Take control

Customizing your social media privacy settings

The online community created by social media platforms can offer all sorts of rewards—new friends, entertainment, a forum for learning, and much more. But sharing on the internet can also raise real privacy risks. This publication presents the potential consequences of oversharing on social media, explains how to achieve your desired level of privacy on the most popular social media platforms and provides useful privacy tips, tools and resources.

The importance of privacy

The internet, social media and other digital options for interacting allow us to reach friends—and strangers—all around the world. While that can be a powerful tool for creating community, most people find it desirable—and smart—to have limits on what is revealed about them and to whom.

For example, it can be risky to broadcast:

- Your schedule and/or travel plans
- What your birthdate and/or mother's maiden name is
- Your children's names and what schools they attend
- Your marital and/or financial status
- A photo of you "partying"

With a chosen audience of family and friends, all this information might be perfectly safe. But when shared with strangers or an unintended audience, they can open you up to harassment or unwanted attention, a damaged image, professional repercussions, stalking, ID theft and other consequences.

Fortunately, social media platforms have evolved to enable users to choose how much privacy

they want and adjust the platform's privacy controls to match their needs.

Levels of control

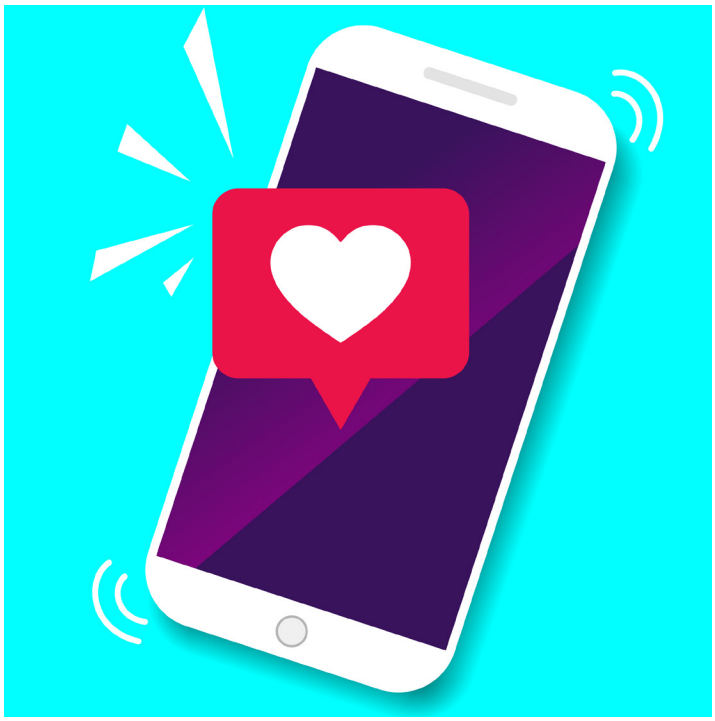
Which privacy controls you are able to adjust, and what your options are for customization, will vary from platform to platform. For example, one may allow you to be more specific in selecting your audience than another. It's important to understand, *before* you begin using a social media platform, what you can—and *can't*—control. If you can't achieve the level of privacy you're comfortable with, you should choose a different platform that better meets your needs.

Typical areas that you'll have some control over in most social media platforms include:

- Profile details (who can see personal information like where you live, relationship status or contact info)
- General audience (who can see your content)
- Audience for a single piece of content (who can see a particular tweet, photo, story, video, etc.)
- Photo tagging (whether you are identified by name in a photo and where the image appears)
- Location sharing (whether your location is announced at the time of a post)
- Activity status (whether others can see the last time you were active on the platform)

In addition to these more common privacy settings, social media platforms offer many other options, including some that may be unique to a particular platform. The only way to know what all your privacy options are is to visit the website or app's *Privacy* or *Help* section. (You can also get tips from users and tech writers by doing an online search for "[name of platform]" plus "privacy options" or "privacy settings" or similar keywords.)

