Questions & Answers

Social media and online video privacy

This backgrounder is designed to help answer additional questions about the material presented in the Consumer Action brochures "What's not to 'Like'? Protecting your privacy on social media" and "Watch out! Online video and your privacy."

A Consumer Action Publication

www.consumer-action.org

Social media and online video privacy

Technology has changed the way we conduct even the most basic everyday activities, from communicating with friends to watching TV. For the most part, new internet-based capabilities have been welcomed as improvements. But interacting online is not without its privacy risks. This backgrounder can help answer many questions consumers have about staying safe and protecting their privacy while taking advantage of the internet.

I. General internet and data safety

What kinds of risks do internet users face?

While there have been significant improvements in internet security, there will always be those—hackers, scammers, stalkers, bullies, etc.—who try to take advantage of any opportunity. Specific risks include having your digital data or personal information taken and used in ways you wouldn't want, being harassed or bullied by someone, having your identity stolen, receiving spam and other unwelcome communications, landing on malicious or counterfeit websites, being exposed to pornography or hate speech, becoming the victim of a scam or fraud, or having your computer infected by spyware or malware.

Fortunately, there are many excellent tech tools you can employ and many simple but effective precautions you can take to stay safe on the internet.

What can I do to protect myself and my family online?

In a nutshell, you should always approach your online activities with the assumption that there are strangers on the internet who don't have your best interests at heart. If you have your guard up, you are better prepared to recognize and avoid potential risks. Your wariness, combined with practices and tools that protect personal data and privacy, will go a long way toward keeping you and your family safe in cyberspace.

What can I do to protect my computer and the data it holds?

There are many ways to protect your computer and data from intruders:

- Password-protect your home wireless network and turn on the encryption feature for your Wi-Fi router.

- Use a firewall.
- Install antivirus software and antispyware.
- Use a spam filter.
- Perform timely software and operating system (OS) updates.
- Set your computer to require a login password or PIN to start up or wake up.
- Back up your files regularly on an external hard drive that you do not keep permanently attached to your computer.

Learn more about firewalls and other tech tools as well as user precautions in Consumer Action's "Put a Lock on It: Protecting your online privacy" brochure (http://www.consumer-action.org/modules/articles/put_a_lock_on_it). You can also find online privacy tools and tips at the Electronic Privacy Information Center's (EPIC) site (https://www.epic.org/privacy/tools.html) and at tech sites such as ZDNet.com and CNet.com.

What can I do to protect my mobile device and the data it holds?

Some of the steps you should follow to protect your mobile device are the same as the ones that help you protect your computer, such as password protecting the device (requiring a passcode to unlock it) and installing software updates when they become available. Because mobile devices are portable, they are more likely to get lost or stolen than a full-size computer, so you should also enroll in a remote locate/lock/erase program such as Find My iPhone (Apple) or Android Device Manager. This allows you to find your device if you've misplaced it, remotely lock it while you try to find it, or delete your data if it's been irretrievably lost or stolen.

When it comes time to sell, trade in, donate or dispose of your device, be sure to "wipe" the data so that the next person who handles your phone can't access your personal information. CTIA-The Wireless Association offers tips and links to instructions for erasing the information on your particular type of mobile device (http://www.ctia.org/your-wireless-life/consumer-tips/tips/how-to-erase-data-on-your-mobile-device).

What do I need to know about password protection?

A strong password is a good way to protect your personal data, and the single strongest way to protect your mobile device from unauthorized access. Here are some tips:

- Create a password that is at least eight characters long and a random mix of letters, numbers and symbols. You can use an online tool such as www.PasswordsGenerator.net for help coming up with one. Consider using a pass*phrase*—a longer version of the password (for example, ilikecookies&milk).
- Use different passwords for your different accounts. Online tools can help you store your passwords without writing them down. (PCMag offers a list of "The Best Password Managers of 2016" at

http://www.pcmag.com/article2/0,2817,2407168,00.asp.) Change your passwords as often as needed to stay safe.

