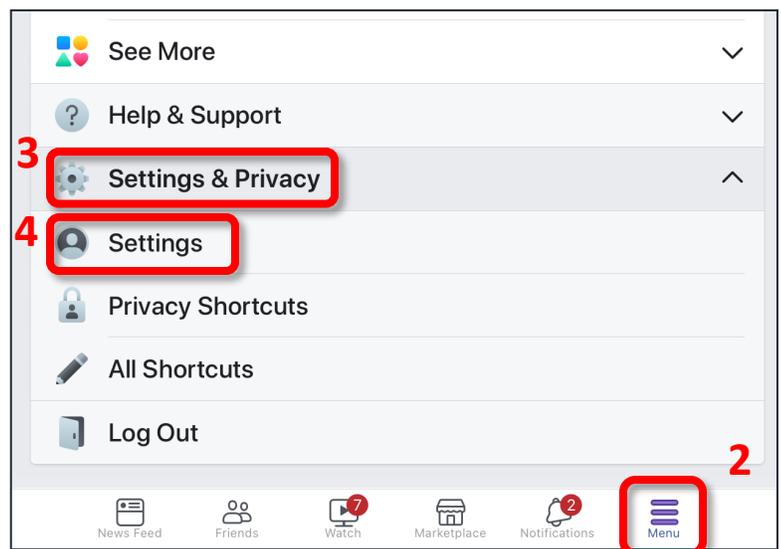
3. Once you have created a post, you have the option to edit or delete what you posted. In the top right corner of your live post, click the **ellipse (...)**.
4. From the menu that appears, select the desired option.
5. The ellipse is also available on comments you make to others posts to edit or delete.

Facebook Settings

Obviously, my first recommendation is to NOT use the Facebook app on your phone, but if you are going to use the app, there are definitely settings you should delve into.

Accessing Facebook Settings

1. Open the Facebook app.
2. In the lower right corner, click the three parallel lines to access the available menu options.
3. Scroll down through the list until you see **Settings & Privacy**.
4. The menu expands out, select **Settings**.



Privacy Settings

1. Open your **Settings**.
2. Scroll down to the **Privacy** section.
3. Tap on **Privacy Settings**.
4. Make changes to your settings as desired.

Who can send you friend requests?

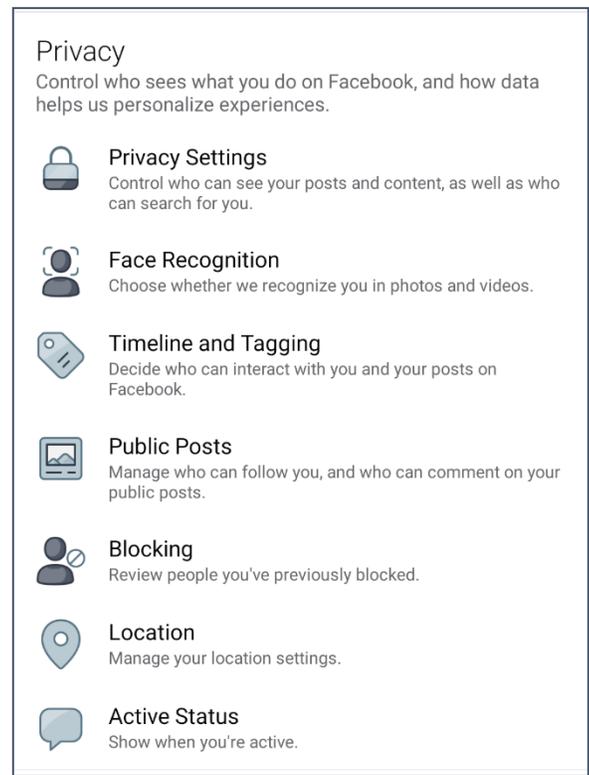
Setting this to Friends of friends limits the audience of people who can make friend requests, however, it means that if you don't have friends in common, you can't receive a friend request from someone.

Who can see your friends list?

Unless you know someone famous, Friends of friends is a reasonable choice.

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

Do you want your Facebook page to come up in a google search of your name? My answer is no. You have to decide this for yourself.



Timeline and Tagging

1. Open **Settings**.
2. Scroll down to the **Privacy** section.
3. Tap on **Timeline and Tagging**.
4. Make changes to your settings as desired.

Who can post on your timeline?

This allows you to restrict who want write on your wall / timeline. If you have family members who passive-aggressively share things on your timeline, restricting this might be useful.

Who can see posts you're tagged in on your timeline?

If someone tags you in a post, who do you want to see that post?

Review posts you're tagged in before the post appears on your timeline?

If someone tags you in a post, do you want to OK it before other people can see it?

Face Recognition

1. Open your **Settings**.
2. Scroll down to the **Privacy** section.
3. Tap on **Face Recognition**.
4. Toggle on or off.

Off-Facebook Activity

Facebook has rolled out a new privacy / security setting that allows you to see how you are being tracked by third parties when you are not actively using the Facebook site. I highly recommend you peruse and clear this list.

