

INTERNET SAFETY FOR **CHILDREN AND PARENTS**

Detective John Stirling 795
Shawnee, KS Police Department

GUIDE AND ATTACHMENTS REFERENCE



J. STIRLING #795
Detective

SHAWNEE, KANSAS
POLICE DEPARTMENT

Direct: 913-742-6795
Dispatch: 913-631-2150
Fax: 913-631-5657
E-mail: jstirling@ci.shawnee.ks.us

5850 RENNER • SHAWNEE, KANSAS 66217

Internet Safety for Children and Adults

Detective J. Stirling 795
Shawnee, KS Police Department

The following material is being provided to you as reference material for the presentation which you are about to see. Please keep this with you and take notes. Information and pictures are provided below. The following information should read along with the presentation.

Predators and predatory behavior

When discussing internet safety you must look at it from both the adult and child perspective. There are times when both children and adults can be perpetrators in these crimes and you must also look at the child's perspective of what they are thinking at the time and why these crimes are occurring to them.

Furthermore, this section on predators and predatory behavior can be examined in three different areas: pictures, apps (applications) and behavior.

Pictures

The first area to examine with pictures is the **background** content of those photos. You must ensure:

- 1) Are the pictures you or your child post publicly viewable by anyone?
- 2) Are you confident that you know the true identity of every person who can view your private photos.

When the photos you post are publicly viewable by anyone, then there is a possibility that you may have a background in a photo that is recognizable to anyone who views them. For example, if photos are posted in real time with a sign for a pool in the background, a person viewing these photos or coming across the photos may recognize or be able to find where those photos were taken, and where the person taking them are at the moment they are posted.

Furthermore you must remember that not everyone who has a profile online is actually who they say they are. A person lying about their identity may befriend you or your child online and convince you they are someone else, gaining your trust and then being able to view the pictures, with recognizable backgrounds, which are not out there for public viewing.

If you have personally met everyone who is a friend on Facebook, a follower on Instagram or Twitter, etc, then you can post pictures with recognizable backgrounds with confidence. If you do not post photos with recognizable backgrounds then you should be fine from this respect.

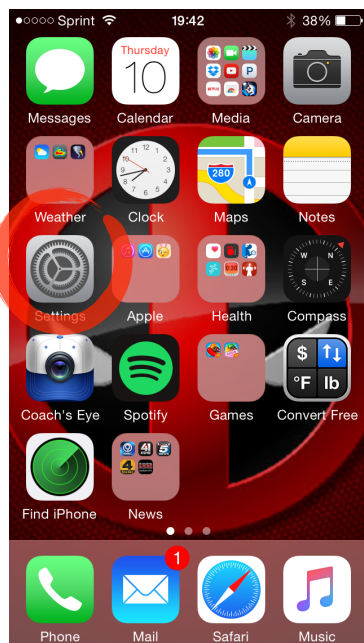
The second area to acknowledge is the **geolocation** capabilities of both the devices and the applications used.

Device: The majority if not all of the modern day devices which can be used (cell phones, tablets, etc) have the capabilities of tracking and recording the GPS coordinates of your devices. GPS is extremely accurate and can be affected by some factors (i.e. weather) but it is always best if you disable this feature for certain applications on your devices.

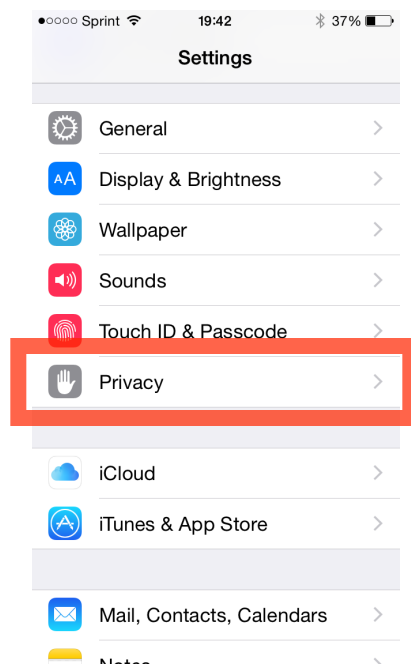
When using certain applications the GPS is needed and is fine to use. For example, the mapping functions to direct you along the road will not work without GPS enabled. However, GPS should be turned off for your camera and any other applications where you communicate with others.

To turn off the geolocation features for an iOS device:

Go to the settings for the device

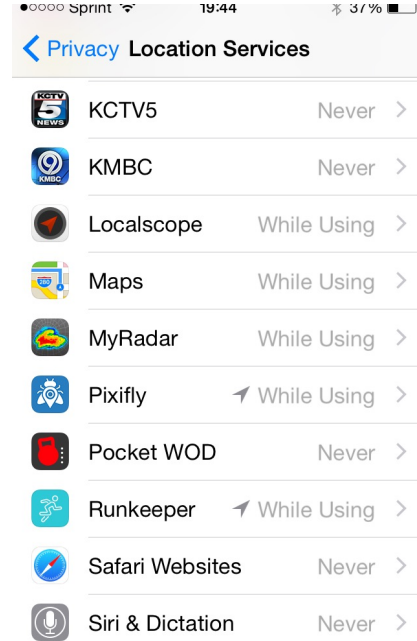
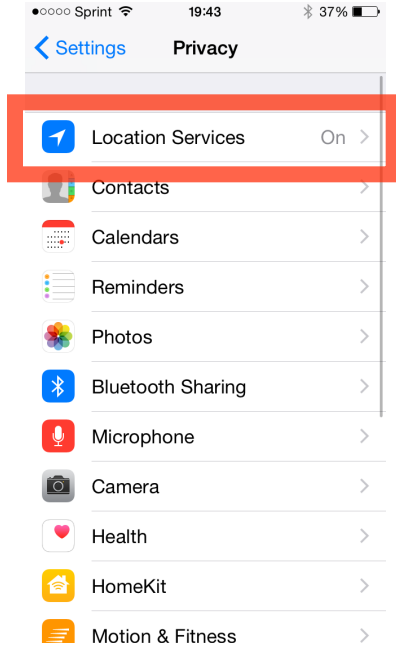


Next access the Privacy settings

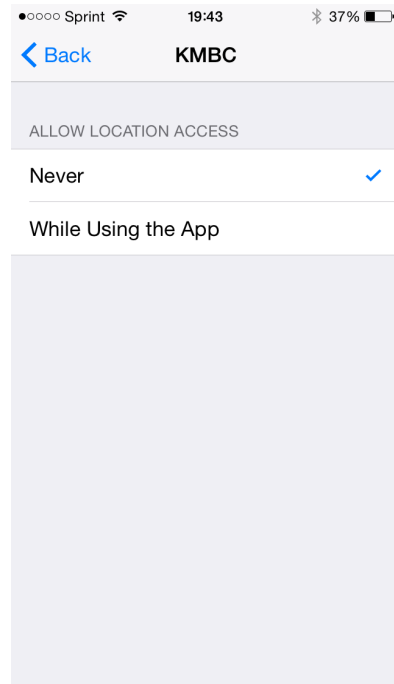


Choose the Location Services menu

Options for each application are available



Picking each application you can change these settings



I recommend you leave the location services on but just choose within the app itself whether it will be on for that program.

To turn the location services off on an Android device:

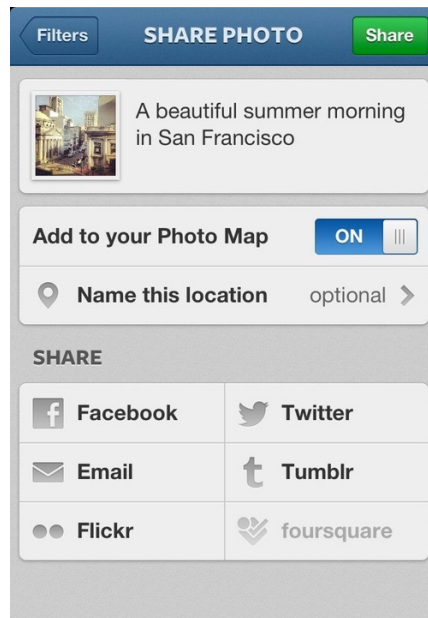
SEE ATTACHED

Within the application: Instagram is a program which has its own geolocation feature that is utilized. The geotags on Instagram uploads are not the location where the photo was taken, even if the GPS tagging was on at the time of the picture being taken. The GPS tags on Instagram uploads are the location where the upload occurred. Instagram also has it's own settings for this.

Allowing the geotagging to take place on Instagram builds a map which perpetrators can find the most common location where you upload photos from; often times this is your home.



GPS tags should be turned off for Instagram in the settings of the phone, if available, AND within the app itself. These can also be selectively turned off for each photo that is uploaded.



These GPS tags can be searched through various websites and mobile applications to find the newest pictures being put up closest to the user conducting the search.

Next we must examine the **content** of the file being sent. As with anything, does it need to be out there and should we send what we are about to send. It is important to remember that pictures on any device or on a computer are nothing but code, 1's and 0's. The applications on the devices (i.e. the gallery) are just programs that allow the code to be rendered into a picture. When the code is sent from one device to another it must first imprint on the device, then pass through a secondary location (likely a server somewhere) and then be imprinted on the other device. These do not necessarily go away quickly and are susceptible to being gathered in a hack or other type of data breach.

As has been shown in years past, SnapChat, for example, leaves remnants of pictures on the devices which can be found later on through an examination (or if the perpetrator knows what they're doing) and even SnapChat was the victim of a data breach where hundreds of thousands of user sent photos were released onto the internet.

Apps (applications)

Applications have evolved to meet our desire for immediate gratification and direct and instantaneous communication with people. Looking through the popular social media apps in the Apple App Store or Google Play store will likely

show you the majority of the popular items present are messengers and applications to meet new people.

Some of the newer, more concerning apps, are designed to allow kids to connect with people in their school. Applications like **After School** and **Jott Messenger** allow people to create profiles and then connect in groups with people at their school. What must be remembered is that no verification is conducted on these apps so a perpetrator can get on Jott Messenger with a fake name and date of birth and instantaneously have access to any child in a school who has created a profile on that application. They can then begin to chat with that child and, likely, see their picture.

After School app icon



Jott Messenger app icon



Again, the content always comes into play because we must examine if the information that is about to be put out online should be put out there considering that it goes through a separate source to reach its final destination.

Behavior

For obvious reasons we would never assume to blame a victim for what has happened to them. No person should have to be a victim no matter what they do online. That being said, there are things children do online which make them more susceptible to being a victim.