- Log out of accounts whenever you are finished and, if you share a computer or device with others, don't let your browser save login information.
- If asked to set up security questions (used in case you forget your password), choose ones that nobody else is likely to know the answer to.
- If a website offers two-factor authentication (2FA), enable it. It's stronger than a password alone because it requires two pieces of information to access the account (for example, a password and confirmation of an onscreen picture/graphic you've chosen, or a password plus a passcode that is sent to you via text message or email).
- Don't share your passwords and logins.

II. Mobile devices and apps

Are there additional or different risks for mobile device users?

In addition to the greater likelihood of loss or theft because of mobile devices' portability, there's also the issue of being able to track your location and access your contacts list. Apps—downloadable software created and offered by many thousands of different sources—present their own privacy and security risks.

Are there ways to avoid having my location tracked by my mobile device?

Sharing your physical location with strangers could compromise your safety and privacy, so avoid apps that announce your location to others and don't give you the option to disable that function.

Some apps, such as those that provide maps and directions, must track your location in order to function as intended, but they don't make the information public. Even with these apps, you can go into the device's settings and turn "location services" (or similar) off when they aren't needed. You can also "clear history" if you choose.

How do I know which of the data on my mobile device is being accessed, by whom and for what purpose?

Each participant in the mobile service chain—wireless service provider, device (OS) manufacturer, app developer/owner, etc.—has its own independent practices and policies regarding what data it collects, how it is used, how long it is kept and what options, if any, it offers users. To understand what is being collected by each participant and why, you would have to delve into that particular company's disclosures of its privacy and data use policies.

How do I change the privacy settings on my mobile device?

Typically, you go into Settings, and from there, go through the list of device functions and features and make adjustments. For example, depending on your device, you might

be able to turn on encryption, opt out of targeted ads, turn off location tracking, adjust the auto-lock setting (in other words, make your phone lock more quickly so that nobody else can access it without the passcode), limit your lock-screen notifications (for example, displaying the last text message to arrive), etc.

Check who has access to your contacts, email, calendar and photos. Many apps want this data. If you are asked for permission the first time you use the app, you will have the opportunity to choose "Don't Allow" or "OK" (or something similar). Otherwise, you can go into your Contacts, Photos, etc. (most likely found under Settings > Privacy) and choose which third parties are allowed to access the data.

ZDNet offers specific tips for iOS (http://www.zdnet.com/pictures/ios-9-iphone-ipad-privacy-security-settings/) and Android (http://www.zdnet.com/pictures/android-phone-tablet-privacy-security-settings/) users. 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.

How do I change the privacy settings in my apps?

Social media apps have their own privacy settings, so in addition to adjusting the privacy settings for your device, you should adjust the privacy settings in each individual app, if necessary. These settings will allow you to do things like restrict who can view your profile or what you share. If necessary, visit the social network and/or app developer's website to get a tutorial on controlling privacy settings.

Are there any risks associated with downloading and using apps?

Apps are the biggest collectors and users of data. They can track your location, access your contacts list and send information to third parties for marketing and other purposes. Many have default settings that enable them to access your device—even modify your settings—at will. There are no specific privacy laws that protect the information apps collect, and most require users to consent to data collection for the apps to work.

Many of these risks can be reduced by vetting your apps (checking their privacy policy and reviews), adjusting the device's and app's settings where possible to match your preferences regarding data collection and privacy, and installing updates as they become available to ensure you have the safest version of the app on your device.

How can I make sure an app I want to download is trustworthy?

To reduce the chances of exposing yourself to data-stealing malware, don't download anything that isn't offered through a trusted source (the Apple App Store or Google Play, for example, or the site of a trusted business, such as your bank). Vet apps yourself by reading reviews and making sure the developer is legitimate. Negative reviews or the absence of reviews should be a red flag. It also helps to check what other apps the developer has in its stable (visible in app stores and/or the developer's website) to see if its been around for a while and has received good reviews for other products.

Read the app's privacy policy. Review and understand the permissions you are giving the app when you download it. If the app doesn't provide a privacy policy, think twice about downloading it.

Once you have downloaded an app, be diligent about updating it so that you always have the newest version available, since updates often contain security improvements.

Where do I find app reviews?

