Social media and online video privacy

Seminar lesson plan and class activities

A Consumer Action Publication

www.consumer-action.org

Social media and online video privacy
Seminar lesson plan and class activities

Lesson purpose:

To make internet users aware of the privacy risks related to social media and online video, prepare them to make wise choices that will help protect their privacy and personal data, and direct them to resources where they can find tools and more information.

Learning objectives:

By the end of the lesson, participants will understand:

- What privacy risks to be aware of when using social media and online video
- The potential negative consequences of a loss of privacy
- What practices they could implement to reduce the risks to their privacy
- What tech tools can help control collection and/or sharing of their data
- How to keep their children safe online
- Their privacy rights, if any, under the law
- Where to file a complaint if they feel their privacy rights have been violated
- Where to find more information

Lesson duration:

2 hours

Materials:

For instructor:

- *What's not to 'Like'? Protecting your privacy on social media* (brochure)
- *Watch out! Online video and your privacy* (brochure)
- Visual teaching aid (PowerPoint presentation with instructor's notes)
- Lesson plan, including activities, answer keys and resources (pages 3-22)
- Class evaluation form (page 22)

Instructor will also need:

- A computer and projector for the PowerPoint presentation (the PowerPoint slides also can be printed on transparency sheets for use with an overhead projector); and
- An easel and pad, or a whiteboard, and markers.

For participants:

- *What's not to 'Like'? Protecting your privacy on social media* (brochure)
- *Watch out! Online video and your privacy* (brochure)
- Goodbye, TMI (exercise) (1 page)
- Privacy, please! (exercise) (1 page)
- Class evaluation form (1 page)

Optional:

- Printout of the PowerPoint presentation

Lesson outline:

- Welcome and training overview (5 minutes)
- The risks of oversharing (10 min)
- Exercising control on social media (20 min)
- Exercise: Goodbye, TMI (10 min)
- “Big Data” and individual privacy (20 min)
- Privacy implications and controls for online video (20 min)
- Exercise: Privacy, please! (10 min)
- Resources (10 min)
- Questions and answers (10 min)
- Wrap-up and evaluation (5 min)

Funding for this project was provided by the Rose Foundation.

Instructor's notes:

This training module consists of two fact sheets/brochures (*What's not to 'Like'? Protecting your privacy on social media*, and *Watch out! Online video and your privacy*); a backgrounder written in Q&A format to help trainers answer frequently asked questions; a lesson plan with class activities; and a PowerPoint presentation. It was created by the national non-profit organization Consumer Action to be used by non-profit organizations providing consumer education in their communities. The entire module can be found online at http://www.consumer-action.org/modules/module_social_media_streaming.

Before conducting the training, familiarize yourself with the fact sheets, the backgrounder, the lesson plan (including activities) and the PowerPoint visual teaching aid.

The PowerPoint presentation contains notes for each slide (appearing below the slide when in Normal view or Notes Page view). These notes offer detailed information about the items appearing on the slide. The learning objectives for each section, along with key points and questions to generate discussion, are included in the lesson plan, as are indicators telling you when to move to the next PowerPoint slide.

Why Adults Learn, a PowerPoint training for educators, provides tips for teaching adults and diverse audiences—it will be helpful to you even if you have taught similar courses before. The slide deck is available at http://www.consumer-action.org/outreach/articles/why_adults_learn/.

WELCOME AND TRAINING OVERVIEW (5 minutes)

➡**SLIDE #1** (onscreen as participants arrive; direct early arrivals to begin reading the fact sheets)

Welcome participants and introduce yourself.

If you have a small group, you can ask individuals to introduce themselves (or, if time permits, ask them to pair off with someone seated near them and then introduce each other to the group) and tell you what they hope to get out of the training. In a larger group, invite a few volunteers to share their expectations. On your whiteboard or easel pad, jot down some of the specific things participants mention. You can come back to this at the end of the class to make sure you've covered these points. (This activity is designed to serve as a brief icebreaker. It will also give you an idea what participants' expectations and needs are.)