There are also aspects of privacy you won't be able to control on all—or maybe any—platforms. Things like data collection (or sharing) by the



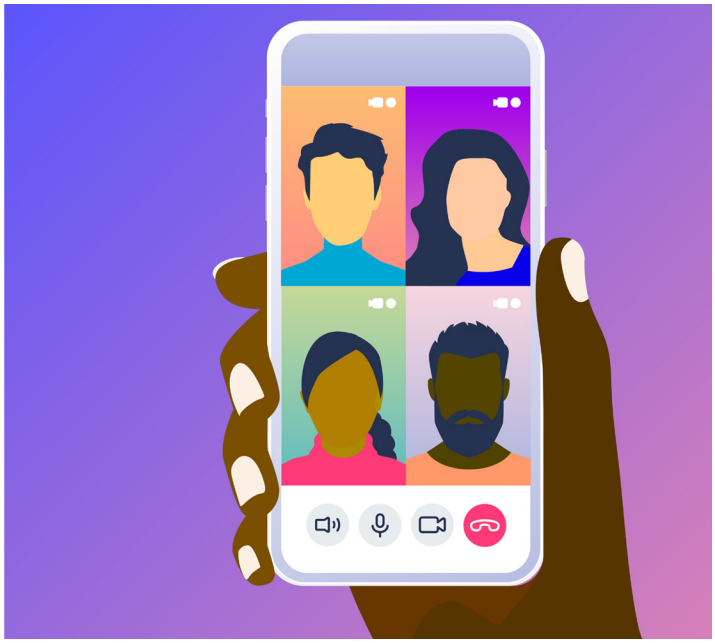
platform itself might be unalterable or partially controlled. If that is unacceptable to you, your only option is to avoid the platform.

Customizing your privacy

All social media accounts start out with the default privacy settings when you open your account. Before your very first post (tweet, etc.), you should adjust the level of privacy to match your preferences. To do this, log in to your account and find the *Settings* (or, in some cases, *Privacy*, or *Settings and Privacy*) section (often found under your profile icon or a "gear" or "tools" icon, or use the *Help* or *Support* features to find and understand the platform's features and tools).

Following is some basic information (and a few tips) for customizing the privacy settings for some of the most popular social media platforms. (You can also do an online search for the name of the social network plus the words "privacy settings" or "privacy tips" to find additional guidance.)

Facebook (*https://www.facebook.com*): Facebook enables users to connect and share with family, friends and communities via their website and mobile app. Certain profile information, including name, profile picture and cover photo,



gender, and username is visible to the public. You have the option to customize a number of other settings, including who your audience will be for your posts, who can see and post to your "timeline," who can send you "friend requests," what information apps can collect from you, whether your profile can be found by search engines, and much more. You can also control your exposure to particular individuals by "unfriending," "unfollowing" or blocking them. Facebook's *Privacy Checkup* helps you review some important privacy settings (on the Facebook website, click the "?" icon in the top right corner of your screen and select *Privacy Checkup* from the menu. From that same "?" menu, you can access *Privacy Shortcuts* (*https://www.facebook.com/privacy/*), a lengthier list of privacy and security options. To access *Privacy Checkup* in the app, select the menu in the bottom right corner of the screen, open *Settings & Privacy*, then *Settings*, and click *Check a few important settings*. *Privacy Shortcuts* is available directly under *Settings* and *Privacy*.

TIP: Many apps and websites allow you to log in using your Facebook username and password. Make sure to check what information the app is requesting permission to access, and limit categories you don't want to share. If you have already used Facebook to sign in to third-party apps or services, you can manage the data you're sharing with the app or website in the *Apps and Websites* section of Facebook's *Settings*.