You can find app reviews in the app stores themselves (Google Play and Apple's App Store), but you should take these with a grain of salt—you never know which reviewers are objective consumers versus friends or foes of the developer. A good source of reviews are expert, third-party tech sites. Check places such as the "App" section of www.PCMag.com and www.Macworld.com, or the "Reviews" section of www.Engadget.com and www.AndroidPolice.com. You can also "google" the name of the app to try to find reviews from trustworthy sources. If there is something seriously wrong with the app, you might see headlines about it come up in your search.

For reviews of children's websites and apps, try www.BeWebSmart.com, which includes tips and resources for parents, such as a webpage on understanding app ratings and how to restrict your kids' access to apps by content rating (http://www.bewebsmart.com/ipod-ipad-iphone/how-to-restrict-apps-by-rating/). Common Sense Media also offers reviews of kids' apps (https://www.commonsensemedia.org/app-reviews).

How do I know what data an app is accessing or collecting?

Generally speaking, apps that collect personal user data must post a privacy policy that explains how the application collects, uses and shares personal data, so start there. When you install an app, you should be asked whether you agree to share whatever information the app requires. You can find out what data an already installed app accesses on your mobile device by going to Settings and then clicking the app name.

I can't find my app's privacy policy—where is it?

It could be that the mobile app you're using doesn't have a privacy policy. If an app doesn't collect personal information, it isn't required by law to have a privacy policy, but the absence of a privacy policy might also be because the developer is not being transparent about its collection and use of personal information. Assuming there is one, look for a link to it in the app store listing or download page. After you download, you should also find a link to it in the app itself. If you still can't find it, contact app support. If you find out there isn't one, or you are uncomfortable with what it says, uninstall the app and let the developer/owner know about your concerns.

While the existence of a privacy policy does not make an app trustworthy—after all, the policy could say that the company collects all your most personal information and sells it to the highest bidder—it does indicate at least some level of transparency.

How can I control what data an app collects and/or how it uses it?

Apps typically require access to some or all of your mobile device data, whether they need it to function or not. Some apps ask for your consent to access particularly sensitive information, such as your location or contacts. If an app asks your permission to access certain types of data the first time you use it, you can say "no," but in many cases, it is a "take it or lose it" proposition. If you've already granted permission and want to rescind it, you can go into the "Privacy" section of the device's "Settings" and turn sharing off for different apps. (This doesn't mean the company will delete any data it has already collected from you.)

Don't ignore notifications of changes to the app's terms of use or privacy policy. Depending on the app and the significance of the changes, you may receive a direct notification (typically by email or from within the app, known as a "push notification"). In other cases, the only way you'll find out about a change might be to revisit these sections in the app or at its website. Uninstall the app if it plans to start collecting or sharing more of your data than you want and there is no way for you to "opt out." If the app is very important to you, see if you can find a comparable app that is more respectful of your privacy.

Learn more in the Federal Trade Commission's (FTC) "Understanding Mobile Apps" (https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps).

What should I do if I believe an app is deceptive?

If you find blatant deceptiveness in an app, you can uninstall the app and submit a complaint to the Federal Trade Commission (FTC) and the app store, if you downloaded the app from one. You can submit a complaint directly to the app developer/owner as well, if you can find the contact information. One way to do that is to open the app and look for the Contact Us or Help/FAQ section, or something similar. The app store where you purchased the app (if that's where you got it) may include the developer's contact information. The FTC warns that "if the developer doesn't provide contact information—like a website or an email address—the app may be less than trustworthy" (https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps).

You can also rate/review the app wherever user reviews are allowed, notifying other consumers of your misgivings about the app.

III. Social media

Are there any risks in using social media?

Any internet-based activity opens you up to certain risks. When it comes to social media, these risks can include invasive marketing efforts, damage to your reputation, identity theft, cybercrime, cyberbullying and even physical crime. But these risks can be managed by practicing caution. In particular, social media users need to understand who has access to their information (profile, posts, tweets, etc.), how that information

could be used (by the social media company, third parties, “friends” and intruders) and how to control what is shared and with whom.

Do social media companies use my information?

