A Consumer Action Publication

Watch out!

Online video and your privacy

How we view video has changed. No longer limited to watching professionally produced shows on TV at home, now you can watch what you want, when you want—"on demand." Thanks to mobile devices, you can also watch where you want. And you can even watch videos that others share, or create your own.

While consumers now have more choices and greater viewing freedom, they also face new risks around personal privacy. Being aware of the privacy issues raised by video streaming and video sharing technology, as well as what you can do to protect yourself, will enable you to manage the risks while still enjoying the show.

Streaming

"Streaming"—watching or listening to content in "real time," as it's sent to you via the Internet—has become an option for many more consumers, thanks to high-speed Internet, mobile and streaming devices, and streaming services and software.

Many consumers are "cutting the cord" to their pay-TV service and replacing cable or satellite service with one or more less expensive streaming services.

This means that if you use more than one streaming video service—Netflix ***and*** Hulu ***and*** Amazon Prime, for example—you are sharing your viewing history and, in many cases, your billing information with more entities than just a single pay-TV service provider.

And there are almost always at least a couple of middlemen between you and your streamed video—your Internet service provider (ISP), the streaming service app or a web browser, and maybe even a TV or device manufacturer.

All this increases the potential for your video choices, viewing history and some personal information to be collected and used by others, often to target advertising or to be sold to online ad firms and data brokers. (Data brokers are businesses that collect and sell information about consumers, typically for marketing purposes.)

The Video Privacy Protection Act (VPPA) of 1988 prohibits video services from sharing a customer's personal information with third parties without the viewer's consent.

However, under a 2012 amendment to the Act, video streaming companies must ask for your permission ***only once*** before sharing information about the videos you rent or buy. (Much of this sharing happens on social media, by choosing to "Like" or "Share" on Facebook.) If you don't opt out when you are first asked, your consent will be in effect for two years, though you do have the right to withdraw it at any time.

States are allowed to enact broader consumer protections than the VPPA provides, and many (including California, Delaware, Iowa, Louisiana, Michigan, New York and Rhode Island) have done so. To find

out if your state has its own laws on video privacy, visit the Electronic Privacy Information Center (EPIC) online (*http://bit.ly/21xf3U2*). Or contact your state attorney general's office; find contact information at the National Association of Attorneys General website (*www.naag.org*).

Broadband Internet customers receive some protections against the misuse or breach of their personal information under the federal Communications Act, which was originally created to protect telephone service customers. Under the 2015 Open Internet Order, broadband Internet service providers only are allowed to use, disclose or permit access to individually identifiable customer information in order to provide services. However, there is still some question about what is considered private customer information. Cable companies, too, are required to protect their subscribers' personally identifiable information, whether they are providing cable, broadband or telephone service.

Because these laws still leave room for privacy concerns for video streamers, you should be proactive about protecting your information. Here are some steps you can take:

- Read the privacy policy for any streaming service or app you consider using, and learn about the privacy settings and "opt out" options it offers. If you're not happy with how the company could use your personal information, look for a different service that may offer greater privacy rights. (The California Department of Justice's "How to Read a Privacy Policy" (*http://bit.ly/1LvfaYN*) offers valuable guidance regardless of which state you live in.)
- When streaming via web browser, experiment with do-not-track tools such as Do Not Track Plus and Ghostery browser plug-ins, and adjust built-in browser privacy settings for greater privacy. You may find that some plug-ins interfere with viewing in the browser. If so, go to your browser preferences, uninstall the plug-in and try it with a different browser. (Generally, apps—software for mobile devices—can track you and send information to third parties for marketing and other purposes, and don't offer do-not-track tools.)
- Test your preferred video streaming services using "Private Browsing," an option in your web browser. Like other do-not-track tools, this could prevent your video streaming service from working, and it probably won't stop the video service from receiving information about you if you are logged in. But if it does work, it may keep your activities from being seen by hackers, and they won't be added to your browser history or cloud storage for others who share a device or account with you to see.
- Check the website or app to see if the option to delete your viewing and/or search history exists. YouTube and Netflix are just two of the video content services that offer this. You may also be able to delete your streaming history from your game console or streaming media player. However, this only prevents your history from being viewed by others who might share a computer, device, TV or streaming account with you. It doesn't typically remove your history from the service provider's records.
- If you do not want your social media audience to know what videos you watch, do not click "Like" or any other social media "Share" buttons that appear on streaming sites such as Netflix.com. (Share movies you want to recommend with specific friends via email or private messaging.)
- If you want to be afforded the protections of the VPPA, you will have to register for an account, pay to watch a video, download an app or take some other step to be considered a "customer" or "consumer" of the service provider. While some uncertainty remains, a court found in 2015 that companies that shared viewing history of "non-subscribers" with third parties did not violate the VPPA.
- If you didn't opt out of disclosure of your viewing history when given the opportunity, and you aren't given additional opportunities to opt out when you choose videos, you can withdraw your consent at any time by following the instructions on the company's website. (The law requires service

providers to notify consumers "in a clear and conspicuous manner" of the ability to opt out of consent to further sharing.)

To file a complaint against your Internet service provider, visit the FCC Internet complaint webpage (*http://bit.ly/1KZvzVz*) or call 888-CALL-FCC (888-225-5322)/TTY: 888-TELL-FCC (888-835-5322).