Instagram (*https://www.instagram.com*): Instagram is a photo- and video-sharing app (owned by Facebook) that allows users to share pictures and short videos with followers, who, in turn, can comment on the images. By default, anyone can view your profile photos and "stories" (photos/videos that vanish after 24 hours), but you have the option to make them private so that only your approved followers can see what you post. You can also remove followers, hide your activity status, block comments on a post, stop people from resharing your story as a message, turn on or off sharing of your Instagram posts to other social networks (Facebook, Twitter, Tumblr, etc.), and more. (Regardless of your privacy settings, any user will still be able to read your bio, and send a photo or video to you directly.) The majority of Instagram's privacy settings are accessed through the mobile app; click on the profile icon in the lower right corner of the screen, then click on the menu icon (three horizontal lines) in the upper right corner, select *Settings* at the top of the list, and from there you can access *Privacy*, *Security*, and other options. Each time you click through to post photos or videos on Instagram, you have the opportunity to view additional settings. Learn more in the Instagram *Help Center* (*https://help.instagram.com/196883487377501*) and the *Privacy and Safety Center* (*https://help.instagram.com/285881641526716*).

TIP: Anyone can tag you in photos and videos on Instagram, except for the people you've blocked. Since not every photo will be one you want to share, you can choose to approve images manually before they appear on your profile (in the app, under *Settings*, tap *Privacy*, then *Tags*, and toggle on *Manually Approve Tags*).

LinkedIn (*https://www.linkedin.com/*): LinkedIn is a platform for professionals, who can share their employment histories, resumes and portfolios; network with other professionals; build their "brands"; and, if desired, look for new jobs. You have control over a number of account and privacy settings, including what you share about yourself and with whom (profile, email address,

connections, etc.), who can see when you're logged in, who is allowed to follow you, and how the platform itself uses your data. If you don't want everyone to know what companies you're following, who you're recommending or every change you make to your profile, be sure to uncheck the *Activity Broadcasts* setting. If you don't want those outside of your network to subscribe to your activity updates (without adding you as a connection), go into the *Choose who can follow your updates* setting and limit this audience to your connections rather than the public. Learn more on the platform's *Managing Your Account and Privacy Settings: Overview* page (*https://www.linkedin.com/help/linkedin/answer/66*). View and change your account and privacy settings at *https://www.linkedin.com/psettings/*.

TIP: If you don't want people to know that you've viewed their profile, turn on the private profile viewing mode. This setting is available in the *Privacy* section of *Settings*, under *Profile viewing options*.

Pinterest (*https://www.pinterest.com/*): Like Instagram, Pinterest is a visually-oriented platform; it allows users to "pin" images and videos of interest (often within a chosen theme) to their boards, browse what others have pinned and share their own curated "board." Compared to other social media platforms, Pinterest's privacy settings are pretty straightforward. You have the option to hide your profile from search engines, and to hide your "pins" from other people by using "secret" boards that are visible only to you and people you invite. These and other options can be accessed by clicking on your profile icon and choosing *Settings*. Get more information about privacy settings in the Pinterest *Help* section: *https://help.pinterest.com/en/article/edit-account-privacy*.

TIP: Pinterest and third parties it partners with use information about your visits to other sites and the apps you use to personalize ads you may see online. If you'd prefer random ads (rather than feeling like you're being monitored) you can set the *Use info from our ad partners* tab to "No" in *Settings*.

Snapchat (*https://www.snapchat.com/*): Snapchat is a messaging app used to share photos, videos, text and drawings that disappear in a few seconds or, in the case of "stories," 24 hours. The short lifespan of "snaps" can give users a false sense of security (in other words, privacy isn't an issue since nothing will be visible for long). Users should still go through the steps of customizing some privacy settings. By default, only users you have added as friends can send you "snaps" or view your "story." However, you should disable the *Quick Add* feature if you don't want to show up in the "suggested" lists of your friends' friends. If you do end up being added to random users' friend lists, you can block them in the *Added Friends* > *Added Me* section under your profile. Your location on "Snap Map" only updates when you have Snapchat open, but you may not want to share it. Your options include *Ghost Mode* (your location won't be visible to anyone else), *Select Friends* (choose specific individuals) and *My Friends* (all the friends you've added) (*https://support.snapchat.com/en-US/news/ghost-mode-timer*). Learn more about your account privacy options at the *Snapchat Support* page (*https://support.snapchat.com/en-US/article/privacy-settings2*).