Social media networks may use account holder information and online activity to inform their own internal activities and practices—by, say, displaying relevant content based on your interests—and they might also sell it to third parties (for example, advertisers who want to hone their targeted marketing efforts and software developers who create games, quizzes, etc. that interact with the social network). These third parties may not abide by the privacy policies of the social network, and might access more information than you expect—including that of your contacts.

Do I have any control over companies’ access to my information?

Maybe. Check the social network’s privacy policy to see what information is collected, how it is used, and whether or not you have any options for withdrawing your consent (real or implied) to sharing, if you want to. You probably don’t have much control over the social media company’s collection of your data while you are at the site or in the app. But you may be allowed to limit information being cross-shared by, for example, not logging in to another site via your Twitter or Facebook account, not clicking the “share” button on other websites, or turning off whatever tracking mechanisms you are able to on your mobile device.

The social media company might also give you some privacy options not related to who can see what you share—for example, on Facebook, you can choose whether to see targeted ads based on your perceived interests or just random ads.

What is my “e-reputation”?

This is the reputation you have developed based on the things that exist about you online, often on social networks—photos, opinions you’ve shared, activities, “likes,” etc. Managing and protecting your e-reputation can save you from embarrassment and allow you to avoid the potential consequences of not putting your best foot forward. Here are some “best practices” for shielding yourself from social media fallout.

- Be aware that many people who do not know you personally may use social media as a source of information to judge you by. Consider what a decision maker—employer, recruiter, college admissions officer, lender, landlord, customer/client, government agency, insurer, etc.—might think about what you’re sharing.
- Understand that anyone you’ve shared with can re-share, or expose, what you’ve shared. And if you post something to another person’s profile, you have no control over who else sees it.
- If desired, delete posts, remove photos, change audiences, etc. so that things you shared in the past aren’t visible to future viewers. (Of course, you can’t do anything about everyone who has *already* seen what you’ve shared.)
- Ask others to remove photos, videos or posts that reflect poorly on you. If necessary, learn the social network’s policy on removing content upon request.

- Do an online search for your name to see what pops up.
- Secure your accounts so that they can't be hacked and used against you.

Learn more about managing your online reputation in Google's Safety Center (www.google.com/safetycenter/families/manage/) and in the Associated Press's article "AP Explains: How to clean up your online reputation" (http://www.mercurynews.com/2016/04/15/ap-explains-how-to-clean-up-your-online-reputation/).

How do I change my privacy settings in social media?

Each social network has its own audience/sharing options, so the exact steps will be different, but they all give you some control over who sees what (e.g., who can view your profile, who can see what you've shared or who can contact you). Don't just accept the default settings, adjust them to match your comfort level. Be sure to make a selection for location announcements, since it is never a good idea to announce your location publicly.
The University of Texas at Austin has gathered privacy options and instructions for Facebook, Twitter, Instagram, SnapChat, LinkedIn and Pinterest on a single webpage: https://identity.utexas.edu/everyone/how-to-manage-your-social-media-privacy-settings. If what you need isn't here, check the Help, Support or Privacy sections of the social network website and/or app. Or do an online search for the name of the social network plus the words "privacy settings."

A prospective employer asked for my social media login—is that legal?

It may be, depending on where you live. There is no federal law that bans an employer from requiring an employee or job applicant to provide their username and password for their private social media accounts. But almost two dozen states have enacted legislation regarding employer access to employee and/or job applicant social media pages, and more states consider passing such laws each year. Not all states provide the same level of protection.

Find out what your state's laws, if any, are at the WorkplaceFairness.org site (http://www.workplacefairness.org/social-network-computer-privacy-workplace#4). Learn more on the topic in Nolo's article "Can Employers Ask for Passwords to My Social Media Accounts?" (http://www.nolo.com/legal-encyclopedia/can-employers-ask-passwords-my-social-media-accounts.html). If you think your rights may have been violated, consider contacting an employment lawyer in your area. Some lawyer referral sources include the Legal Aid Society (https://las-elc.org/), WorkplaceFairness.org (http://www.workplacefairness.org/find-attorney) and your state or local bar association (http://bit.ly/2abJBCC).

How do I make sure my child is safe on social media?