Review the contents of participants' packets. Ask the class to take a look inside their packets and make sure they have all the materials needed.

➡**SLIDE #2**

Present the learning objectives of the training (also listed on the first page of this lesson plan).

THE RISKS OF OVERSHARING (10 minutes)

Learning objective: Be aware of the types of information you might not want to make public and the risks of sharing too much on social media.

Key points (slides 3-4):

- Not everyone on the internet has your best interests at heart.
- There are many types of information that, if shared, could be used against you.
- You can't control how others use or share your information—something to be aware of anytime you share something.
- Before sharing anything, you should consider the potential consequences if it were to become public.

Questions to generate discussion:

- Why do you think social media is so popular? What does its popularity say about our desire to interact and share?
- What kinds of things would you never share on social media? Why not?
- Have you ever witnessed a negative outcome as a result of social media sharing? What was shared, and what happened?

Note: When generating discussion, allow a moment or two for participants to respond. You can jot down responses on your easel pad or whiteboard.

➡SLIDE #3

Introduction: Using the internet in general, and specifically social media, is a favorite pastime for people of all ages. Sharing online is so commonplace that many users seem to forget that they are not engaged in an intimate conversation with their family members and close friends. Their trusting nature and, in some cases, a lack of understanding about what constitutes oversharing and how personal information could be used against them can lead to serious consequences.

Go over slide notes.

Slide notes: Though the internet and social media offer countless opportunities for positive interaction, not everyone online is your friend. Here are some ways that you or your family could be harmed by others in cyberspace:

- **Spam and aggressive advertising:** Spam is unwelcome email and instant messages, which may offer goods of no or little value or a promise of financial rewards if you give the sender money. This is mainly a nuisance, though it could be costly for those who respond. Aggressive marketing efforts, including pop-up ads, are another online nuisance.
- **Scams:** These include any attempt to cheat you out of your money or personal data. A common tactic is "phishing"—sending emails that attempt to "hook" you by appearing to be from a legitimate business. Often these emails link to a "spoofed," or copycat, website that captures any personal data that you enter, installs malware (malicious software) onto your computer or device or steals your money.

- **Identity theft:** ID theft is the use of your personal data for financial gain (accessing your accounts or opening new credit accounts in your name, for example) or to commit some other crime.
- **Stalking and cyberbullying:** Online stalking is the repeated use of electronic communications to harass or frighten someone, for example by sending threatening e-mails or posting harassing or malicious messages on social media. Cyberbullying is the use of the internet to bully a person, typically by sending or posting messages and/or images intended to intimidate, embarrass or harass.
- **Physical crime:** This could include things like a home robbery or violence against someone.

➡SLIDE #4

Go over slide notes.

Slide notes: Online sharing has become so commonplace that you might not even recognize what constitutes oversharing and what the risks could be. It's important to be aware of both in order to enjoy social media without potentially serious consequences.

•"Oversharing" means revealing information that could be used against you in some way. For example, announcing the dates of your upcoming vacation could enable someone to use it as an opportunity to rob your home; a photo you posted of you at the beach on the day you called in sick to work could get back to your boss; announcing your location could lead a stalker right to you; a photo of you at age 17 with a beer in your hand could cause a college admissions officer to question your judgment; sharing that you went water-skiing yesterday could put your disability insurance claim for a leg injury in jeopardy.

- Your "e-reputation" is the picture that a compilation of all the information that exists about you on the internet paints. It is your "digital" reputation, built through photos, tweets, articles, etc. by you and by others about you. It includes what you've "liked," the groups you've joined, etc., as well as non-social media information such as lists showing what causes and political candidates you've donated to. It's important to be aware of this so that you can avoid doing anything that paints a picture of you that does not match what you want people to see. Oversharing can shape your e-reputation in ways that are not beneficial to you.
- What you share may be shared by others—something that many people forget when choosing what to share. Many social media users believe they are sharing only with those they trust by adjusting their privacy settings to make things non-public. What they might forget is that they don't have control over how what they share might be shared with others. For example, you might have "friended" a coworker on Facebook when you first started your job and got along great. He gave you a "thumbs up" when you posted that disparaging video impression of your boss, but six months later, he's after your job and has decided to leak the video to your employer. One of the best ways to avoid oversharing is to consider how what you share could affect you or others if it were to go public—then choose accordingly.