TIP: While Snapchat gives the illusion of impermanence, it's possible for a recipient to take a screenshot of a Snap you send, making it permanent (and shareable). The app will notify you if a recipient took a screenshot of your message. That knowledge should help you decide what to send to that person in the future. While these notifications are helpful, be aware that there are tutorials online that explain how to take a screenshot and *not* trigger the notification!

Tumblr (*https://www.tumblr.com/*): Tumblr is a blogging platform that enables users to post images, GIFs, videos, music, text, links and more. The platform allows users a limited number of privacy controls, such as hiding your activity status, preventing people from finding you via your email address, hiding your blog from search engine results, and putting restrictions on which third-party apps—if any—can access your Tumblr data. Visit the Tumblr *Help Center* for information about which settings you can adjust and how: *https://tumblr.zendesk.com/hc/en-us*.

TIP: Your primary blog—the one you set up

when you open a Tumblr account—is public, and not password-protected, by default. For more privacy, you can set up secondary blogs, which can be password-protected so that only visitors with the password, or Tumblr users you've added as members, can access it.

Twitter (*https://twitter.com/*): Twitter allows users to communicate in short messages (280 characters) called tweets, which can also include links, photos and videos. By default, your Twitter account is public, meaning your tweets and information can be viewed by anyone. You have the option to make your account private, meaning that: only Twitter users you have approved can subscribe and see your tweets; tweets that were previously public will be hidden from anyone but your approved followers; your tweets will no longer appear in Google searches or be "retweetable"; and any direct replies you send will not be seen, unless you send them to your approved followers. You can make this and other changes in the *Privacy and safety* section (*https://twitter.com/settings/safety*) of your account settings. While there, uncheck—or do not check—the *Add a location to my Tweets* box if you want to keep your location private (advisable). You can also make some choices about individual tweets you send and receive. Visit Twitter's *How to control your Twitter experience* page (*https://help.twitter.com/en/safety-and-security/control-your-twitter-experience*) for a clear guide to what you can and can't control on the platform.

TIP: If you are sensitive to certain words or phrases, you can "mute" (filter out) tweets that contain them by adding those words to your list. Look for *Muted words* under *Settings and privacy*. You can also "block" or "mute" entire accounts, a key difference being that when you block someone, they are notified, while muting is more subtle (no notification).

YouTube (*https://www.youtube.com/*): YouTube is a video sharing service. When you upload a video, it is set as "Public" by default, which means anybody can view it. But you can change that to "Private" or "Unlisted" during upload or later. A private video won't appear on your channel or in search results, and can only be seen by you and the audience you select. An unlisted video means that only people whom you've given the video link to can view it and post comments. Unlisted videos don't appear in the *Videos* tab of your

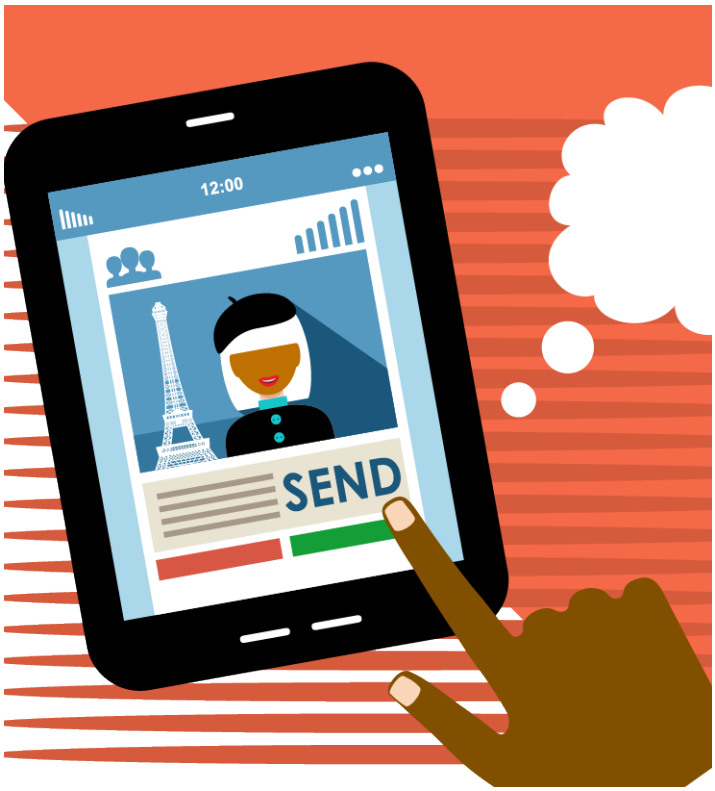
channel page or in YouTube's search results (unless someone adds your unlisted video to a public playlist). If someone has posted your personal information or uploaded a video of you without your consent and they refuse to remove it, or you are uncomfortable contacting them, you can ask YouTube to remove the content (*https://support.google.com/youtube/answer/2801895*). Visit YouTube's *Privacy and safety center* for more information about using YouTube safely (*https://support.google.com/youtube/topic/2803240*).