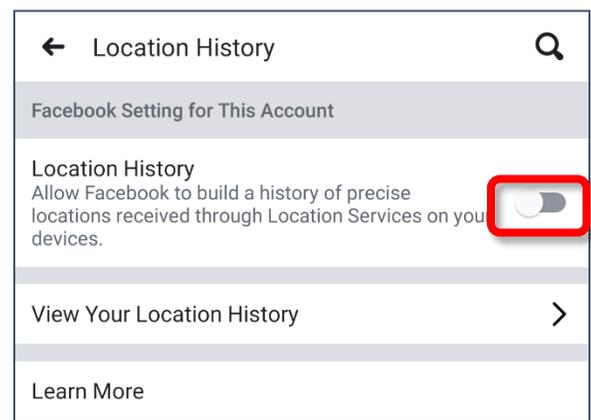
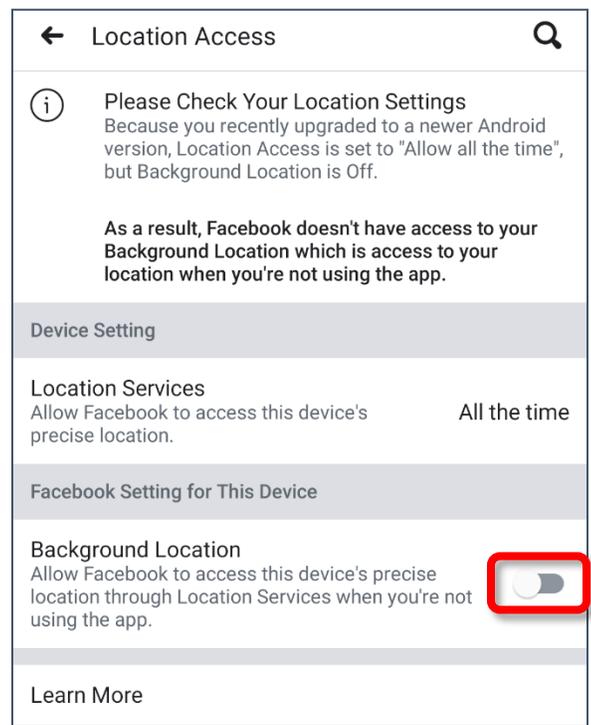
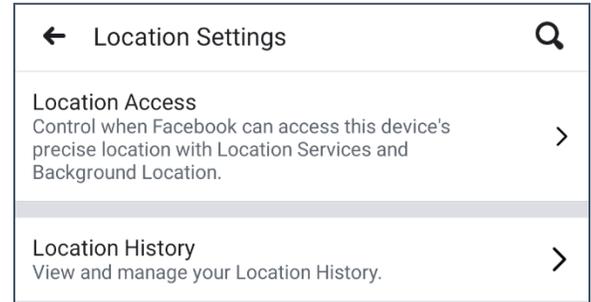
https://www.facebook.com/off_facebook_activity

Location Settings

In general, unless you use Check-in, there is no reason to allow Facebook to know your location. I recommend turning all location settings off. If this setting has been on, assume that Facebook knows precisely where you live, and all the places you frequently visit, including the homes and family members and your favorite stores.

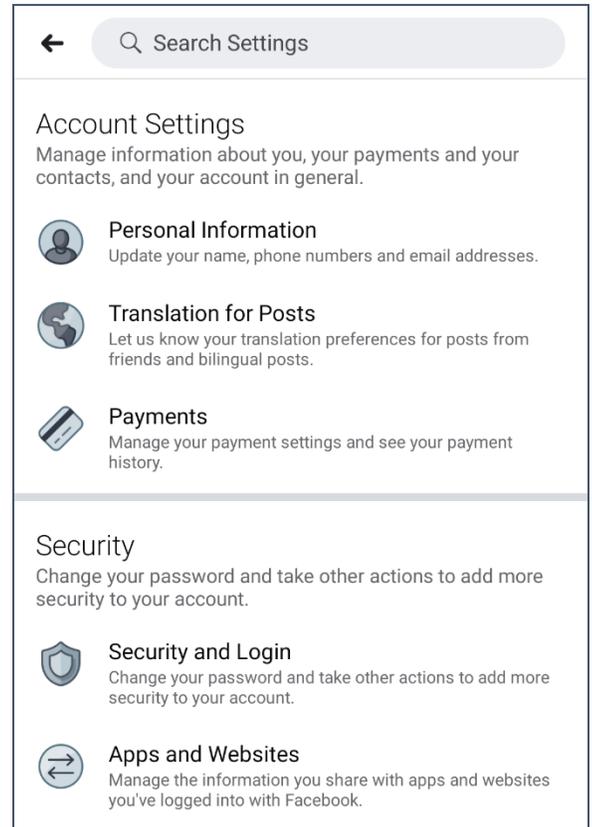
Accessing Your Location Settings

1. Open your Settings, then scroll down to the **Privacy** section.
2. Select **Location**.
3. Open **Location Access**.
4. Facebook will act like it is vitally important it knows where you are at all times. It is **NOT**.
5. Toggle **OFF** the setting to give Facebook **Background Location**. Facebook definitely does NOT need to know where you are when you are not using the app.
6. Select **Location Services** (under Device Setting) and change this setting to **Never**. Or if you use Check-in, you can set it to when you are actively using the app. But I highly recommend **Never**.
7. You should also clear your location history and tell Facebook it cannot build a location history. This won't change what information Facebook has used in the past, but it will keep Facebook from using your location going forward.