The first step is to educate yourself on the types of apps and sites that are popular with kids today, and the code language teens use when sending texts they don't want their parents to understand (often used for "sexting"—sending sexually explicit text

messages). An article at Parent.com (http://www.upstateparent.com/story/life/2015/10/30/socialmedia-positives-negatives-kids-experts-say/74885906/) lists 12 popular apps along with a description of what they do, and provides a list of commonly used codes (for example, LMIRL stands for "Let's meet in real life" and 9 indicates "Parent watching").

In the same article, an expert recommends parents install apps such as WebWatcher (http://www.webwatcher.com/) and Net Nanny (https://www.netnanny.com/) on their child's phone or tablet to monitor their online activity.

Check and adjust the privacy settings on your child's mobile device and in apps just as you do for your own accounts and devices. Disable location tracking in apps to prevent predators from knowing where your child is.

In addition to having a frank discussion with your child about the risks of the internet, acceptable and unacceptable online activity, and how their future could be affected by what they do online today, you should assure your child that they will not lose access to the internet as punishment for being honest with you. You don't want to discourage them from confiding in you.

Learn more about protecting your kids and helping them make smart choices at www.CommonSenseMedia.org.

What is cyberbullying?

According to the American Academy of Pediatrics, cyberbullying is the deliberate use of digital media to communicate false, embarrassing or hostile information about another person. It is considered by some to be the most common online risk for teens today. Teach your child to never bully anyone, and to immediately report being bullied or witnessing the bullying of others.

Learn more about why cyberbullying is different from traditional bullying, who is at risk, what you can do to prevent it and where to report it (at www.StopBullying.gov).

What if I don't like what someone else shared about me—can I make them remove it?

If you find something that you would like removed, contact the poster to make a request. Unless they are violating the law, you might not have much leverage, but it doesn't hurt to ask. Social networks typically have a process through which you can make such requests. (For example, Facebook allows you to report a privacy rights violation due to someone's post of an image: https://www.facebook.com/help/contact/144059062408922?ref=u2u.) However, your request must meet the social network's criteria for removing content. Check the company's policies and procedures. You can also "flag" the content, which might get attention but doesn't guarantee removal.

While you can't control what someone else shares about you in their own accounts, there may be tools for preventing them from showing up in your account. For example, Facebook offers an option to review posts you are "tagged" (named) in before they post to your own timeline for others to see.

IV. Video and TV

Are there any privacy risks associated with video streaming?

Since video streaming is done via browsers and apps, it is likely that internet service providers (ISPs), online advertisers and apps are tracking our viewing histories. In fact, cross-device tracking is commonly used by advertisers to link information about your online behavior across multiple internet-connected devices, such as smartphones, tablets and smart TVs. This tracking typically results in targeted ads. If you don't want to reveal your viewing history via social media, you might have to take special care to avoid inadvertently sharing it.

Of course, any account has the potential to be breached, and that includes accounts with video streaming services and sites. A breach could result in the theft or misuse of your account and viewing history. Even worse, some very bad players use online videos as an opportunity to infect viewers' computers and devices with malware.

All these potential risks raise questions about the rights of internet users to control what is done with their personal information. Unfortunately, at this time the answers are not so simple and viewer rights are not particularly robust.

How do I avoid my viewing history being shared on social media?

First, don't click "Share," "Like" or similar buttons that would result in your viewing history being shared on social media. If you do want to share this information, be sure you have the desired audience selected. Under the Video Privacy Protection Act (VPPA), streaming video providers are required to obtain customers' consent in order to share information about their viewing preferences on social networks, so you can take the opportunity to deny consent. However, the video privacy legislation was weakened in January 2016 when the Senate tweaked the rules to allow blanket permission online (not to exceed two years or until consent is withdrawn by the consumer, whichever comes first) instead of requiring it on a case-by-case basis.

If you choose to share video in a social network, adjust your settings so that it is shared only with your intended audience. For example, when you upload a video on YouTube, it is set as "Public" by default, which means anybody can view it. But you can change that to "Unlisted" or "Private" during upload or after. A "private" video can only be seen by you and the users you select. It won't appear on your channel or in search results and will be invisible to other users. An "unlisted" video means that anyone who has the link to the video (because you shared it with them) can view and post comments to it. 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. Each social

network will have its own way for users to select their audience. Read the company's policies to understand any exceptions.