The two main mistakes children make are contradictory in nature. They tend to believe that

- 1) Everyone I meet online is telling the truth and is who they say they are
- 2) I am anonymous and no one can figure out who I am

Children will message or chat with random individuals without knowing who they are, where they are from, or if they really are another child. In addition to this, there are VIDEO messaging applications which allow children to be randomly connected with individual via video, not knowing what is going to pop up on the screen when that connection is made. Two of these apps are **Chat Roulette** and **Omegle**.

Chat Roulette



Omegle



When examining the perpetrator behavior it is important to remember that they are persons who conduct solicitation and targeting of children are professional liars. The stigma of their crime forces them to hide their activities from even those who are closest to them. They will use lies, flattery and whatever other means necessary to make a victim comfortable and to coax information or other things out of him / her. Nothing that is said by an adult (or a child who may actually be an adult) online can be taken at face value when they are talking to kids.

It is also important to remember that if an adult tells a child that this is “their first time” or they “normally don’t go for younger people”, this is more than likely impossible. Pedophilia is a sub-category of a broader **mental disorder** known as a paraphilia. The Diagnostic and Statistic Manual (DSM), used to categorize mental disorders, recognizes paraphilia as a mental disorder and identifies eight specific sub-categories, with Pedophilia being one of those. Another paper published in 2009 identified a possibility of as many as 549 different kinds of paraphilias. As is commonly recognized, mental disorders are not easily treated and it is possible that they can not be treated at all.

In addition to this, pedophiles have their own subculture where they meet and discuss the best ways to solicit children, stay away from Law Enforcement, trade

photographs of children, encrypt these files on their devices, etc. This takes place on the deep web (dark web) which comprises about 80-90% of the internet and is only accessible through specific web browsers. This should tell you that pedophiles are so acutely aware of what they are doing that they have actively sought to create communities or find communities of like-minded individuals in places that are more difficult to find and trace.

These communities share their ideas and photographs in the form of “how-to” manuals and forums that can not be found by your normal web search or accessed through normal web browsers.

Bullying and cyberbullying

28% of students in today's schools have been a victim of bullying and 30% admit to having participated in bullying behavior. Furthermore, 70% of students have been witness to bullying behavior and generally do nothing. It is averaged that bullying type behavior will stop within 10 seconds if an individual says something and intervenes.

The incidents of cyberbullying are even more staggering:

Cyber Bullying Statistics

- Depending on the age group, up to 43% of students have been bullied while online. 1 in 4 have had it happen more than once.
- 35% of kids have been threatened online. Nearly 1 in 5 have had it happen more than once.
- 21% of kids have received mean or threatening e-mail or other messages.
- 58% of kids admit someone has said mean or hurtful things to them online. More than 4 out of 10 say it has happened more than once.
- 53% of kids admit having said something mean or hurtful to another person online. More than 1 in 3 have done it more than once.
- 58% have not told their parents or an adult about something mean or hurtful that happened to them online.

Wherever there is an audience to listen to these cyber attacks on children, the activity will take place. It is important to not overlook ANY application or forum because it can take place anywhere on the internet. Applications like Instagram, Yik Yak, 4chan, Vine, Kik and Ask.fm can be, and are, used to bully children.



There are also legal ramifications for possible bullying behavior that can be used if the situation deemed them appropriate.

Harassment by Telecommunications Device (KSA 21-6206) - Using a telecommunications device to make or transmit any comment, request, suggestion, proposal, image or text which is obscene, lewd or lascivious, or with the intent to abuse, threaten or harass any person at the receiving end, make or transmit a call, whether a conversation ensues or not, with the intent to harass the person at the receiving end, etc.

Criminal Threat (KSA 21-5415) - Any threat communicated with the intent to place another person in fear for their safety or contamination of a food supply.

Identity Theft (KSA 21-6107) - Obtaining, possessing, transferring, using, selling or purchasing any **personal identifying information** with the intent to defraud that person or anyone else to receive a benefit or to misrepresent that person in order to subject them to economic or bodily harm. Personal Identifying Information includes but is not limited to name, address, date of birth, social security number, passwords, usernames or other log-in information that can be used to access a person's personal electronic content including but not limited to content stored on a social networking site.

Stalking (KSA 21-5407) - Engaging in a course of conduct targeted at a specific person that would cause a reasonable person to fear for their safety or the safety of their family. Course of conduct is defined as two or more acts over any period of time which evidence a continuity of purpose including but not limited to threatening the safety of that person or their family, following approaching or confronting the person or a member of their family, appearing at or in proximity to their residence, employment, school, etc, causing damage to that person's property or the property of their

family, harming a pet belonging to that person or that person's family, any act of communication.

Unlawful Acts Concerning Computers (KSA 21-5839) - pretty much covers anything you could do with a computer that you shouldn't.

“The Cloud”

You must remember that the cloud is not an amorphous object somewhere up in space where our information is “securely” stored. This name gives off the connotation that our information is up in the air somewhere and can not be accessed. The “cloud” is actually just servers sitting in a room with a lot of storage space. When information is in a server or any computer, especially one that is as “secure” as the cloud, it becomes an inviting target for hackers. In 2014 there were 621 confirmed data breaches resulting in well over 2 million victims of identity theft. Home Depot, SnapChat and the iCloud have all been successfully hacked resulting in a tidal wave of fall out and information being leaked to persons with malicious intent.

As we refer back to previous sections of this document, if you send something from one place to another it must go through a “middle man” to get there, even text messages. If you bet on the fact that these servers will, at some point, be hacked, have you sent anything that you do not desire to be out there for public consumption.

Tips, tricks and what to do

Several things to think about:

1. Be nosy with your kids. Know how many accounts on what sites they have and check the content for those locations. How much time do they spend alone with internet capabilities? Remember that every adult, when they were a kid, tried to get away with as much as they could when their parents weren't looking. Why would you assume that today's children would be any different?
2. Set the example for your kids on how to behave online and with their devices.
3. Do research, learn what's out there and how to find it (see below).
4. Encourage your children to talk to you if something happens and know that they will not be judged if they do bring something up.
5. Contact Law Enforcement and let us help.

Don't forget to check the settings, especially privacy and GPS settings, on all your device's applications AND on your social networking sites. Stay away from things like Facebook checkin which allows you to throw your precise location out to everyone who wants to look in and see where you are. Remember, they may be looking for where you are and they may be looking for where you're not.



Be aware of hidden files applications which mimic calculators or outright say they are for hiding files. These are designed to keep your eyes away from things that are supposed to not be seen. Again, find these items and know how to search for them.

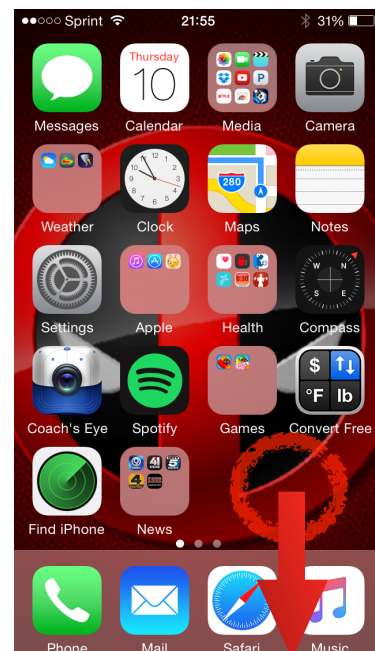


Do not use public WiFi to do anything important, especially banking, checking email, etc. The same thing goes for the free WiFi at hotels and other businesses, do not trust it because there is a possibility that it is a hacker / scammer looking to find your personal information.

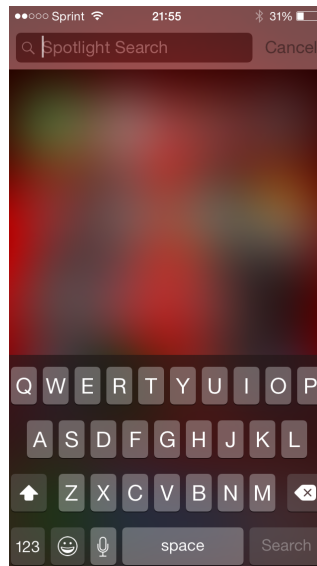
Finding items on iOS devices which have been downloaded

Kids can, and do, download items from the App Store and then delete or hide the icons so that they will not be seen by parents. These can be found in a couple of ways. The first way is if you hear about something that may be of concern and you don't want your kids to have it. You can start by searching the device for this application.

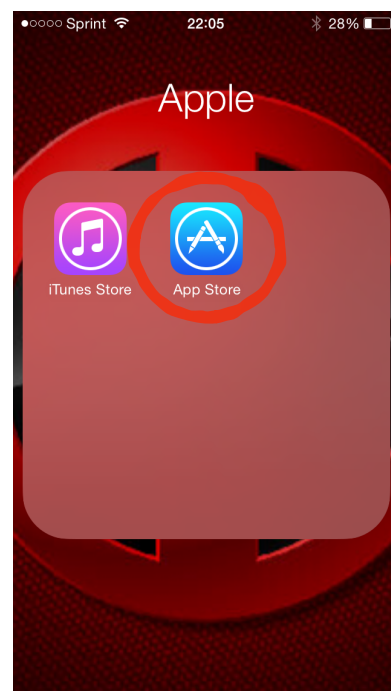
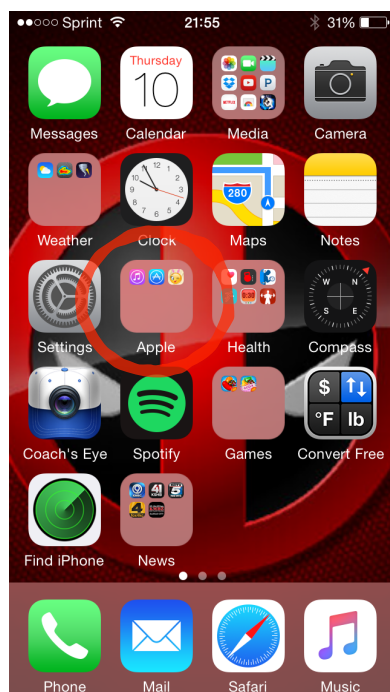
To search the iOS device simply place your finger at any blank area of the screen and pull down.