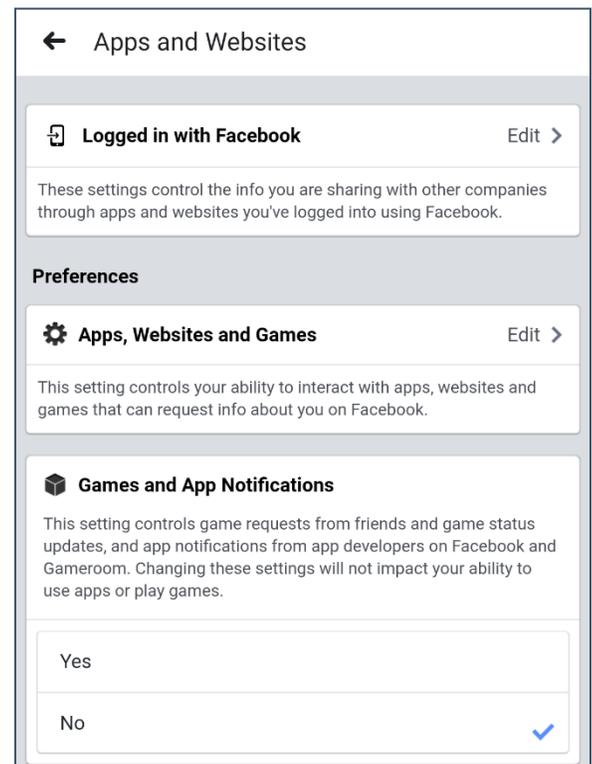


Apps within Facebook

1. Open your **Settings**.
2. Scroll down and then select **Apps and Websites**.



3. Check each of these settings to see what (if any sites) you have logged into with using your Facebook credentials.
4. Check and see what (if any) apps have been given permission to your profile.
- 5.



Web Browsers

Product	Site
Chrome	https://www.google.com/chrome/
Firefox	https://www.mozilla.org/en-US/firefox/new/
Opera	https://www.opera.com/

Web Browser Add-Ons

Product	Availability	Site
AdBlock Plus	Firefox, Chrome, Safari	https://adblockplus.org/
Disconnect	Firefox, Chrome, Safari, IE	https://disconnect.me/disconnect
Do Not Track Me	Firefox, Chrome, Opera, Safari, IE	https://abine.com/index.html
Ghostery	Firefox, Chrome, Safari, IE	https://www.ghostery.com/
HTTPS Everywhere	Firefox, Chrome, Opera	https://www.ghostery.com/

Texting Apps that Work over WiFi

Whatsapp: <https://www.whatsapp.com/>

Telegram: <https://telegram.org/>

Snapchat: <https://www.snapchat.com/>

Skype: <https://www.skype.com/en/>

Signal: <https://signal.org/>

Hangouts: <https://hangouts.google.com/>

Phone Apps

Closing Apps on an Android Device

1. Tap the Recent Applications Menu button, usually at the lower left of the screen. A list of open apps appears
2. To close an individual app, click the **x** beside the app or swipe right on the app.
3. To close all open apps, if available, tap **Close All**.

To be clear, stopping an app frequently leaves parts of that app still running in the background. To end all processes of that app, you need to force stop the app.

To Force Stop Apps on an Android Device

1. Open your device settings. (Typically available from the list of all applications or by pulling down from the top of the screen to open the system tray, and tapping the gear icon.)
2. From the list of available settings, choose **Apps** or **Applications**. (Depending upon your phone.)
3. Scroll through the list to find the specific app you want to close and/or keep from running in the background.
4. Towards the top of the screen, tap the **Force Stop** button.
5. The device asks if you are sure you want to do this, tap **Force Stop**.

Closing Apps on an iOS Device

1. Double tap on the home button to bring up a screen that displays the open apps.

OR

Swipe up twice from the bottom of the screen.

2. Drag an app up towards the top of the screen to close it.

Emoticons

(.V.)	Alien
O:-)	Angel
X-(Angry
~:O	Baby
:-D	Big Grin
(*v*)	Bird
:-#	Braces
</3	Broken Heart
=^.^=	Cat
*<:o)	Clown
O.o	Confused
B-)	Cool
:_(Crying
:'(Crying
\:D/	Dancing
_	Dazed
:O3	Dog
#-O	Doh!
:*)	Drunk
//_ ^	Emo
>:)	Evil Grin
<><	Fish
:-)	Frown
:(Frown
:-)	Frowning
=P	Frustrated
:-P	Frustrated
8-)	Glasses
\$_ \$	Greedy

:->	Grin
=)	Happy
:-)	Happy
:)	Happy
#	Hashtag
<3	Heart
}	Hug
:-	Indifferent
X-p	Joking
:-)*	Kiss
:-*	Kiss
:*	Kiss
(-){(-)	Kissing
XD	Laughing
=D	Laughing Out Loud
)-:	Left-handed Sad Face
(-:	Left-handed Smiley Face
<3	Love
=/	Mad
:-)(-:	Married
@	Mention
<:3)~	Mouse
~,~	Napping
:-B	Nerd
^ _ ^	Overjoyed
<l:o	Partying

:-/	Perplexed
=8)	Pig
@~)~~~~	Rose
=(Sad
:-)	Sad
:(Sad
:S	Sarcastic
:-@	Screaming
=O	Shocked
:-O	Shocked
:-)	Smile
:)	Smile
:-Q	Smoking
:>	Smug
:P	Sticking Tongue Out
:O	Surprised
:-J	Tongue in Cheek
:-&	Tongue Tied
=-O	Uh-oh
:-\	Undecided
:-E	Vampire
=D	Very Happy
;-)	Winking
;)	Winking
-O	Yawn
8-#	Zombie

Acronyms

AF: As (naughty word)
AFK: Away from Keyboard
BTW: By the Way
B/C: Because
BFF: Best Friends Forever
BRB: Be Right Back
CU: See You
CYT: See You Tomorrow
DGMW: Don't Get Me Wrong
EOD: End of Discussion
EOM: End of Message
F2F: Face to Face
FAQ: Frequently Asked Questions
(pronounced fak to rhyme with pack)
FREX: For Example
FTW: For the Win
FWIW: For What It's Worth
FYI: For Your Information
GR8: Great
HTH: Hope This Helps
ICYMI: In Case You Missed It
IDC: I Don't Care
IDK: I Don't Know
IIRC: If I Remember/Recall Correctly
IMHO: In My Humble Opinion
IMO: In My Opinion
IOW: In Other Words
IRL: In Real Life
J/K: Just Kidding
L8R: Later
LOL: Laugh(ing) Out Loud
MYOB: Mind Your Own Business
noob / noob: Newbie