What recourse do I have if someone shares a video of me I don't like and won't remove it?

Each social network has its own procedure for reporting, or "flagging," content and its own criteria for removing content. For example, YouTube allows you to "Report" a video by clicking on the flag icon (under the word "More" below the video when viewing in a browser). You will be asked to explain why you think the video should be removed (for example, it violates your privacy or is offensive), and YouTube staff will review your request. Generally speaking, the video will be removed if it violates YouTube's "Community Guidelines" (https://www.youtube.com/yt/policyandsafety/communityguidelines.html)—otherwise it will stay. If the video is particularly damaging, yet the social network won't remove it, legal action could be an option.

It's illegal for video of you in a public place to be used for commercial purposes without your signed release. And it's generally illegal to photograph or record you without your permission in private settings—places where you have a "reasonable expectation of privacy," such as your home or a public restroom.

Does my ISP have to keep my account and activity information private?

In early 2016, the FCC proposed new rules for broadband internet service providers that would apply the privacy requirements of the Communications Act to ISPs. The new rules would require ISPs to allow customers to opt out of the use of their information for marketing purposes and to obtain consent (opt-in approval) from customers before using their information (or sharing it with non-affiliate third parties) for any purpose not directly related to the provision of service or the marketing of other communications-related services.

Unless and until these or other rules are implemented, your ISP may have leeway to use your information as it chooses. This includes information about you personally (billing, etc.), as well as when you are online, the websites you visit (and what they can glean from your activity), the apps you use and even your physical location if you are using a mobile device. However, depending on where you live, you may have some protections under state law. For example, Nevada and Minnesota prohibit ISPs from disclosing personally identifying information (PII), and Minnesota also requires ISPs to get permission before disclosing the subscriber's online activity. Check with your state's Public Utility Commission for information about the rules in your state (https://transition.fcc.gov/wcb/iatd/state_puc.html).

What privacy rules does my cable/satellite television service provider have to follow?

Under the federal Cable TV Privacy Act, cable TV operators are required to protect subscribers' personally identifiable information, and must provide an annual written

notice of:

- What personally identifiable information is collected and how it's used;
- How long the information is maintained;
- Where and when the subscriber may access the information; and
- Any legal limits on the company's collection and disclosure of customer information, and what your rights are.

Under federal law, cable and satellite service providers are also prohibited from using the cable system to collect or disclose personal information for advertising purposes without a subscriber's written or electronic consent and must take action to prevent unauthorized access to PII in subscriber accounts. File a complaint with the FCC (https://consumercomplaints.fcc.gov or 888-CALL-FCC) if you believe a television or internet company has violated your privacy rights.

In a few states, including California, protections may also apply to the apps that cable companies provide to watch content on websites or mobile devices.

V. Big Data and marketing

What is Big Data?

"Big Data" refers to the large volume of consumer data that is collected, aggregated and summarized for purposes such as statistical analysis. It is the result of all our digital and online activities, including where we visit on the internet, how we use our mobile devices, what we watch on TV, what we do and share on social media, etc. It is used by companies for all sorts of things, including developing products and services (in other words, predicting what consumers will want), targeting ads and preventing fraud.

How can websites and online marketers get my information?

The easiest way for anyone to get your personally identifiable information is for you to hand it over to them, which is what you often do when you establish an account, fill out a form, join a social network or enter an online contest.

Companies also can get general information—data that, on its own, couldn't be tied directly and specifically to you—about your online activity without your even knowing it by using tracking technology. In a nutshell, when you visit a website, the site can transfer files—"trackers"—to your computer or device that monitors what you do, not only at that particular site, but wherever you go on the internet. Taken together, this activity record can be used to develop a profile on you that is very valuable to advertisers and other businesses. This information can, in some cases, be combined with information from other databases to assemble an even more specific profile that could include things like your gender, ZIP code, homeownership/renter status, parenthood, interests and even medical issues.