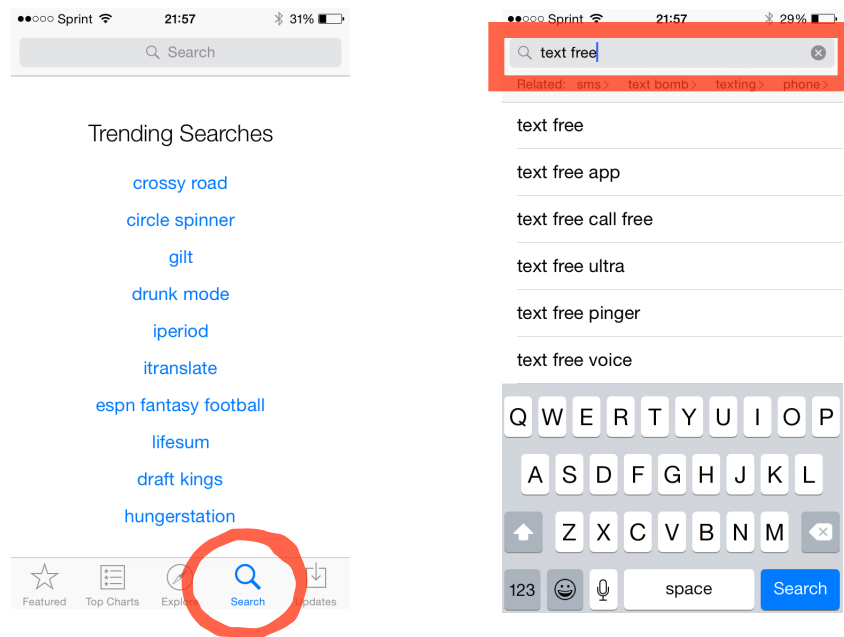
This will access the search screen and you can type in any program to see if it is installed.



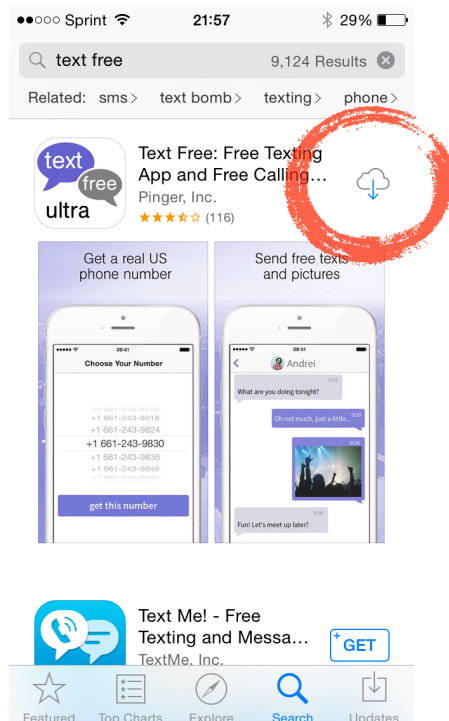
If you do not find it located on the device but still want to know if it's been downloaded at some point on your account, from the main screen select and go to the App Store.



Once in the App Store, select the search option and type in the name of the program you are looking for

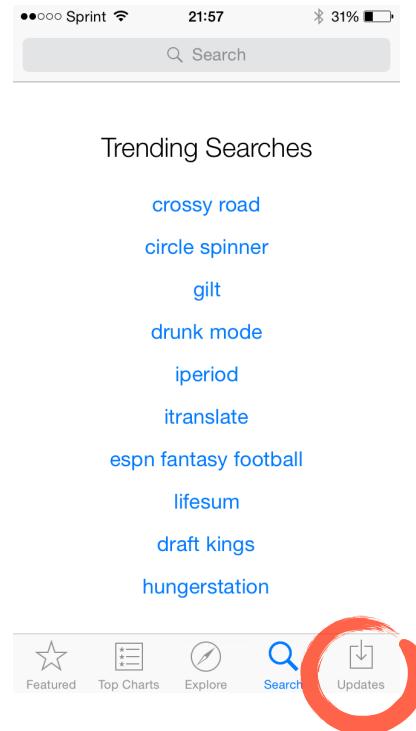
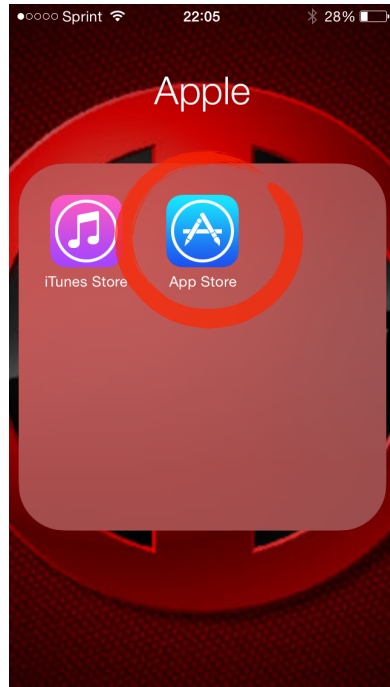


Once you choose the program you are looking for it will pull it up in the store. If it shows a box with either GET or a price (i.e. \$2.99) inside of it, that program has not been purchased on your account at any point. If it shows a box with the word OPEN inside, the program is currently installed on your device and is likely hidden somewhere. If it shows the cloud icon below, the app has been purchased at one point and placed on your device but has since been deleted.

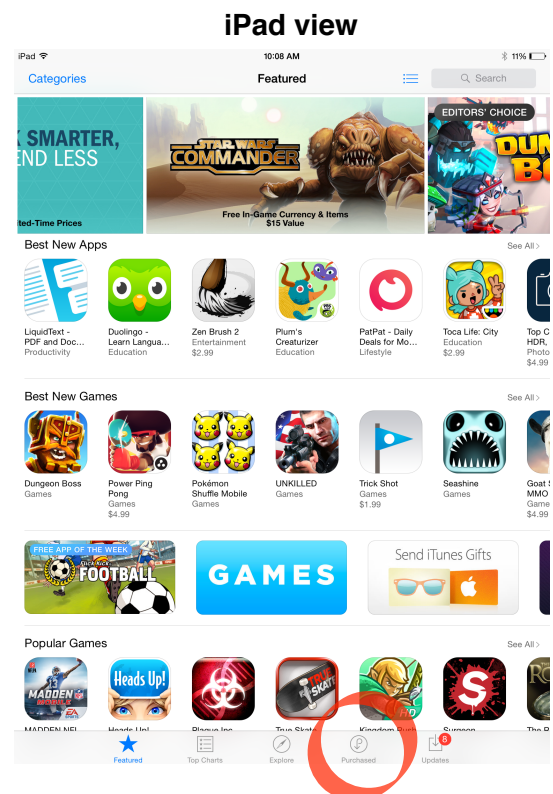
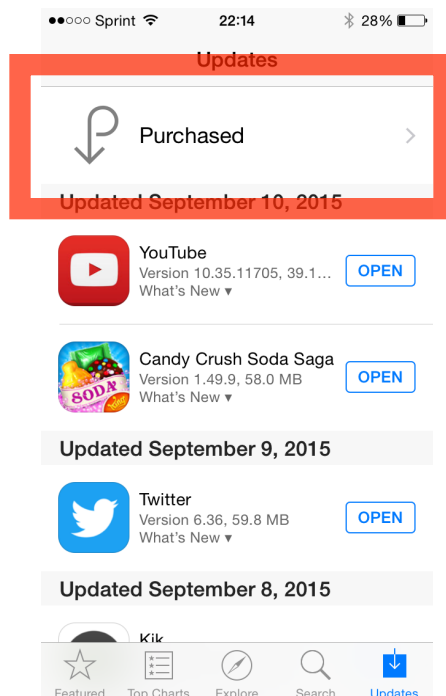


If you just want to see a list of items that have been purchased on your account (even across multiple devices, that is an option as well.

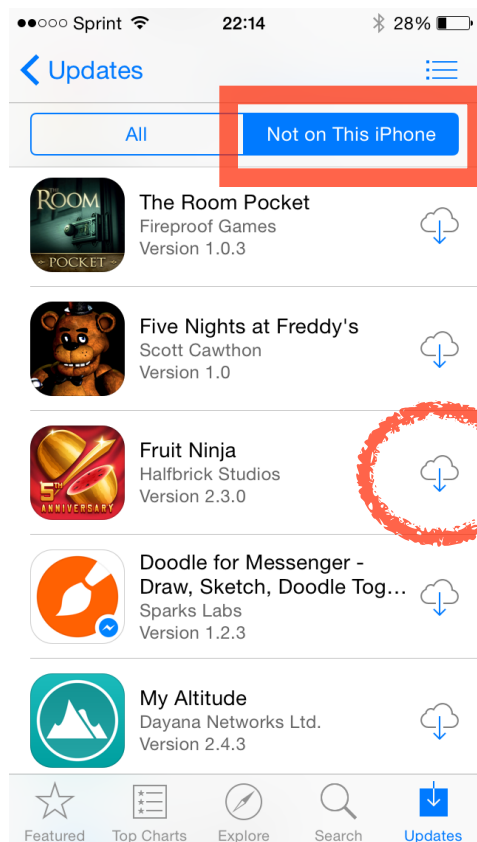
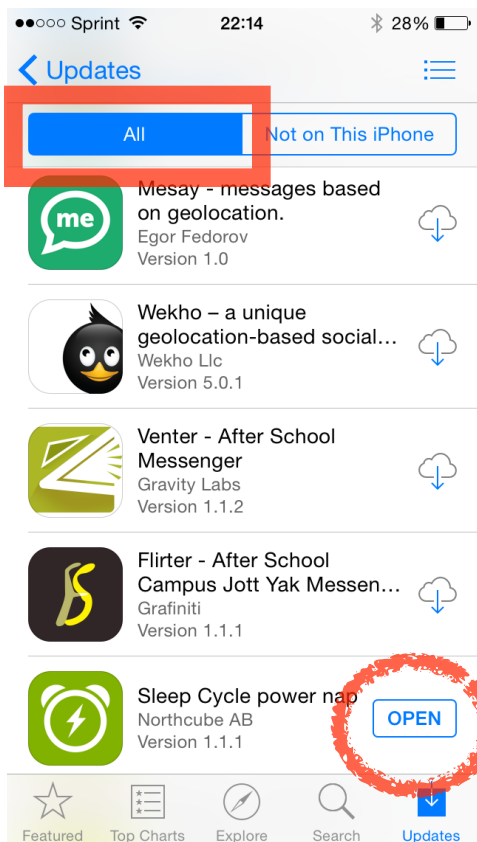
Again, access the App Store but this time select updates.



From the updates screen you will be able to view the purchased items. NOTE: this menu is part of the bottom dock on iPad's and does not need to be accessed through the updates screen.



From here you will be able to view everything that has been purchased on any device through your Apple account (ALL) or things that have been purchased on other devices (Not on this iPhone / iPad). The symbol next to the apps will either be the box saying OPEN, indicating it is still on the device



LOCATION SERVICES ON ANDROID DEVICES



In regards to turning off the location services from Android devices, there are different methods depending on what device you are working with, and, within these devices, there are potentially different methods for each. I will separate these into Device 1 and Device 2 sections and there will be separate method sub-sections within.