To file a complaint against a company that offers services, content, products and apps over broadband Internet, visit the Federal Trade Commission (FTC) complaint webpage (*www.ftccomplaintassistant.gov*) or call 877-FTC-HELP (877-382-4357).

Smart TVs

Any device that connects to the Internet is vulnerable to data breaches by hackers. This includes "smart" TVs—Internet-enabled television sets. In tests, security researchers were able to hack into a smart TV and turn on its built-in camera and microphones, and there is the potential to steal logins and passwords or install malware (malicious software).

There is also the potential for smart-TV manufacturers to gather and share your viewing history. Smart TVs employ something called "automatic content recognition (ACR)" to identify what you're watching and then send that information in real time to third-party vendors, typically for marketing or analytics purposes.

While the risks sound serious, they are similar to the risks you face anytime you're on the Internet, and some of the steps you should take to protect your privacy are the same. (Get more online safety tips in "Put a Lock on It: Protecting your online privacy" (*http://bit.ly/put-a-lock-on-it*).)

- Install all updates to the TV operating software. Often, updates address newly discovered security issues.
- Download apps only from trusted sources.
- Don't enter sensitive personal or financial information using the TV's web browser or apps.
- If possible, create a "guest" account on your Wi-Fi network and connect your TV to that. That way, if hackers get in, they can't reach your computer or other devices on the network. (Look for instructions for your Wi-Fi router online, or contact the manufacturer or your ISP for help.)
- When you first set up your smart TV, you will most likely be given the chance to opt out of content tracking. If you aren't, or if you miss it, you can turn tracking off later. (*Consumer Reports* offers instructions (*http://bit.ly/1QHcK5v*). You can also check the TV's settings, or contact the manufacturer for help.)

Smart TVs are programmed to recognize certain spoken words, like "TV on." Depending on the TV brand/model, you should be alerted to "listening" mode by a microphone that appears on the screen, a beep or some other signal.

The voice data typically is transferred to a third-party server for processing so that your request can be fulfilled. It's not likely that this would be a threat to your personal privacy—at least not any more than the iPhone's Siri and similar voice-command electronics. But if you want to turn this function off, you can. The process will be different for different TV models, but generally it will require you to change the settings via the Menu button on your remote control.

Pay-TV accounts

Cable or satellite television ("pay-TV") account holders must be notified when they sign up for service, and at least once per year after that, what types of personal information the provider will collect, how it will be used and how long it will be kept.

Pay-TV companies can't collect your personally identifiable information—information that could potentially identify a specific individual—without your written or electronic consent except as needed to provide services or detect the unauthorized use (theft) of cable service. And they can't disclose your personally identifiable information without your written or electronic consent (or, in some cases, without giving you an opportunity to prohibit or limit disclosure) except as needed to provide services or in response to a court order.

If the cable service provider violates your privacy rights, you can sue the company and be awarded actual damages up to $1,000, punitive damages and attorney fees.

Livestreaming and video sharing

Livestreaming video apps such as Meerkat and Periscope enable users to share real-time video taken with their mobile device. This raises new questions about the privacy of bystanders.

Privacy laws typically don't protect people when they are out in public. So, generally speaking, it is legal for someone to take and share video of you when you are in a public place, such as on the street, in a park or at a rally. However, it's not legal to use that video for commercial purposes unless you have signed a release.

In a private setting—anyplace where you would have the reasonable expectation of privacy, such as in your home or a hotel room—photographing, videotaping or recording you without your permission is generally illegal.

YouTube, home to millions of shared videos, allows individuals to request removal of any video posted without their consent that contains their image or voice, full name, financial information, contact information or other personally identifiable information (*http://bit.ly/1XW4bcM*). Other services may offer something similar; check the service's website for information.

Here are some tips for protecting your privacy in livestreamed or shared video:

- If you don't want to risk being included in a video, consider avoiding places or events where videotaping is likely to occur.
- If you are given the option to sign in to video sharing services using your Facebook or Google account login but you don't want your viewing history to be tied to those accounts, create a separate login account. (If you have used Facebook or Google+ to sign in to third-party apps or services, both allow you to review and disconnect from third-party logins.)
- Ask anyone sharing your image to remove it if you don't want it used publicly. (If it was taken in a public place and is not being used for a commercial purpose, they may not agree to remove it, but you can still ask.) If your image is being used for commercial or promotional purposes—even if it was taken in a public place—you have the right to sue if you haven't given your consent.
- If you are sharing video you have created, adjust the privacy settings of the video sharing website or app to match your preferences. Look for privacy tools under the "Settings" or "Privacy" tab. Your choices might include allowing anyone to see your video, allowing nobody to see it, allowing only friends or followers to see it, allowing only those with a password to see it, and more. You might also be able to control who can embed (share, or post) your video and where. Privacy options will vary among service providers.

About 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 and financially prosper.

Consumer advice and assistance: Submit consumer complaints to: *www.consumer-action.org/hotline/complaint_form/* or 415-777-9635. Chinese, English and Spanish spoken

About this guide

Consumer Action created this guide with a grant from the Rose Foundation.