NNTR: No Need to Reply
NOYB: None of Your Business
NP: No Problem
NRN: No Reply Needed
NSFW: Not Safe for Work
OMG: Oh My God
OMY: On My Way
OTOH: On the Other Hand
OT: Off Topic
OTP: On the Phone
ROTFL: Rolling on the Floor Laughing
RTFM: Read the Fantastic Manual
RU: Are You
SFLR: Sorry for Late Reply
SO: Significant Other
TBC: To Be Continued
THX: Thanks
TIA: Thanks in Advance
TL;DR: Too Long Didn't Read
TMI: Too Much Information
TTYL: Talk to You Later
TUVM: Thank You Very Much
TYT: Take Your Time
UR: You Are / Your
woot / WOOT: Hooray! Yay! Yippee!
WS: Wait
WFM: Works for Me
WRT: With Regard To
WTH: What the H(eck)
WTF: What the (naughty word)
YMMV: Your Mileage May Vary

Technology Glossary

Add-on

An accessory piece of software designed to increase the capability of the software to which it is appended.

Address Book

See [Contacts](#)

Alexa

Amazon's virtual assistant.

Algorithm

A set-of rules to be followed in calculations or problem-solving operations. Algorithms are frequently used to manipulate data sets.

Android

Googles mobile operating system, built on open source software.

Anti-Virus

A program that protects you from malicious software. Most anti-virus programs have options for purchasing additional security measures such as firewalls, email scanning, etc.

App

Short for [Application](#).

Apple ID

This is the username and password that you create with Apple to link a specific device to your Apple account. If you have an iPad and an iPhone, you would use the same Apple ID with both of those devices.

Apple

Technology company that designs and develops hardware and software.

Application

A piece of software that lets your device do something, like play music or give directions. An application is the same thing is a program or a software program.

Autocorrect

Autocorrect is when your device automatically changes what you were typing to what it thought you wanted to type.

Autoplay

When you visit a website and music or video starts playing without asking.

Backup

A copy of computer data that is taken and stored somewhere else, to be used in the event of data loss.

BCC

Blind carbon copy. Secretly send a copy of the message to someone else. The primary recipient cannot see that this person received the message.

Blockchain

Also Block Chain. A list of records (blocks) linked using [cryptography](#). These records are a cryptographic hash of the previous block, a timestamp, and transaction data. Blockchains are generally used on a peer-to-peer network. Data in one block cannot be altered without changing all other blocks.

Blog

An online journal that allows one or more writers to share information. Posts are displayed in reverse chronological order.

Bluetooth

A wireless technology that allows data to be shared over short distances using short-wave UHF radio signal. [Named for King Harald "Bluetooth" Gormsson.](#)

Browser Add-on

See [Browser Extension](#).

Browser Extension / Add-On

A small software module that is used to customize a web browser.

Browser Hijack

Where a malicious piece of software modifies a web browser's settings without your permission.

Browser

Short for [Web Browser](#).

Browsing Data

The list of web pages you have visited, as well as associated data, such as page title and time of visit.

Brute Force Attack

Where a hacker tries many passwords or passphrases in an attempt to break into your account. The longer your password (or passphrase), the harder it is for someone to use this kind of attack to break into your account.

Cache

Temporary storage space that allows your computer to quickly bring up information, such as previously viewed web pages.

Cambridge Analytica

A British political consulting firm that used misappropriated digital assets, data mining, and other processes to influence political elections around the world.

CC

Carbon copy. Send a copy of the message to someone else. The primary recipient can see this person received the message.

Cellular Data

The connection your cell phone makes to a cell tower that allows you to do things like surf the internet, download emails, and send SMS messages.

Cloud / Cloud Storage

Digital storage in pools, spread across multiple [servers](#) (sometimes in multiple locations) that is available to verified users through an internet connection. Storage that is physically somewhere other than where you are. Cloud storage is generally accessible from multiple devices, because those files are stored on a hard drive that belongs to a company that hosts the cloud service. Cloud storage is like a self-storage unit for your electronic files, except you can access your stuff from anywhere.

Code

Computer code or program code. A set of instructions that form a program that tells a computer what to do.

Codec

A device or program that encodes/decodes a data stream, such as an audio file, for storage.

Contacts / Contact List

A collection of screen names and the various data associated with them, such as email addresses and telephone numbers.

Cookie

A piece of data that a website saves on your computer. Cookies were designed to save user information such as preferences or logins, but can sometimes be read by third parties. Cookies are also used to collect browsing data long-term.

Cortana

Microsoft's virtual assistant.

CPU

Central Processing Unit. The bit of a computer or electronic device that processes information.

Cryptocurrency

A digital asset that uses strong [cryptography](#) and is designed to work as a form of money. They used decentralized control, or a public financial database to keep track of who owns what.

Cryptography

Greek for “hidden writing”, it is the study of secure communication—creating protocols to keep third parties from reading private messages.

Data

Units of information.

Data Breach

The release of secure or private information. A data breach can be accidental or malicious, such as when an individual hacks into a system to steal information.

Database

An organized collection of information. Complicated databases link information between multiple tables allowing for analysis of the contained information. An address book is a basic database.

Denial of Service Attack (DOS)

A cyber-attack where the malefactor seeks to make a network resource (such as a website) unavailable by flooding the target with requests or visits.

Directory

A system that catalogs / organizes computer files.

DNS

Domain Name System. The phone book of the internet. DNS translates names (olliatwvu.org) into [IP](#) addresses, so web browsers can find and access those resources.