I would recommend that you not just rely on one of these methods in and of itself, but to check all methods for your device and determine that it has been turned off through all possible formats. Additionally, this will ensure your comfort in the fact that it has, indeed, been taken care of.

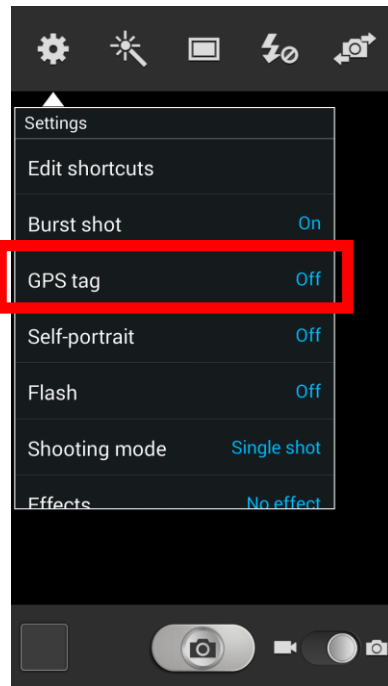
*Device 1 in these examples is a Samsung Galaxy SIII while Device 2 is an LG LS660

Device 1 - Method (a)

The first way to turn off geotagging is the easiest for Android. Simply open the camera from the main screen until you are at the point you are ready to take a photograph and select the settings cog when available.

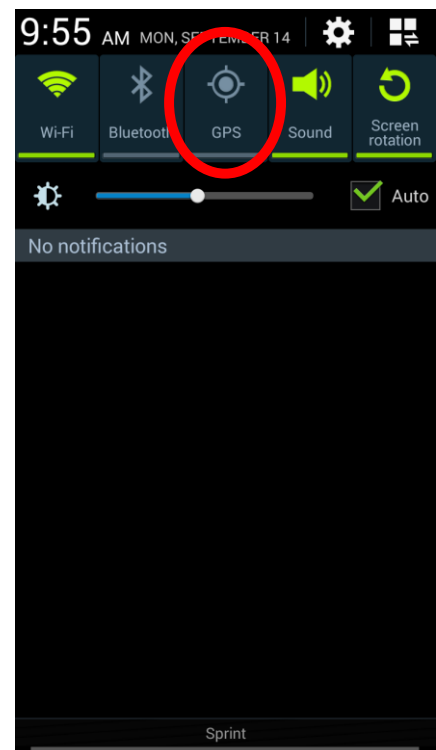


From here a menu will appear and you will see an option for “GPS tag”. Make sure this is turned off.



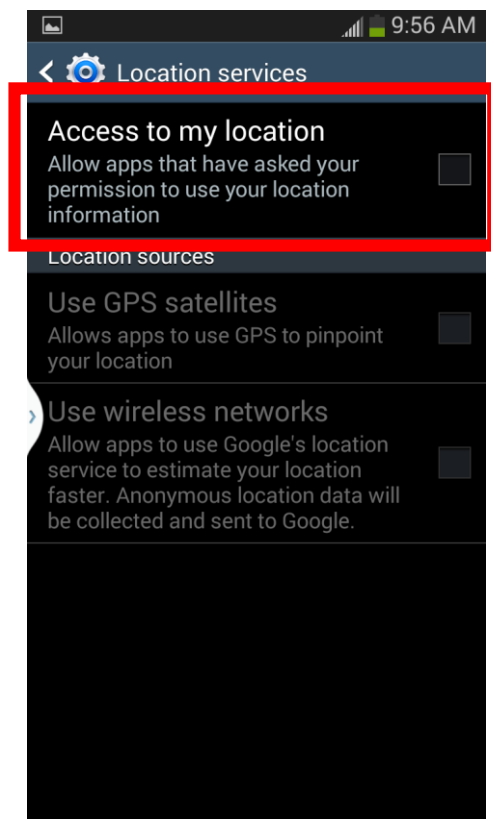
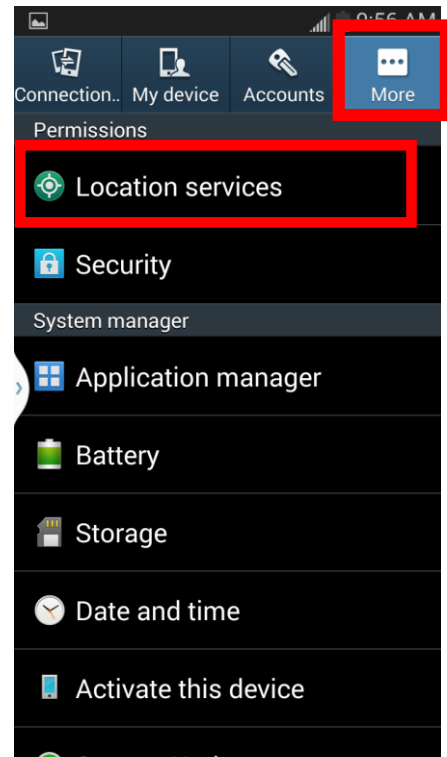
Device 1 – Method (b)

The second method to check is from the main screen of your phone. Place your finger on the top of the screen and swipe down to obtain the status bar dropdown menu. From here there should be an option for GPS. Make sure this is deselected, likely if it is on it will be illuminated or green in color and if it is not it will be greyed out.



Device 1 – Method (c)

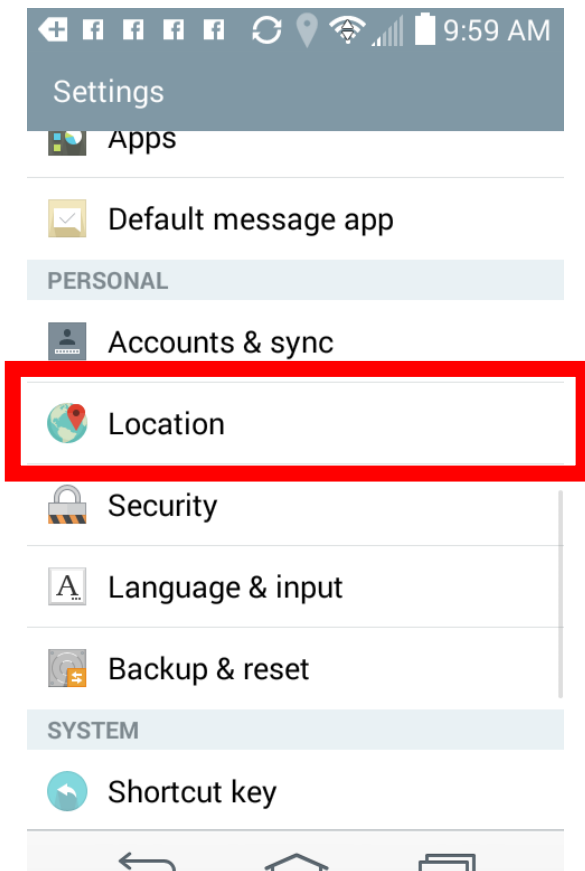
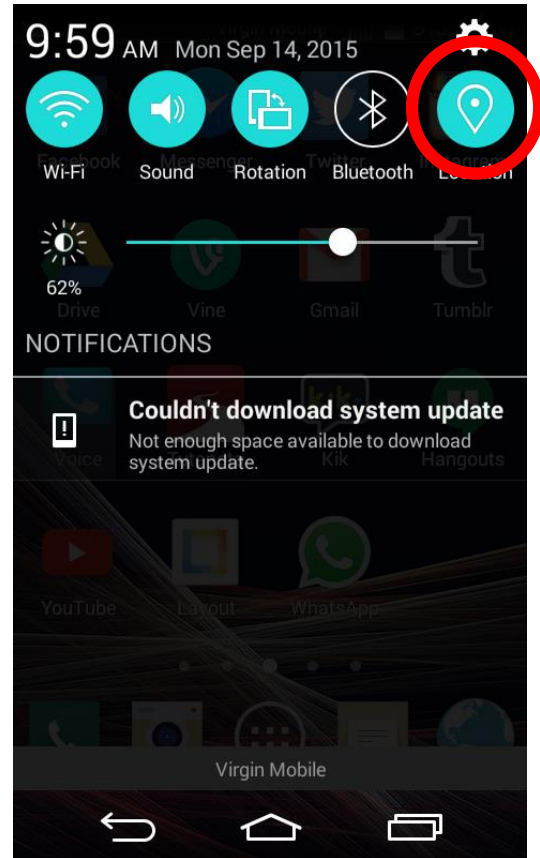
From the main screen of your phone go to settings and, on the top bar go to “More”. You will then see the option for “Location services”. Select this option.



Once you have accessed this menu, deselect the box which is titled **“Access to my location”**. This box reads “Allow apps that have asked your permission to use your location information.”

Device 2 – Method (a)

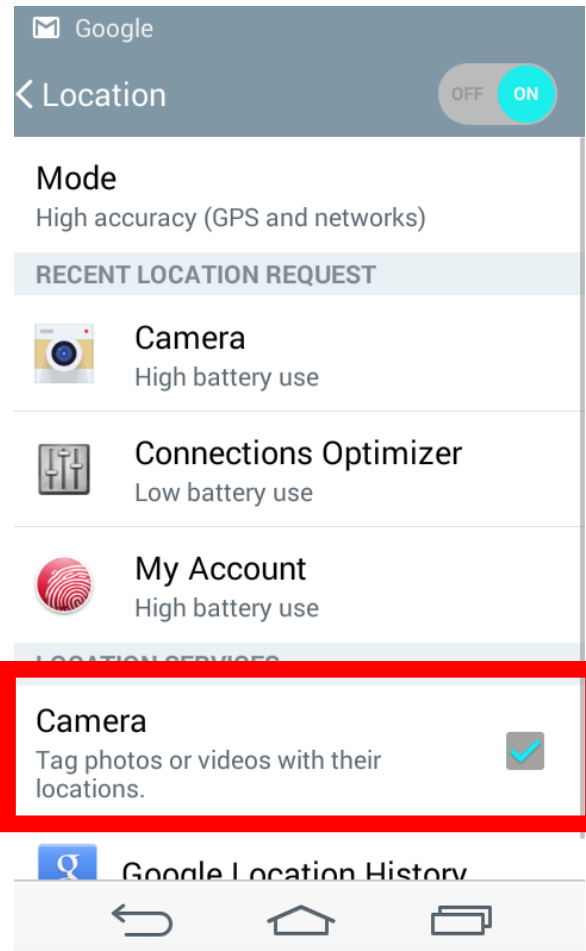
The first method for this device is the same as method (b) from the previous device. From the main menu simply place your finger at the top of the screen and swipe down to open the menu bar. Make sure the icon for “Location” is deselected (i.e. not filled in).