TIP: If you don't want your viewing history being shared on social media, don't click "Share," "Like" or similar buttons associated with a posted video. If you do want to share this information, be sure you have selected the desired audience.

Privacy best practices

1. Do your due diligence. Check the social media platform's privacy policy before opening an account to find out how your personal information and/or the data on your device could be used, and how much control you have over your privacy. You probably don't have much control over the company's collection of your data while you are at the site or in the app, but it might give you some control over data sharing with third parties, whether or not you see targeted ads, and the collection of specific types of data such as precise location. If you open an account, read all notices from the company so that you don't miss any policy changes. If you're unhappy with a change, cancel your account and/or uninstall the app. (If possible, download your data before leaving.)

2. Be discreet. You don't have to fill in every field when creating your profile—anyone who needs to know your birthdate, school, email address, phone number and other personal details most likely already does. Likewise, don't post information or photos—your vacation plans, your new sports car, the interior of your home, etc.—that might make you more attractive to scam artists or thieves. And understand that if you post something to another person's



profile, you have no control over who else sees it.

3. Think before you share. What might the repercussions be if your post, tweet, video, etc. were broadcast to the world? Since it's possible that something could be shared with people outside of your intended audience—purposely or unintentionally—ask "What would my parents, significant other, teachers, college admissions officer, current or future employer, coworkers, clients, lender, insurer, landlord, law enforcement, etc. think about this?" "How could a criminal, stalker, etc. use this information?" Protect your "e-reputation"—many people who do not know you personally may use social media as a source of information to judge you by.

4. Enlist your friends. Real friends care about your reputation and respect your privacy. Tell them what your privacy boundaries are and ask them to maintain them. If someone has posted something in their own social media account that could be an issue for you, ask them to remove it. If that doesn't work, you can find out if the social network has a policy for removing certain types of images or content if requested.

5. Smaller is often safer. Don't accept requests or invitations from people you don't know just to build up your audience. Instead, curate your lists, so you don't share with "followers" and connections that you don't know well enough to trust. The larger your inner circle, the greater the risk that your privacy and security could be compromised. Understand that anyone you've shared with can re-share or otherwise expose what you've shared. (Also, close any social media accounts you don't use anymore so that there's no risk of them being compromised.)

6. Lock intruders out. Use every available tool and safety practice to keep others out of your accounts and devices. Set strong passwords (an impossible-to-guess string of eight-plus characters). Use a different password for every social media account (password managers such as LastPass or 1Password can help you manage them). Enable two-factor authentication (login requires entry of a code sent to your device). Lock your phone so that a passcode is required to open it after a time-out of only a few minutes.

7. Keep your whereabouts under wraps. Don't share your location in real-time with your connections or the public on social media. While it might be relatively safe to say you recently spent a week in Hawaii, telling your audience that you're at the airport, en route to a two-week vacation in Maui, could put you at risk for burglary, stalking, etc. Turn off GPS tracking in apps for which location data isn't essential.