DNS Hijacking

Where a malefactor redirects visitors from a valid website to a different destination—often one that exists to steal data.

Domain Name

The string of text that identifies a place on the Web. A basic domain name is a word or abbreviation followed by a period followed by the domain extension: wvu.edu

Domain

The sometimes arbitrary grouping that designates what a website does or where it is based. The most common domains are .com .net .edu and .org. The domain is what you should check first when you want to verify the authenticity of a website. [Internet Top Level Domains](#).

Download

To move data and files from the internet or a server to your computer or mobile device.

Email Header

The portion of an email message that contains the routing information. The header can be used to help determine if a message is fraudulent.

Email

Email is an electronic letter sent from one email address to another email address. Email addresses always have an @ (at sign) in them. Sending an email on your phone requires the use of cellular data. Each email address is unique, and email addresses are often used as unique identifiers or login credentials by databases.

Emoji

Small images used to represent emotions, ideas, or expressions. 😊

Emoticons

Representations of facial expressions using keyboard characters. These are used to portray moods or feelings. For example, a smiling face could be :) or ☺ See page **Error! Bookmark not defined..**

Encryption

The encoding of data so that only authorized persons or devices can read/view the information. The stronger the encryption, the more unlikely it is that a malefactor could decode the intercepted data through a brute force attack.

External Storage

Devices that store data outside of a computer or other electronic device. They are often removable, such as USB thumb drives.

Facebook

An online media and networking company.

Facial Recognition

Technology capable of identifying or verifying a person from a digital image. Facial recognition can be used to unlock an electronic device.

Firewall

A security system that monitors incoming and outgoing network traffic to prevent unauthorized access to a system.

Firmware

A specific class of software that provides control for that specific device's hardware.

Folder

See [Directory](#).

Follow

Choose to see another user's posts in their content feed.

Force Stop

A way to completely stop an app that is running in the background. An app that has been closed may still have bits active and collecting data.

Google

A technology company that specializes in services and products related to the internet.

GPS

Global Positioning System is a piece of hardware that allows a device to contact a satellite to determine the location of the device in latitude and longitude. On most devices, software makes these data points usable to the end user by placing them on a map.

Hardware

The electronic components of a device; the bits you can touch. A cell phone, a keyboard, and a CPU are all hardware.

HDR

High Dynamic Range. A photographic process where a camera takes multiple pictures at different exposures and combines them into a single image—this allows all areas of your image to be well-exposed, but can also look unreal if used too much.

Home Screen

The main screen of a computer or mobile device. Home screens are typically personalized by the user so that no two home screens will look alike.

Hotspot

A type of Wireless Access Point. A device that allows you access the internet from a public place. Hotspots are generally open and unsecured and you should assume any data you submit is visible to people with ill-intent.

Hover text

When you hold your cursor over a hyperlink, the document should display the URL for that link. This allows you to verify links.

http

Hypertext Transfer Protocol is how data is moved between a website and an end user.

https

Hypertext Transfer Protocol (Secure) is an encrypted form of http. This protects against interference or snooping by third parties.

iCloud

Apple's cloud service.

Icon

A graphic representation of a program, file or function.

Information Security

The protection of data and the mitigation of risks, generally on computer networks.

Install

A process that writes the code used to run the program (application) onto the hard drive of your device. Installing a piece of software embeds it into the device and allows it to work.

Internet

A system of inter-connected computer networks.

Internet Service Provider

An organization that provides internet access.

iOS

Apple's mobile operating system.

IP Address

Internet Protocol Address. A numerical label given to an individual device that can connect to a computer network.

iPad

Apple's tablet computer, running iOS.

iPhone

Apple's cellular phone, running iOS.

iPod

Apple's music player. The iPod is general similar to an iPhone, only without cellular service.

ISP

See: [Internet Service Provider](#)

iTunes

Apple's music service.

Key

A set of instructions to [encrypt](#) or decrypt a message.

Keylogger

Keystroke logger (also keyboard capture). A piece of hardware or a software program that can record every character struck on the keyboard.

Location Services

Information from [GPS](#), wireless access points, cell towers, and [Bluetooth](#) devices that helps your phone know where you are.

Lock Screen

The opening screen or interface of an operating system. A lock screen keeps unauthorized users from accessing the data and information on a device.

Login Credentials

The information required to access a site or system. A username and password are credentials, as are a finger print or retina scan.

Lossless Compression

A form of data encoding that maintains the original quality of the file but with a large file size.

Lossy Compression

A form of data encoding used to reduce file size at the cost of data quality.

Messenger

An app that allows users to send text messages and images to other users in a system.

Metadata

A data set that gives you information about other data. A card catalog contains metadata.

Microblogging

Online platform for broadcasting short messages or pictures. Twitter is a microblogging platform.

Micro-SD

Micro-Secure Digital Card. Smaller size [SD card](#), used in phones and lightweight devices. Comes with an adapter that allows for the transfer for files from a portable device to a computer.

Moderator

A person who keeps an online discussion from getting out of hand. Moderators usually have the ability to mute or ban a user who is misbehaving.

MMS

Multimedia Messaging Service is a kind of text messaging that allows you to send text messages that contain pictures or audio, as well as messages longer than 160 characters or to multiple people.

Mobile Carrier

A wireless service provider that allows users to connect portable devices (such as phones) to the internet through a cellular service.

Mobile Data

Wireless internet access through a cellular data connection.

Network

A group of computers connected for the purpose of sharing resources. A network can be as small as two computers or as vast as the Internet.

News Feed

The main page of Facebook, where you see content posted by users you have chosen to follow. These content can be text or images.

Notification

A message displayed by an electronic device to provide an alert, reminder, or other communication.