Device 2 – Method (b)

From the main screen access the settings menu and scroll down until you find “Location”. Select this option.

From here, you will find what apps have recently requested your location. Below that is a box that reads “**Camera**” and “Tag photos or videos with their locations”. Deselect this box.





The Complete Guide to Facebook Privacy Settings

by Dan O'Halloran on March 11, 2015

in Facebook, Computers and Software, Computer Safety & Support, Tips & How-Tos, Privacy, Tech 101, Social Networking :: 53 comments



Privacy concerns and privacy controls on Facebook are ever changing. When you post a picture of your kids at a family gathering, which one of your Facebook friends can share it? What private information are those Facebook game apps collecting on you for "third-party uses"? How can you limit who sees certain posts? Every action you take on Facebook has privacy and sharing implications that need to be considered before you upload that next selfie.



Fortunately, thanks to vocal demands for transparency from both Facebook users and government regulators around the world, Facebook has been making the process of managing your privacy easier. Below is our step-by-step guide to taking full control of your Facebook privacy settings.

Privacy Checkup

Three quick steps help make sure you're sharing with the right people



1 Your Posts

This controls who can see what you share when you post from the top of News Feed or your profile. Your current setting is **Friends**.

Who would you like to see your next post?

Friends

Changing this here will set the audience for your future posts, but you can change it whenever you post and we'll remember your choice for next time.

[Learn More](#)[Next Step](#)[2 Your Apps](#)[3 Your Profile](#)

The basic privacy options

Recently, Facebook introduced a more user-friendly guide through its vital privacy settings. By clicking the padlock symbol in the upper right of any Facebook page that you are logged into, you will get a dropdown window presenting you with walkthroughs of your current settings as they pertain to "Your Posts", "Your Apps" and "Your Profile".

Your posts

Starting with Your Posts, you can check your default sharing setting. We recommend the Friends setting over the Public one. When set to Public all your posts can be seen by anyone on or off Facebook. Unless you're a celebrity or running a page that is used to generate interest in a business you run, you will likely want to keep your activity restricted to those you have Friendened.

The Friend setting has a few tweaks you should be aware of as well. By clicking on the sharing setting button, then the More Options button, you will see the Custom option. Click on that and you will see that you can include all your Friends, while excluding the names of certain Facebook friends you don't want seeing your updates. It is also important to note that the Friends of anyone tagged in your post or photos will be able to see that post unless you uncheck the option in this window.

If you have joined any Facebook groups or made lists of Facebook friends, you can restrict the posts that way or hide your posts from those groups and lists as well. You just want your college friends to see your late night party pictures? You want to make sure your work friends don't see your selfie at the beach when you called in sick? This is where these restrictions could come in handy both on a per post basis or as an overall option.

Finally, remember that you can change the sharing settings of any individual Facebook update by clicking on the sharing button to the left of the Post button. You can even go back to change settings of previous posts by clicking on the people icon at the top of the post, to the right of the date stamp.

Privacy Checkup

Three quick steps help make sure you're sharing with the right people



Great! Your future posts will be shared with **Friends** until you change it again. You can change this whenever you post, or on your [Privacy Settings](#) page.

2 Your Apps

Here are the apps you've logged into with Facebook. You can edit who sees each app you use and any future posts the app makes for you, or delete the apps you no longer use.

Remember, you can always edit your apps by going to your [App Settings](#).

| | | | |
|---|-------------------|---|---|
|  | Bubble Witch Saga |  Public ▼ |  |
|  | Spin |  Only Me ▼ |  |
|  | EverQuest Worlds |  Only Me ▼ |  |
|  | Pet Rescue Saga |  Only Me ▼ |  |
|  | Candy Crush Saga |  Friends ▼ |  |

[Learn More](#)

[Next Step](#)

Your apps

Remember the Candy Crush Facebook game you played too much last year? How about that Instagram Facebook app you forgot you installed? Each app on the site you agreed to install has permission to post to your Friends list unless you told it otherwise at the time you installed it. Can't remember? This part of the tool shows you each app attached to your account and what sharing permissions it has. These settings also control who can see that you have the app installed.

If you don't use the app anymore, just delete it by clicking on the x. While checking my own app list while writing this guide, I found many apps I no longer use that had sharing rights on my account. I deleted all that I'm not actively using and set the sharing permissions of the remaining ones to Only Me.


3 Your Profile

Your profile helps people connect with you on Facebook. Take a second to review some of the info on your profile and who you're sharing it with.

Email

 @facebook.com

 Friends ▼

 @gmail.com

 Public ▼

Birthday


October 26

 Friends ▼

 Friends ▼

Hometown

California

 Friends of Friends ▼

Relationship

Married to

 Friends of Friends ▼

Just a reminder, you may have more info on your profile. Go to the [About](#) section of your profile to make sure it's up-to-date and shared with who you want.

About Page

Finish Up!

Your profile

Here you can see the privacy setting on your email addresses, birthday, hometown, relationship status and other personal details about your life. Under emails it will show the one you registered with when you first signed up for Facebook as well as one Facebook has assigned to you (which you likely will never use). I discovered that I left my Gmail account public, which I hadn't meant to.

For your birthday, the sharing settings are split between the day/month and the year. That way your Friends can wish you happy birthday on Facebook on your special day without necessarily knowing your exact age.

For hometown, this setting only affects what your Friends can see. Advertisers and others may still access this information, especially if you are using the Facebook app which tracks your location automatically.

Finally, if you have set a relationship with another Facebook user, it will be shared unless you set otherwise.

It's important to note that this is only a PARTIAL list of the information you're sharing. To see the full list, click the About Page button, which will take you to your profile page. On there, you can review the various sections—Work and Education, Places You've Lived, Contact and Basic Info, Family and Relationships, Details About You—and make changes accordingly using the icons in the top right corner.

Privacy Settings and Tools

| | | | |
|-----------------------|---|-----------------|----------------------------------|
| Who can see my stuff? | 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 |
| Who can contact me? | Who can send you friend requests? | Everyone | Edit |
| | Whose messages do I want filtered into my inbox? | Basic Filtering | Edit |
| Who can look me up? | Who can look you up using the email address you provided? | Everyone | Edit |
| | Who can look you up using the phone number you provided? | Everyone | Edit |

The advanced privacy options

Here you can exert more control of what is being shared with whom. Which is never a bad idea. You've likely gone through this at least once in the past, but it's a great idea to review your settings at least once a year.

To get to the advanced privacy settings, click the drop down arrow in the top right on any Facebook page, click "Settings," and then "Privacy" in the left navigation column.

Who can see my stuff?

Who can see your future posts? This is the same as the Your Posts section above.

Review all your posts and things you're tagged in Ever been tagged in an embarrassing photo uploaded by that distant college classmate? You can use the Activity Log page and select the Posts You've Been Tagged In (in the left column) and the Photos > Photos of You (also in the left column) to check out what you've been tagged in. You can then remove the tag (click the checkbox on the left of the post or photo and then click on the the Remove Tag button at the top of the page) or simply hide them from your Timeline (click on the cog wheel to the right of the post or photo.)

Limit the audience for your old posts for your Timeline This will revert all your previous posts from "Public" or "Friends of Friends" to just "Friends". But if you've tagged a Friend in one of your posts, their Friends can see that since that is the default setting when tagging someone.

Who can contact me?

Who can send you friend requests? The default is Everybody, but the only other choice is Friends of Friends.

Whose messages do I want filtered into my inbox? When you see the word inbox, you think email, but Facebook means messages from other Facebook users. Click on Messages under your profile picture in the upper left corner of the screen. You'll see an Inbox column with many of the messages you've received from your Friends and a second tab marked Others. Using the Basic Filtering option here, you'll see messages from Friends and Friends of Friends. The Others tab will have messages from other people which **Facebook defines as:**

- A member of a group you're in messages you or includes you in a message
- A friend who isn't on Facebook uses your contact info to send you a message from the Messenger app

The Strict Filtering option will move Friends of Friends messages to the Other tab.

Who can look me up?

Who can you look you up with the email address you provided? If someone types in the email address you registered with, they can send you a message which will likely land in the Other tab on the Messages page. You can restrict it to Friends of Friends or just Friends (who can message you anyway), if you don't want to be bothered.

Who can look you up using the phone number you provided? Same as the email address.

Do you want other search engines to link to your timeline? Your first impulse may be to turn this off, but Facebook only allows information you've marked as Public to be shown to other search engines. They see it as a way for friends not on Facebook to find you. They do this with your basic information they always make public which is, according to Facebook, "...your name, gender, username and user ID (account number), profile picture, cover photo and networks."

Timeline and Tagging Settings

| | | | |
|--|--|--------------------|-------------------------|
| Who can add things to my timeline? | Who can post on your timeline? | Friends | Edit |
| | Review posts friends tag you in before they appear on your timeline? | Off | Edit |
| Who can see things on my timeline? | Review what other people see on your timeline | | View As |
| | Who can see posts you've been tagged in on your timeline? | Friends of Friends | Edit |
| | Who can see what others post on your timeline? | Friends of Friends | Edit |
| How can I manage tags people add and tagging suggestions? | Review tags people add to your own posts before the tags appear on Facebook? | Off | Edit |
| | When you're tagged in a post, who do you want to add to the audience if they aren't already in it? | Friends | Edit |
| | Who sees tag suggestions when photos that look like you are uploaded? | Friends | Edit |

Timeline and tagging options

Now that you've mastered the basics, go down to the next section, Timeline and Tagging. From there, you can control exactly who sees what on your timeline, who can post to your timeline, and who can tag you in photos and posts.

To customize your timeline settings, click on the down arrow in the far upper right corner to reveal a drop-down menu and select Settings.

Who can add things to my timeline?

Who can post on your timeline? It's set by default to Friends and the only other option is to allow only yourself to post on your timeline.

Review posts friends tag you in before they appear on your timeline? If you are concerned about getting tagged in a photo that you don't want all your friends on Facebook to see, this is the setting for you. Once enabled, you'll have to manually approve any photo or posts you are tagged in before they appear on your timeline. Note that this only affects your timeline; those updates will still appear in searches, the news feed and other places unless you un-tag yourself.

Who can see things on my timeline?

Review what other people see on your timeline? This is a perfect way to check that your mother or boss won't see what you don't want them to.

Who can see posts you've been tagged in on your timeline? These areas give you a great deal of flexibility, with options ranging from Everyone to Friends of Friends to custom lists. Using these two in conjunction with manually approving what photos and updates you've been tagged in goes a long way to keep prying eyes away from more sensitive Facebook updates.