You could be identified even more specifically through the IP (internet protocol) address assigned to your connection by your internet service provider. This is like your internet "return address," and it is tied to the name, physical address and other information in the account records. If you have multiple users and/or computers/devices, it can't pinpoint who did what on what machine—just that the activity came from your account. This information, however, is not available to third parties, and typically is disclosed by the ISP only if it is required to do so under the law (in response to a subpoena, for example). Learn more about IP addresses at www.WhatIsMyIPAddress.com.

Learn more about online privacy in the Privacy Rights Clearinghouse's fact sheets "Online Privacy: Using the Internet Safely" (https://www.privacyrights.org/online-privacy-using-internet-safely) and "Securing Your Computer to Maintain Your Privacy" (https://www.privacyrights.org/consumer-guides/securing-your-computer-maintain-your-privacy). Learn about tracking and privacy technology at the Federal Trade Commission's "Online Tracking" page (https://www.consumer.ftc.gov/articles/0042-online-tracking).

What are "cookies"?

Cookies are a type of tracker. They are small files installed on your computer by many of the websites you visit. The information they gather often is used to target marketing efforts, but it also is used for things like remembering items in your shopping cart and recognizing you as a repeat visitor. You can set your browser to delete cookies automatically whenever you exit, or to not accept cookies at all, but that can inhibit the functionality of the site. Instead, consider enabling or disabling cookies on a site-by-site basis, and only for third-party cookies (those placed by someone other than the website you visit). Check the Help section of your browser for instructions.

Some websites use a newer technology called local shared objects (LSO), or "Flash cookies." These are pieces of data saved on your computer by websites that use Adobe Flash software, and they are difficult or impossible to permanently delete. Web beacons are another technology—small, invisible images embedded in web pages—that track your website visits. "Fingerprinting"—a technology that takes a "picture" of your computer when you visit a website—is another tracking option that many companies use. Learn more about fingerprinting in this Forbes article: http://www.forbes.com/sites/josephsteinberg/2014/07/23/you-are-being-tracked-online-by-a-sneaky-new-technology-heres-what-you-need-to-know/#6f63fe6140b2. Learn about the range of tracking technologies and what you can do to control tracking at the FTC website (https://www.consumer.ftc.gov/articles/0042-online-tracking).

Why should I be concerned about online tracking and data gathering?

Some types of tracking can be relatively harmless, and even helpful—for example, allowing you to return to a website and find items you selected still in your shopping cart.

Excessive tracking—collecting a lot of data, or data that is not needed to enhance the functionality or user experience of a website doing the tracking—can lead to marketing messages that are, at best, a nuisance or, at worst, exploitative (for example, inducing

children and young adults to desire things that are not in their best interests). It can also be very creepy and potentially embarrassing to see evidence that you are being watched—for example, an ad for an ointment that is used for a skin condition that you researched online.

One of the bigger dangers in tracking and Big Data is that the information that has been gathered about you could be used to engage in unfair business practices—for example, increasing the price of an item (an airline ticket, for example) after you've demonstrated serious interest by visiting the site multiple times. It could also enable businesses to discriminate by, say, not making loan or insurance offers, or making less attractive offers, to some consumers based on assumptions about their marital status, race, location, etc. Many consumer advocates are also reasonably concerned that the de-identified, or anonymized, data could be re-identified using "hidden" personally identifiable information.

How do I know how a website will use my information and/or site activity?

Read the site's "Privacy policy" to learn what data the company collects, how it could use your information and whether or not it will sell or trade any of it. You can typically find the privacy policy through a link on the homepage, under "About Us" or via the website search box. If the site doesn't have a privacy policy, steer clear of it. While there isn't a standalone federal law that requires a privacy policy, there are several federal and state laws that, when taken together, essentially require a privacy policy for the vast majority of websites. Plus, even if a privacy policy isn't legally required, a website owner that values its visitors will be transparent about its data collection and use practices.

If you are uncomfortable with the types of information the company could collect or how it might use or share it, try to find a different website to use. Or find out if the website you want to use offers the option to "opt out" of collection and/or use of some types of consumer information. On any website, limit how much you reveal about yourself until you are sure you want to establish a relationship with the company. This is particularly true of personally identifiable information, which, if lost or compromised (breached), could be used in illegal or exploitative ways.