EXERCISING CONTROL ON SOCIAL MEDIA (20 minutes)

Learning objective: Understand how to limit *what* you share and with *whom* so that you and your family can enjoy social media while avoiding or reducing the potential privacy risks.

Key points (slides 5-8):

- You can—and should—take measures to limit your audience on social media.
- Those you knowingly share with might share your information with others without your knowledge or permission.
- The use of apps requires that you take different and/or additional precautions to protect your privacy.

- A privacy policy is not a guarantee of consumer-friendly data use practices, but the absence of one is red flag.
- Parents can protect their children by discussing acceptable and unacceptable social media communications, setting clear rules, monitoring their online activity and taking advantage of parental controls.

Questions to generate discussion:

- Do you feel like you're in control when you use social media? Why or why not?
- What do you think might be some of the risks of letting people know where you are or where you will be?
- At what age do you think children should be allowed to use social media? Why that particular age?

➡SLIDE #5

Introduction: Considering how many internet users have active social media accounts, online sharing clearly is an important part of many people's lives. Being safe online doesn't mean having to give up the things you enjoy. It does mean making conscious, well-informed choices. Once you understand what you can and can't control on social media, you can take the steps necessary to align your privacy needs with your desire to share.

Go over slide notes.

Slide notes: You wouldn't yell out your vacation plans, relationship status and other personal information in the middle of a crowded street, yet that's essentially what many social media users do. Indiscriminate sharing is risky; it's also avoidable.

•You can limit your audience on social networks—and you should take advantage of the ability to do so. 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. For example, on Facebook, you can select your audience for future posts from a dropdown menu under "Who can see my stuff?" Options include Public, Friends, Only Me, and Custom. You can also make a selection for "Who can contact me?" You can find these types of options for your other social media accounts by looking under "Security and Privacy Settings" (Twitter) or a similar heading/section. Be sure to make a selection for location announcements. For example, to keep your location private on Twitter, do not check the "Add a location to my Tweets" box. You can also delete your previous location information in this same area. 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.

- Privacy settings are effective for future posts, tweets, etc., but don't get a false sense of security from resetting them ***after*** you've already shared. Even though the content will no longer be shared from that point forward, someone you willingly shared with in the past could take your message, photo, etc. and share it with others without your permission or approval. Also, some basic information about you might always be available to the public. For example, Facebook displays your name, profile picture, cover photo, gender, networks, username and user ID publicly, including with apps, regardless of your privacy settings. Instagram will allow you to keep your photos private, but will still allow any user to read your bio and send a photo or video to you directly.

- While you can't control what someone else shares about you in their own account, 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.
- To avoid someone else changing your account settings so that things are shared more broadly than you want, make sure your social media accounts are secure and can't be hacked. Never reveal your social media logins.
- It's not a bad idea to find out what's out there (on the internet) about you in an effort to manage your e-reputation. Do an online search of your name in quotes. If you find something that you would like removed, contact the poster/account owner 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 content removal 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. "Flagging" the content might get attention but it doesn't guarantee removal.

➡SLIDE #6

Go over slide notes.

Slide notes: Apps are software programs that add functionality to mobile devices (smartphones and tablets). Social media companies offer apps that enable users to access the network and their accounts on the go. Apps require that users take special precautions to protect their privacy.