Who can see what others post on your timeline? This area gives you a great deal of flexibility, with options ranging from Everyone to Friends of Friends to custom lists. Using this in conjunction with manually approving what photos and updates you've been tagged in goes a long way to keep prying eyes away from more sensitive Facebook updates.

How can I manage tags people add and tagging suggestions?

Review tags people add to your own posts before the tags appear on Facebook? This is an important option if you are concerned about a photo popping up on your timeline. This applies only to photo tagging by your Facebook friends. You'll always be notified if someone who's not your friend tags you in a photo.

When you're tagged in a post, who do you want to add to the audience if they aren't already in it? This one sounds more complicated than it is. Often a Facebook friend of yours will make a post and tag you in it. The option here allows all of your Facebook friends to see an update or photo you've been tagged in by someone they aren't friends with themselves (the Friends of Friends function). You can choose to remain tagged but have none of your other Facebook friends see that update, limit who sees that update to certain groups of friends, or you can outright block certain Facebook friends altogether by using the Custom option.

Who sees tag suggestions when photos that look like you are uploaded? Facebook uses face-matching technology to suggest who you should tag in photos. It will only suggest people that are on the user's friends list. If you don't want to show up as an option when your friends are tagging photos, set this to No One.

Manage Blocking

| | | |
|----------------------------|---|---------------------------|
| Restricted List | When you add friends to your Restricted list they can only see the information and posts that you make public. Facebook does not notify your friends when you add them to your Restricted list. | Edit List |
| Block users | Once you block someone, that person can no longer see things you post on your timeline, tag you, invite you to events or groups, start a conversation with you, or add you as a friend. Note: Does not include apps, games or groups you both participate in. | |
| | <div><div>Block users</div><div><input type="text" value="Add name or email"/></div><div>Block</div></div> | |
| Block app invites | Once you block app invites from someone, you'll automatically ignore future app requests from that friend. To block invites from a specific friend, click the "Ignore All Invites From This Friend" link under your latest request. | |
| | <div><div>Block invites from</div><div><input type="text" value="Type the name of a friend..."/></div></div> | |
| Block event invites | Once you block event invites from someone, you'll automatically ignore future event requests from that friend. | |

| | |
|--------------------|---|
| | <div>Block invites from <input type="text" value="Type the name of a friend..."/></div> |
| Block apps | Once you block an app, it can no longer contact you or get non-public information about you through Facebook. Learn more. |
| | <div>Block apps <input type="text" value="Type the name of an app..."/></div> |
| Block Pages | Once you block a Page, that Page can no longer interact with your posts or like or reply to your comments. You'll be unable to post to the Page's Timeline or message the Page. If you currently like the Page, blocking it will also unlike and unfollow it. |
| | <div>Block Pages <input type="text" value="Type the name of a Page..."/></div> |

Manage blocking

If you want to take steps to keep people away from your profile, this is the section for you.

Restricted list

If you don't want to un-friend somebody but also don't want them to see all of your information, you can add them to the Restricted List. This means they can see your public information, but they have no way of knowing you've limited their view (unless they happen to see someone browsing your profile who isn't restricted).

Block users

You can also just straight up block somebody. This means this person cannot be your friend. This is an excellent setting if you have stalkers or other people consistently bothering you. Note that this does not stop them from interacting with you in apps, games or groups you're both a part of.

Block app invites

In addition to blocking and restricting people from your profile, you can also block app invitations on a user-by-user basis. So if your Aunt Jackie keeps bombarding you with FarmVille apps, you know what to do.

Block event invites

Tired of your nephew inviting you to his New York City raves every weekend? Typing the name of the Facebook user into this section will stop you from seeing any future event invites from that person.

Block apps

Some apps and Facebook games are great fun at first, but after a while, you want to drop them. You can remove the app or game (see the Apps you use section, below) or block the app, which means it can no longer contact you or get non-public information about you through Facebook. If you are getting emails from the app, you will have to use the unsubscribe link at the bottom of the email.

Block pages

This will remove all notifications and functionality with a Facebook Page (a public page for businesses and celebrities).


App Settings


Logged in with Facebook 2


Logged in Anonymously


Search Apps


On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available, including to apps ([Learn Why](#)). Apps also have access to your friends list and any information you choose to make public.

**Goodreads**
Friends

**Marvel: Avengers Al...**
Only Me

 **Apps, Websites and Plugins**
Lets you use apps, plugins, games and websites on Facebook and elsewhere.
Enabled.
[Edit](#)

 **Apps Others Use**
People who can see your info can bring it with them when they use apps. Use this setting to control the categories of information people can bring with them.
[Edit](#)

 **Old Versions of Facebook for Mobile**
This setting controls the privacy of things you post using old Facebook mobile apps that do not have the inline audience selector, such as outdated versions of Facebook for BlackBerry.
[Friends](#)

Customize app privacy

You handled a lot of this with the Privacy Checkup, but in the Settings section there is additional controls for the Facebook apps you use.

App settings

If you haven't already, you can click on each app and change who can see the updates they put on your timeline or disable them altogether.

Apps, websites and Platforms

Disabling this option means not only will all apps working with your account stop working, but you won't be able to log in to websites or other third-party sites with your Facebook account.

Apps others use

When your Facebook friends use certain apps, those apps access your public information and more. See a full list in the image to the right. There's quite a bit you may not be comfortable

Apps Others Use ×

People on Facebook who can see your info can bring it with them when they use apps. This makes their experience better and more social. Use the settings below to control the categories of information that people can bring with them when they use apps, games and websites.

sharing without your knowledge. Most of it is enabled by default. Be sure to go through the list and check off what you don't want shared.

And that's Facebook Privacy in a nutshell

That covers your privacy setting options on Facebook. If you want to dig in even further, Facebook has a page explaining the basics of Facebook privacy tools as well as Facebook's latest data policies.

[shocked woman with laptop via Shutterstock, all other images via Facebook]

- ☒ Bio

☒ Birthday

☐ Family and relationships

☐ Interested in

☐ Religious and political views

☒ My website

☒ If I'm online

☐ My status updates

☐ My photos
- ☐ My videos

☐ My links

☐ My notes

☐ Hometown

☐ Current city

☐ Education and work

☐ Activities, interests, things I like

☐ My app activity

If you don't want apps and websites to access other categories of information (like your friend list, gender or info you've made public), you can turn off all Platform apps. But remember, you will not be able to use any games or apps yourself.

CancelSave

7 must-know privacy tips for Instagram newbies

by [ben patterson](#) on april 28, 2015, 11:11 am

in [apps](#) | [how-tos](#) | [phones](#) | [privacy](#)



So, what's the big deal about [Instagram](#), you ask? Well, it's not just a smartphone app for adding eye-popping color filters and blur effects to your photos. Above all, Instagram is about sharing your latest snapshots with friends, other Instagram users, and yes, the world.

But what if you're not feeling the need to show off your Instagram-dipped photos to ... you know, everyone? Luckily, it's easy to control exactly who does—and doesn't—get to see your latest works of digital photo art.

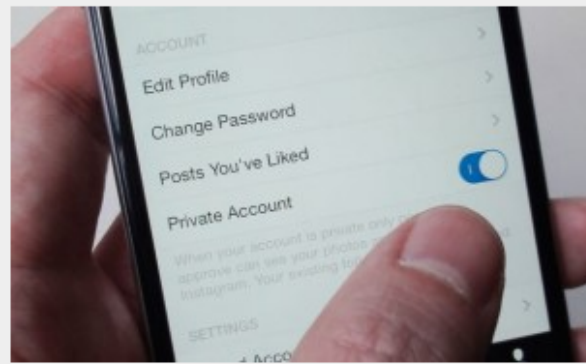
Read on for a few beginner-focused tips on how to get the most out of Instagram without becoming an exhibitionist in the process, starting with...

1. Change the privacy setting for your photo feed

Taking a photo with Instagram doesn't just save the image to your phone's photo gallery. It also publishes your snapshot to your Instagram photo feed—which, by default, is wide open to anyone who cares to look.

Don't want just anyone gawking at your Instagram pictures? If not, just turn on "Private Mode," which blocks your Instagram photo feed from everyone except your hand-picked "followers."

- Tap the profile button in the bottom-left corner of the Instagram interface (it's the one that looks like a little silhouette), then tap the Settings icon (in iOS, the one that looks like a gear, or the three-dot button for Android) in the top corner of the screen.
- Now, see the "Private Account" setting? Flip the switch to the "on" position.



Don't want just anyone gawking at your Instagram pictures? Set your account to "private."

All done? If so, your Instagram photos are no longer accessible to the public, nor will they show up in public searches.

Of course, all bets are off if you decide to share your Instagram shots on Facebook or Twitter, so make sure to double-check which social services are selected on the final confirmation page before tapping the "Share" button (or, in the case of Android, the blue button with the checkmark).

Speaking of which...

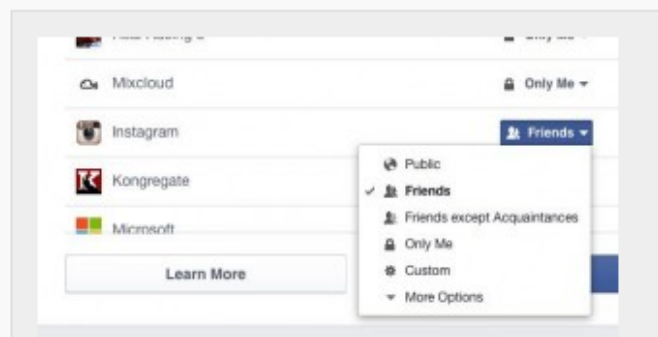
2. Double-check your Facebook sharing settings

Instagram makes for an easy-as-pie way to share your latest photos with your Facebook friends. Here's a question, though: when you share Instagram photos through Facebook (which you can do by tapping the Facebook setting on the final confirmation pag

e before posting a photo to your feed), who are your photos being shared with?

Well, there's an easy way to check exactly how Instagram is sharing your snapshots on Facebook.

- Visit your Facebook account, click the Privacy Shortcuts (the one shaped like a padlock) in the top-right corner of the page, select Privacy Checkup, then click the blue Next Steps button.



There's an easy way to check exactly how Instagram is sharing your snapshots on Facebook.