Online Chat

Real time communication over the internet through (generally short) text messages.

Open Source

Computer code or plans that can viewed, modified, and shared by the general public.

Operating System

An Operating System is the base upon which software and apps are added. An Apple device generally uses iOS (iPhones) or macOS (laptop computers). PCs typically used the Windows OS, but there are other operating systems, such as Linux that can be installed. Non-Apple cell phones frequently use some form of the Android OS. How your device looks and works is dependent upon the operating system installed.

OS

See [Operating System](#).

P2P

[Peer-to-Peer](#)

Passcode

This is the secret code to get into a specific device.

Password Manager

A program that stores electronic passwords.

Password

The secret code to access a restricted resources. Passwords are usually required to use a minimum of eight characters, and contain special characters, such as numbers or upper case letters.

PayPal

A method of online money transfer and payments.

Peer-to-Peer

A distributed network that shares tasks or work between devices of the same level.

Permissions

Access rights to a device or program or resources.

Phishing

A fraudulent attempt to gain personal or sensitive information, by sending an email or creating a website that pretends to be from a real company or person, but is not.

Play Store

Goggle's app store, where users can download or purchase programs to run on their Android devices.

Podcast

A digital audio file made available on the Internet for downloading to a computer or mobile device, typically available as a series, new installments of which can be downloaded automatically.

Post

A message, comment, image, or other item that is placed on the internet, generally on a website.

Predictive Text

An input technology that guesses what you want to type both from what you are currently typing and, if you have allowed the software to learn, from what you have typed in the past. Predictive text makes typing faster and easier if you have good software on the back end.

Privacy

The information that is shared between your device and the external resources to which it is connected, as well as how that information is used, and with whom that information is shared.

Program

A program is a piece of software that lets your device do something like send a text message or video chat. A program is the same thing as an application.

Public Network

An electronic connection where the traffic between devices is visible to anyone.

Reply All

A response to an electronic message that is returned to ALL recipients of the original message.

Reply

A response to an electronic message.

Ripping

Extracting digital content from a container, such as a CD or DVD. Ripping a CD means that the music is copied without loss from the CD to your computer.

ROT-13

One of the most basic forms of [encryption](#); a substitution encryption where characters are rotated 13 places.

Router

A networking device that forwards data between networks.

Scraping

Web scraping, web harvesting, web data extraction is extracting data from websites—gathering up information available on a public website.

SD Card

Secure Digital card. Removable memory that is used in devices like cameras, because it can be easily switched out when full. Allows for easy transfer of files from device to computer without a cable.

Search Engine

A software system designed to find information on the web. The results from a search engine can be webpages, files, or images. Generally, behind the scenes a program runs an algorithm that crawls through the web cataloging everything it sees. This catalog is then organized by a different program where pages are associated with various terms.

Security

Protecting electronic systems from theft or damage. This can be protection from physical theft, but often refers to electronic damage, where systems can be disrupted or data stolen.

Server

A device (or program) that allows you to access something not on the device you are physically touching. A mail server stores your email and drops it to your device upon request. A web server allows you to connect to the internet.

Settings

An app that allows you to customize your computer, device, or program.

Siri

Apple's personal assistant.

Smart Device

An electronic device that connects to other devices or the internet through a wireless protocol such as Bluetooth or Wi-Fi.

SMS

Short Messaging Service. A brief message that is sent from one phone number to another phone number. SMS does not use cellular data.

Snooping

Unauthorized listening in to data transmission.

Snopes

One of the first internet fact-checking resources, Snopes started as a site to debunk urban legends, but expanded into general fact-checking. (<https://www.snopes.com>)

Social Media

Interactive computer technologies and websites that allow for the sharing of information. Facebook is the most famous social media site, and allows friends to connect automatically. LinkedIn is another type of social networking site that focuses on career and job networking.

Software

The programs that run on your computer or phone, on top of the operating system. Can also be called applications or programs.

Spam

Unsolicited electronic messages (especially advertising).

Spoofing

When a person or program pretends to be someone else, by falsifying data, to gain access to your account or data.

Spyware

A piece of malicious software that secretly installs itself to gather information about the user or device.

Status Bar

A graphical element, usually at the top or bottom of a device's screen, which displays information about the state of the device. Some settings commonly found on the status bar are sound/volume, time, and battery life.

Streaming Service

Online entertainment provider that delivers content over the internet. Movies, music, and TV are some of the most common types of content.

Sync

See [synchronize](#).

Synchronize

When a file is synced, changes to that file are saved are pushed from one device to all other devices with access to that file, via a remote server.

Tag / Tagging

A keyword or term added to the metadata of a piece of information. In social media, when someone is tagged, they are alerted to a post made by another user.

Terms of Service

The rules you agree to abide by when you sign up use an online service.

Text Message

A brief message that is sent from one phone number to another phone number via a protocol called SMS. Text messages are generally limited to 160 characters, and messages with more characters than that will be broken down into multiple messages when sent. Text messages are asynchronous: a message sent to someone whose phone is off is delivered when their phone is turned back on. Text messages generally do not require cellular data but do require a cellular connection.

Third-Party Apps

Software created by someone other than the manufacturer of a device or operating system.

Timeline

A display of items in chronological order. Twitter has a timeline; Facebook has a news feed.

TOS

See: [Terms of Service](#)

Tracking

The ability of website software to keep tabs on visitors to the site. Collecting information about your use or interaction with a web page. In addition to when you viewed a page, websites can collect information on your IP address, location, and what browser you are using.

Trojans

A type of malicious computer virus that presents itself as a useful item, such as a document.