8. Resist temptation. That enticing story just might be clickbait (a piece of content designed to lure you to click a link that leads to nuisance, inaccurate or malicious content). Don't click on unknown links, which could be designed to infect your computer with a virus or data-stealing spyware. As enticing as they are, quizzes, games, coupon offers and other inducements are often just ways to get you to disclose personal information.

Learn more

StaySafeOnline.org Manage Your Privacy Settings page (*https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/*) provides direct links to instructions for customizing your privacy preferences in all of the most popular devices, search engines, social platforms, etc.

The University of Texas's Center for Identity website (*https://identity.utexas.edu/everyone/how-to-manage-your-social-media-privacy-settings*) provides detailed instructions and tips for managing your privacy on Facebook, Twitter, Instagram, Snapchat, LinkedIn and Pinterest.

FightingIdentityCrimes.com Social Media Security Center (*https://www.fightingidentitycrimes.com/social-media-education-center/*) provides a thorough overview of social media privacy (concerns, collected information, risks, etc.) along with links to instructions for adjusting your privacy settings on eight of the most popular platforms.

Electronic Privacy Information Center (EPIC) Online Guide to Practical Privacy Tools (*https://www.epic.org/privacy/tools.html*) teaches about all sorts of online privacy tools available to keep you safe online, from antivirus software and firewalls to password managers and virtual private network (VPN) software.

The Federal Trade Commission (FTC) Understanding Mobile Apps page (*https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps*) explains what

you need to understand about apps, including how to manage privacy and security concerns.

ZDNet offers tips to guide iOS (*https://www.zdnet.com/pictures/new-to-ios-11-change-these-privacy-and-security-settings-right-now/*) and Android users (*https://www.zdnet.com/pictures/android-phone-tablet-privacy-security-settings/*) through device-specific privacy settings. (You can also check the "Support" website for your device—for example, *https://support.apple.com/iphone* for the iPhone. If you're having difficulty, type in "How do I change the privacy settings on a [name of your type of device]?" in a search engine to get device-specific information.)

The California Department of Justice's Privacy Enforcement and Protection Unit offers its *How to Read a Privacy Policy* guide (*https://www.oag.ca.gov/privacy/facts/online-privacy/privacy-policy*) to help consumers understand a company's disclosures about how it will use the data it collects, and what they should reasonably expect. (Though it is from a California agency, the information is useful regardless of where you live.)

About Consumer Action

www.consumer-action.org

Through education and advocacy, Consumer Action fights for strong consumer rights and policies that promote fairness and financial prosperity for underrepresented consumers nationwide.

Consumer advice and assistance: Submit consumer complaints to: *https://complaints.consumer-action.org/forms/english-form* or 415-777-9635. (Spanish-language complaints can be submitted to: *https://complaints.consumer-action.org/forms/spanish-form/*.)

Our hotline accepts calls in Chinese, English and Spanish.

Consumer Action publications

Fake News: Recognizing and stemming misinformation (*https://www.consumer-action.org/english/articles/fake_news*) explains how internet users can have a real impact on thwarting fake news. Learn how to evaluate the accuracy of what you read or hear, avoid "fake news" and refrain from spreading false stories.

Watch out! Online video and your privacy (*http://www.consumer-action.org/modules/module_social_media_streaming*) explains the privacy issues presented by video streaming and video sharing technology and what you can do to protect yourself.

Put a Lock on It: Protecting your online privacy (*http://www.consumer-action.org/modules/articles/put_a_lock_on_it*) offers information about general online safety and privacy.

Personalized privacy: Customizing your Facebook settings (*https://www.consumer-action.org/english/articles/facebook_privacy_controls*) explains how Facebook users can protect their privacy, offers specific tips for fine-tuning your preferences on the Facebook website and in the app, and links to resources where readers can learn more.

About this guide

Consumer Action created this guide in partnership with Facebook.