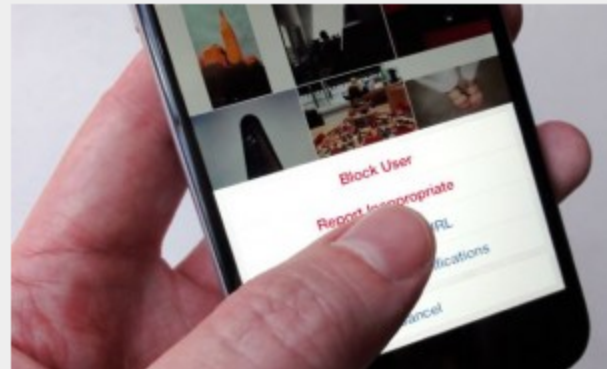
- Find Instagram in the “Your Apps” section (assuming you’ve already connected Instagram to your Facebook account), then check its privacy setting (anything from “Public” to “Only Me”). Want to make a change? Just select a new setting from the pull-down menu.

3. Block random followers

As with Twitter, anyone on Instagram can follow the photo feed of anyone else—including you—unless their profiles are set to “private.”

Let’s say, though, that a few strangers managed to follow your Instagram photos before you set your account to private mode. Now what?

If you don’t want random followers checking out your snapshots, you can always just block them.



If you don’t want random followers checking out your snapshots, you can always just block them.

- First, head to your profile by tapping the profile button in the bottom-right corner of the screen.
- Now, see where your number of Instagram followers is listed? Tap the number, and you’ll arrive at a list of all the Instagram users following your photo feed.
- See anyone you don’t want thumbing through your photos? Tap their name to view their profile, then tap the three-dot menu button in the top-right corner of the screen.
- A pop-up window will appear with a few options, including “Block User.” Tap “Block User,” and clang! No more peeking at your Instagram photos for them.

4. Edit your profile

Your fellow Instagram users (well, the ones you don’t already know in real life, anyway) only know as much about you as you reveal in your Instagram profile.

Indeed, the only detail you need to reveal in your profile is your Instagram user name—which could be anything, really.

To edit your profile, tap the profile button in the bottom-right corner of the page, tap the Edit Your Profile button, then add—or delete—any personal details you like.

5. Wipe photos off Instagram’s photo map

Instagram boasts a nifty feature that pins any photos you choose to a “photo map” that’s viewable from your profile.

Snap the vista from, say, the top of the Empire State Building, and other Instagram users will see it pinned to a map of midtown Manhattan, if you so choose.

It’s a neat feature for showing your friends where you trekked on your vacation, but you might want to think twice before sharing your home address—or the location of your friends’ homes, for that matter.

Before sharing a photo on Instagram, take note of the “Add to your Photo Map” setting on the final confirmation page, then ask yourself: do you really want the location of your photo pinpointed on a map?



What if you’ve already posted a stack of Instagram photos on your photo map? Never fear. Here’s how to peel them off.

If not, make sure the “Add to your Photo Map” setting is switched off.

OK, but what if you’ve already posted a stack of Instagram photos on your photo map? Never fear. Here’s how to peel them off.

- Tap the profile button in the bottom-right corner of the screen, tap the Photo Map tab (it’s the teardrop-shaped icon) on your profile page, then tap the Edit button in the top-right corner of your Photo Map.
- Zoom in and tap a specific photo you’d like to wipe off your Photo Map.
- Another option: tap the grid button at the bottom of the screen (for iOS) or tap the three-dot menu button in the top corner of the screen and select “View All” (on Android) to “deselect” some or all your Instagram photos from your map.

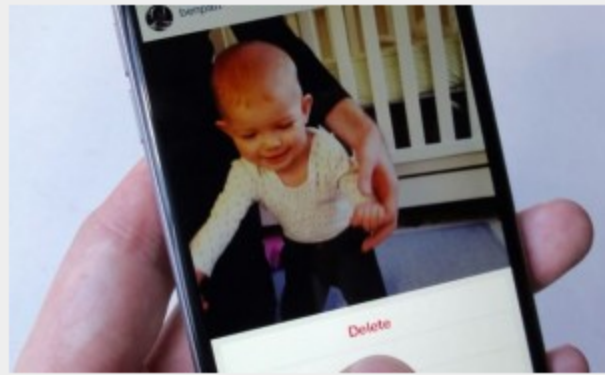
Note: Have you already set your Instagram photos to “private”? If so, no one else but you can see your photo map, not even your followers.

6. Delete photos from your photo feed

Did you take and share a photo on Instagram that, on second thought, you wish you hadn’t?

No, you can't make your Instagram followers "unsee" a photo (oh, if only you could), but you can delete it from your photo feed even after you've shared it.

- Tap the profile button in the bottom-right corner of the screen.
- Below your profile details, you should see all the photos you've shared in Instagram. If your photos are displayed in a grid, tap one to select it; otherwise, just scroll to the photo you want to delete.
- Just below the photo and over to the right, you'll see a little menu button marked with three dots; tap the button, and a pop-up will appear with a series of options, including a "Delete" button. Tap "Delete," and whoosh—your photo's gone from your Instagram photo feed, if not from the memories of your followers.



You can't make your Instagram followers "unsee" a photo, but you can delete it from your photo feed even after you've shared it.

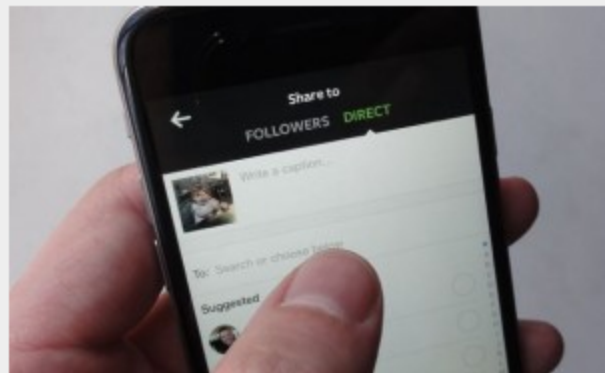
7. Share photos only with specific Instagram followers

Just snap a pic that you'd like only a few of your Instagram followers to see? Well, you're in luck.

A feature called "Instagram Direct" lets you pick and choose which Instagram pals can see your latest snapshot.

Here's the trick: take a new photo using the Instagram app, then tap the "Direct" tab when you arrive at the final confirmation page.

When you do, you'll see a list of all your Instagram followers; just scroll down and select the ones with whom you'd like to share the photo.

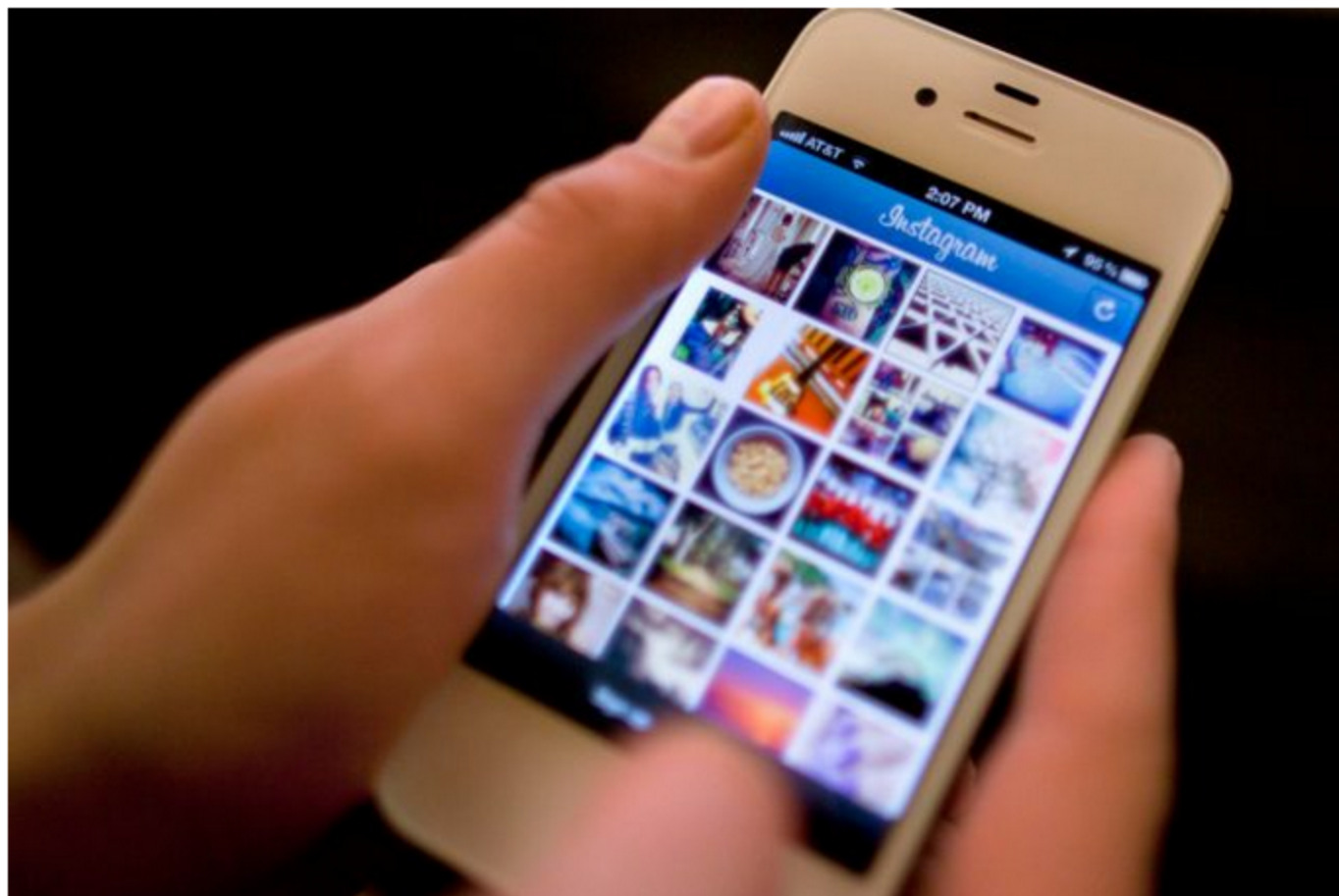
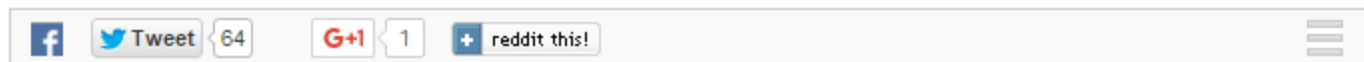


A feature called "Instagram Direct" lets you pick and choose which Instagram pals can see your latest snapshot.

Tue Feb 10 2015 Posted by Simone Lai at 06:00 AM

What you need to know about Instagram privacy settings

How to make your posts private and other tricks on keeping your data safe on Instagram.



AP PHOTO

Your baby's first smile. Your new house. Your last-minute vacation.

Your exact location.