Two-Factor Authentication

This is a way to make both your device and your account more secure. When you log into your Apple ID on a new iPad (or iPhone) for the first time OR you log into iCloud from a computer you have never used before, Apple wants you to verify that YOU are the person attempting to access your account.

TXT

[Text message.](#)

Unfollow

To stop seeing a user's posts in your timeline or news feed. On Facebook, you can unfollow someone by still remain friends with them.

Uninstall

The removal of a software program or application from the operating system of a device. Although uninstall removes the visible aspects of a program, there are often bits and pieces of the program left behind.

Unique Identifier

A piece of data that is unique to a record. Telephone numbers and email addresses are often used as unique identifiers because no two individuals have the same ones. Unique identifiers allow data records to be linked across databases.

Upload

To move files from your computer to a [cloud service](#) or [network](#).

URL

Uniform Resource Locator is the address of a space on the web. Every website has a unique address, and that address can often tell you something about the web page you are visiting.

USB

Short for Universal Serial Bus, this is the industry standard for cables that connect devices and their peripherals through a wire. This connection can be used for both communication and power. There are several types of USB connections: USB, USB-mini, USB-micro, and the newest standard, USB-C.

User

The person operating a device or program.

User Data

Any type of data generated by people interacting with software programs. User data includes: Explicit Data, which is given by a user directly such as name, address, email, and phone number; Implicit Data, which is not provided by the user directly but gleaned through analysis of user interactions, such as pages visited, session duration, or type of device; and finally External Data which has been gathered from third parties with whom an organization has a relationship.

Username

Also called Account name, login ID, user ID. The credentials you use to access an electronic resources, such as your computer or a website. Every account on a website or device must be unique to that service, so as to keep account information separate.

Virtual Personal Assistant

A software program that performs tasks or services based upon verbal commands. Some of the most well-known services are Siri and Alexa.

Viruses

A piece of malicious software that inserts itself into another software program that it uses to replicate itself. Ransomware is a software virus.

Voice-Over IP

A method of and group of technologies that allow you to deliver voice communications across the internet.

VOIP

See [Voice-Over IP](#)

Web

Also called the World Wide Web, this is an information space on the Internet that is accessible from devices such as computers, cell phones, and tablets, using a [URL](#) as the address.

Web Browser

A software program that allows you to access sites on the Internet, or web.

Web Cookie

See [Cookie](#).

Weblog

See [Blog](#).

Website

A location connected to the Internet that maintains one or more pages on the World Wide Web

Wi-Fi

Short for wireless (the “fi” is an arbitrary syllable added on)

Widget

A graphical element that displays information or provides quick access to certain parts of an app. Mobile devices frequently have a weather widget that is linked to your weather app, and which tells you the current temperature and forecast.

Wireless Access Point

A device that allows your device to access the internet. If a wireless access point (or router) does not have a password, it is unsecure, and you should assume that anyone can see what you are doing on your device.

Wireless Router

A piece of hardware that allows devices to connect to the internet without being plugged into the wall. Your wireless at home should be password protected, so that strangers cannot access all devices in your home using that wireless network.

Wireless

A technology that allows computers to connect to a network and/or the internet without using a physical connection. Wireless is available in an area when a wireless access point (also called a hotspot) has been created and made accessible to devices. Public wireless is less secure and caution should be used (ie, don't make purchases or send private emails over a wireless network). Private wireless networks (such as in your home) should be secured with a password.

World Wide Web

An information system on the Internet which allows documents to be connected to other documents by hypertext links, enabling the user to search for information by moving from one document to another.

References

The Complete Guide to Facebook Privacy (Wired.com)

<https://www.wired.com/story/facebook-privacy-apps-ads-friends-delete-account/>

How to Use Facebook's Privacy Settings (Consumer Reports)

<https://www.consumerreports.org/privacy/facebook-privacy-settings/>

How to Secure your Facebook Account (CNet & Lifewire)

<https://www.cnet.com/how-to/secure-your-facebook-account-in-six-easy-steps/>

<https://www.lifewire.com/how-to-secure-your-facebook-timeline-2487774>

Facebook's Notifications Are Out of Control. Here's How to Tame Them. (NY Times 2019)

<https://www.nytimes.com/2019/05/30/smarter-living/stop-facebook-notifications.html>

How to Memorialize a Facebook Account

<https://www.facebook.com/help/1506822589577997>

What You Don't Know About How Facebook Uses Your Data (NYT - 2018)

<https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html>

Everything you've ever posted publicly on Facebook has probably been harvested. So what?

<https://www.cbc.ca/news/technology/facebook-scraping-public-profile-data-so-what-where-why-1.4610146>

We're Keeping Track of All of Facebook's Scandals So You Don't Have To (Fortune - 2018)

<https://fortune.com/2018/04/06/facebook-scandals-mark-zuckerberg/>

A recent history of Facebook scandals (2019)

<https://www.trtworld.com/magazine/a-recent-history-of-facebook-scandals-26157>

The Facebook and Cambridge Analytica scandal, explained with a simple diagram (Vox - 2018)

<https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>

Facebook, Cambridge Analytica and data mining: What you need to know (CNet - 2018)

<https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/>

Facebook's latest controversy has echoes of Cambridge Analytica scandal (CNN - 2019)

<https://www.cnn.com/2019/05/11/tech/facebook-rankwave-korean-data/index.html>

Facebook's Secret Censorship Rules Protect White Men From Hate Speech But Not Black Children (ProPublica - 2017)

<https://www.propublica.org/article/facebook-hate-speech-censorship-internal-documents-algorithms>

Under Facebook's new algorithm, conservative meme pages are outperforming all political news pages (Media Matters - 2018)

<https://www.mediamatters.org/blog/2018/07/24/under-facebook-s-new-algorithm-conservative-meme-pages-are-outperforming-all-political-news-pages/220768>