What is Do Not Track (DNT)?

Do Not Track (DNT) is a browser setting that tells websites you do not want your online activity to be tracked. If you want to activate DNT, change the setting (typically turned off by default) in the browser's Preferences. You can also go to the browser's support page or use the Help function in the menu bar to get instructions for Do Not Track or other privacy settings, such as "private browsing" or "incognito browsing." But be aware that even if you enable Do Not Track, many sites and companies ignore DNT signals (compliance is voluntary), so there are no guarantees that you won't be tracked despite your efforts. However, if a company/site *has* made the commitment to honor DNT, it is legally required to do so.

Lifehacker's "The Best Browser Extensions that Protect Your Privacy" makes specific recommendations for "plug-ins" that improve the privacy functions of your browser in

some way (http://lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034). TechWorld offers a list of "The best 8 secure browsers 2016" (http://www.techworld.com/security/best-8-secure-browsers-2016-3246550/).

What is a virtual private network (VPN)?

A "virtual private network" serves as a middleman between your computer and the internet. With a VPN, your online activity is no longer associated with your personal IP address. Instead, it is encrypted and associated with the VPN server's IP address. Whether or not you should use a VPN depends on a number of considerations, including how often you use public Wi-Fi. How-To Geek explains "How to Choose the Best VPN Service for Your Needs" (http://www.howtogeek.com/221929/how-to-choose-the-best-vpn-service-for-your-needs/) and PCMag offers a list of the "Best VPN Services of 2016" (http://www.pcmag.com/article2/0,2817,2403388,00.asp).

Can I activate Do Not Track in an app?

While browser users can employ do-not-track tools and adjust built-in browser privacy settings, apps stand alone and work outside browsers. There are ongoing efforts on both the state and federal levels to hold app developers and others more accountable for how they collect, use and share consumer data. Until the law requires stronger safeguards from companies, it's up to you to protect your personal information.

How do I avoid annoying ads on my computer or mobile device?

"Ad blockers" help stop intrusive ads. Look for ad-blocking software in your app store. Similar software exists for computer browsers, thought Facebook has already implemented technology on its computer (not mobile) website that essentially renders all ad blockers useless, and other companies have reportedly been considering doing the same. (Facebook does have an "ad preferences" tool that allows users to opt out of seeing certain types of ads on the site.)

Learn about what ad blockers are available to you in Tom's Guide's "Best Ad Blockers and Privacy Extensions" (http://www.tomsguide.com/us/pictures-story/565-best-adblockers-privacy-extensions.html).

What is COPPA?

The Children's Online Privacy Protection Act (COPPA) gives parents control over what personal information websites can collect from their children under age 13. In 2013, the law was updated to include a child's online activity, geolocation information and photos, videos and audio files that contain a child's image or voice as data that can't be collected without a parent's approval. Because of this law, many social networks don't permit users under 13. If you think a website is violating COPPA, file a complaint with the Federal Trade Commission at https://www.ftccomplaintassistant.gov/ or 877-382-4357.

How do I understand a privacy policy?

Despite the fact that the FTC suggests in its guidelines that privacy policies be written in easy-to-understand English, it might not be obvious to users what to look for. To help consumers understand a company's disclosures about how it will use the data it collects, and what they should reasonably expect, the California Department of Justice's Privacy Enforcement and Protection Unit offers an online guide, "How to Read a Privacy Policy" (http://www.oag.ca.gov/privacy/facts/online-privacy/privacy-policy). Though it is from a California agency, the information is useful regardless of where you live.

Where can I learn about my state's internet privacy laws?

One place to look is the National Conference of State Legislatures website (http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx). You can also contact your state attorney general's office directly (www.naag.org).

Consumer Action
www.consumer-action.org

Through multilingual consumer education materials, community outreach and issue-focused advocacy, Consumer Action empowers underrepresented consumers nationwide to assert their rights in the marketplace and financially prosper.

Consumer advice and assistance:
Submit consumer complaints to our advice and referral hotline:
www.consumer-action.org/hotline/complaint_form/ or 415-777-9635.

Chinese, English and Spanish spoken

This publication was funded by the Rose Foundation for Communities and the Environment.