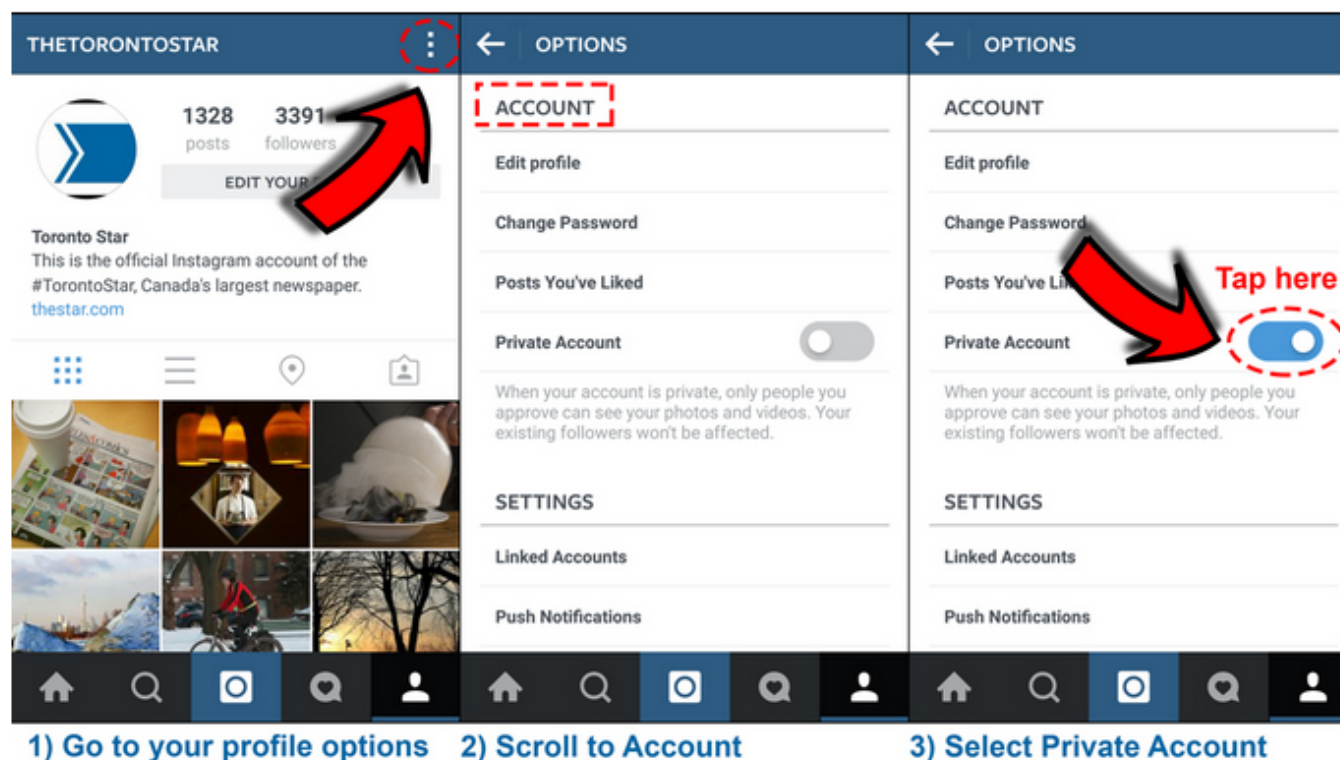
With every post you share on Instagram, you're exposing little bits of information. Some of this is harmless. But imagine if someone figured out exactly where you live and that nobody would be home for the next week. Are you setting yourself up for an easy break-in? Are you putting your family and friends in danger?

You might be. By default, your Instagram posts are public.

How can I change this?

On your profile page beside your profile picture, tap the profile options icon (iPhone users will have a gear

icon, Android users will see three dots) and set your profile to “Private Account”. New followers will now have to request your permission to see any of your posts.



Here's how to change your Instagram privacy settings.

That was easy. Is that all?

Not quite. If you are posting your Instagram photos and videos to other social media platforms like Twitter, Facebook and Foursquare, they will be visible based on the privacy settings you have set there. If someone has access to the actual Instagram link, the post will also be visible.

What if I don't want a certain follower to see my posts?

If you have followers you don't want, especially if your profile was public, you will have to specifically block those users. Not to fear; they will not be notified that they have been blocked.

What about hashtags? Will my photo hashtagged with #selfie be visible to everyone searching #selfie?

If you hashtag your posts and your profile is private, only your followers will be able to view the content. It will not be visible to the public.

Should I add photos to my Photo Map?

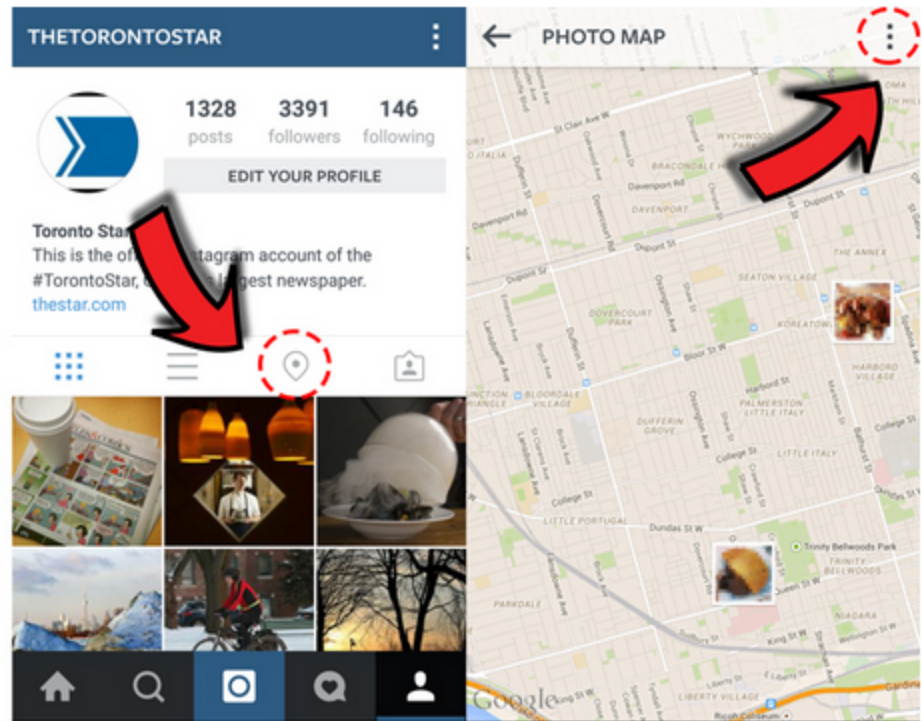
An old social media experiment from 2013 showed comedian [Jack Vale](#) surprising people at a California shopping centre by calling out their names and nicknames, wishing one woman a happy birthday, and even describing someone's pet dog left at home. He did this all by doing a simple search for people near his location.

That's why you should think twice about adding pictures to your Photo Map. If your posts are set to private, only your followers will be able to see your Photo Map. The location is also visible to anyone you send direct photos or videos to. So yes, geotag your poolside cabana and Mount Everest hike photos to make your followers jealous, but you might not want to use Photo Map for photos taken in your home, office, or friends' homes.

Oops. Is there a way I can wipe a private location I've already put on Photo Map?

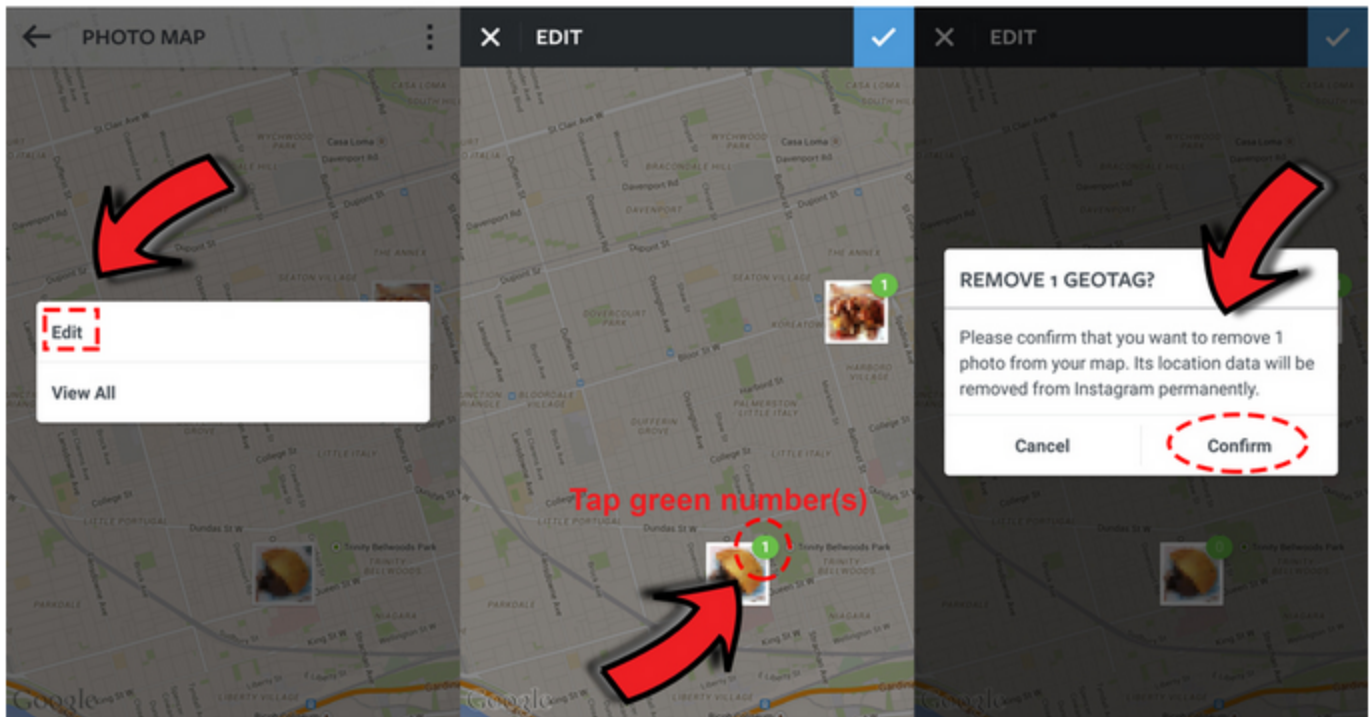
Yep. Follow these steps on how you can wipe that information:

How to remove photos from your Instagram Photo Map



1) Find your map here

2) Click here to edit map



3) Select Edit

4) Choose which photos to remove

5) Confirm your changes

« Newsweek Twitter feed briefly hacked, ISIS's Cyber Caliphate claims responsibility

How popular apps allow advertisers see our personal information »