Guess what? Facebook still tracks you on Android apps (even if you don't have a Facebook account)
<https://privacyinternational.org/blog/2758/guess-what-facebook-still-tracks-you-android-apps-even-if-you-dont-have-facebook-account>

If Facebook is stalking me, what about Instagram? (Washington Post, 2020)
<https://www.washingtonpost.com/technology/2020/01/30/help-desk-if-facebook-is-stalking-me-what-about-instagram>

Facebook attacked over app that reveals period dates of its users (Guardian - 2019)
<https://www.theguardian.com/technology/2019/feb/23/facebook-app-data-leaks>

Explain me like I'm five: What is Cryptocurrency (Medium)
<https://medium.com/meetngreetme-ico/explain-me-like-im-five-what-is-cryptocurrency-ed1276d5f4c5>

Everything you need to know about Facebook's Libra cryptocurrency (CNet)
<https://www.cnet.com/news/everything-you-need-to-know-about-facebooks-libra-cryptocurrency/>

Payments giants abandon Facebook's Libra cryptocurrency (BBC 2019)
<https://www.bbc.com/news/technology-50023008>

Facebook's digital currency dealt another blow (BBC 2019)
<https://www.bbc.com/news/business-50037223>

Facebook Removes Misleading Trump Census Ads
<https://www.nytimes.com/2020/03/05/technology/facebook-trump-census-ads.html>

Facebook Approved Ads With Coronavirus Misinformation (Consumer Reports – 2020)
<https://www.consumerreports.org/social-media/facebook-approved-ads-with-coronavirus-misinformation>

Sensitive to claims of bias, Facebook relaxed misinformation rules for conservative pages
<https://www.nbcnews.com/tech/tech-news/sensitive-claims-bias-facebook-relaxed-misinformation-rules-conservative-pages-n1236182> (NBC 2020)

Right-wing media thrives on Facebook. Whether it rules is more complicated.
<https://www.vox.com/recode/21419328/facebook-conservative-bias-right-wing-crowdtangle-election>
(Vox 2020)

2020 Election

Facebook takes down Russian operation that recruited U.S. journalists, amid rising concerns about election misinformation
<https://www.washingtonpost.com/technology/2020/09/01/facebook-disinformation-takedown/>
(Washington Post 2020)

Russians Again Targeting Americans With Disinformation, Facebook and Twitter Say
<https://www.nytimes.com/2020/09/01/technology/facebook-russia-disinformation-election.html>
(New York Times 2020)

Facebook Said To Delete Strike Warnings For Conservative Platforms That Post Misinformation
<https://www.forbes.com/sites/vidhichoudhary/2020/08/07/facebook-said-to-delete-strike-warnings-for-conservative-platforms-that-post-misinformation/#359425f411a7> (Forbes 2020)

Facebook executive: we got Trump elected, and we shouldn't stop him in 2020

<https://www.theverge.com/2020/1/7/21055348/facebook-trump-election-2020-leaked-memo-bosworth> (The Verge 2020 (link to NYT Paywall))

Political Advertising on Social Media Platforms

https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/voting-in-2020/political-advertising-on-social-media-platforms/ (American Bar Association 2020)

FactCheck.org 202 Election

<https://www.factcheck.org/tag/2020-election/>

Index

Facebook Controversies	1	Using Facebook Messenger in Your Browser	14
Scams	1	Using Messenger in Your Browser	15
Retaining users' deleted videos (2018)	1	Turning off Active Status.....	15
Data-Breaches 2018-2019	1	Finding Missed Chat Messages	16
Scraping Public Profiles	1	Facebook App on Android.....	17
Apps Sharing Personal Data (- 2019).....	1	News Feed.....	17
Rohingya (2018-2019).....	1	Posts.....	20
Facebook Algorithm and "Censorship"	2	Public vs Friends vs Groups	20
Russian Meddling.....	2	Facebook Settings.....	22
Cambridge Analytica (2014-2018).....	2	Accessing Facebook Settings.....	22
Facebook Tracking	3	Off-Facebook Activity.....	23
Unique Identifiers	3	Location Settings	24
Web Cookies	3	Apps within Facebook	25
Libra Cryptocurrency	4	Facebook App on iOS	27
And Yet...	4	News Feed.....	27
Making Your Facebook Use More Secure.....	4	Posts.....	29
Using Facebook	5	Public vs Friends vs Groups	29
Facebook Website on a Laptop (or Desktop)...	6	Facebook Settings.....	30
News Feed.....	6	Accessing Facebook Settings.....	30
Posts.....	9	Off-Facebook Activity.....	31
Public vs Friends vs Groups	9	Location Settings	32
Settings	11	Apps within Facebook	33
Accessing Your Facebook Settings.....	11	Web Browsers	34
Privacy	12	Web Browser Add-Ons	34
Timeline and Tagging.....	12	Phone Apps	34
Face Recognition	12	Closing Apps on an Android Device.....	34
Off-Facebook Activity.....	13	To Force Stop Apps on an Android Device	34
Location History.....	13	Closing Apps on an iOS Device	34
Apps within Facebook	14	Emoticons	35
Seeing Your Facebook Apps	14	Acronyms	36
Removing Apps.....	14	Technology Glossary.....	37
Messenger.....	14	References.....	47
Facebook Chat Options	14	Index	50

Please Support OLLI@WVU!

Osher Lifelong Learning Institute
Mountaineer Mall Unit C-17
PO Box 9123
Morgantown, WV 26506-9123
Phone Numbers:

Office: (304) 293-1793
Email Address: olli@hsc.wvu.edu
<http://www.olliatwvu.org>