- **Vet your apps.** Download apps only from trusted sources such as the Apple App Store or the Google Play store, which are likely have to done some work at weeding out any bad apples (no pun intended), or get them directly from a trusted source/developer—for example, a banking app from your bank's website. Read reviews; negative reviews or the absence of reviews should be a red flag. You can find reviews in app stores, or you can do a web search for the app's name to see what comes up. Online tech websites such as CNET.com and PCMag.com offer reviews by experts. 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 and/or permissions notice.** Many apps can access most of the info on your device. For example, on Facebook, in addition to public information about you, apps also have access to your friends list. Most apps will tell you upon installation which of your data they will access and ask you whether you agree or disagree. In many cases, this is a take-it-or-leave-it proposition, so you will have to make a decision about whether the app's data access and use policy is acceptable or not. If not, uninstall it and look for a similar app that better meets your privacy needs. 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. You might also look for privacy seals such as TRUSTe, BBBOnLine and ESRB (this one signifies that a child-directed website or app complies with applicable laws and requirements such as COPPA). Apps/companies that display these seals must meet certain minimum privacy standards and must answer to complaints submitted by consumers. Check out Techlicious's "The Worst Apps for Privacy" (http://www.techlicious.com/tip/the-worst-apps-for-privacy/) for some insight into app privacy practices and what to look for. Another site, www.PrivacyGrade.org, has assigned privacy grades to Android apps based on some techniques a team of Carnegie Mellon University researchers has developed to analyze privacy-related behaviors.
- **Adjust privacy settings.** Do this both within the social media account *and* for your device. Avoid location announcements—they can be risky. (Allowing an app to track your location [not announce it] makes sense

only if the functionality of the app requires that information—for example, to send a car to pick you up, to give you directions or to notify you of nearby businesses.)

- **Opt for automatic software updates.** These often patch security flaws. If an app requires a manual update, it might be because it requires your permission to access additional data. Pay attention when you are asked to grant permissions (Agree/Disagree) by an app you've been using. Stay on top of changes to policies/practices so that you can uninstall the app if the level of privacy you're comfortable with is reduced. If warranted (you feel the app is deceptive or is violating users' privacy rights), complain to the app developer and app source (if different), and the FTC (contact information in notes for next slide).

➡SLIDE #7

Introduction: The risks that kids face as a result of using social media can be different and even more serious than those that adults face. This is due in part to their open and trusting nature and their lack of life experience. As a parent, you have to step in to keep them safe. Short of forbidding your children from using social media, the best ways to keep them safe online include alerting them to the risks, setting clear rules, keeping a watchful eye and maintaining open communication with them.

Go over slide notes.

Slide notes: Social media offers the potential for both positive and negative experiences for teens who use it. You can reduce the opportunity for negative online experiences by taking some precautions. (Visit the FTC's "Kids and Socializing Online" webpage for even more tips: https://www.consumer.ftc.gov/articles/0012-kids-and-socializing-online.)

- Don't allow young children to use social media. (Most social media websites and apps require that kids be 13 to sign up. However, this is not necessarily out of concern for the child's safety but because the Children's Online Privacy Protection Act (COPPA) prohibits companies from collecting certain information from kids younger than that. Report COPPA violations to the Federal Trade Commission (FTC).)
- Before allowing your children to use the internet and social media, discuss the risks and set rules. SafeKids.com (which links to SafeTeens.com) provides a 10-point list of online safety rules for kids (www.safekids.com/kids-rules-for-online-safety) that you can share and discuss.
- Instruct your children not to reveal private information online. Caution them against oversharing in general, and provide specific examples of what is unacceptable, like posting pictures of themselves or others without first discussing it with a parent, or sharing their password or account login information, even with their best friend.
- Warn your children about the risks of communicating with strangers. Explain that there are adults with sinister motives who pose as other young people online. (In fact, some predators reach children through online games that allow them to communicate anonymously with other players.) Explain that its never okay to go alone to meet someone from the internet, share photos of themselves, etc. "Friend your kids"—in other words, join their network—and actively monitor their online and social media activity, including who they interact with.
- Discuss cyberbullying, why it's wrong, and that you should be notified if your child witnesses it or is a victim. Save any evidence (for example, the message itself or a screenshot) and report online harassment of a child and predatory behavior to the proper authorities, which may include school officials, local police or the CyberTipline (http://www.missingkids.com/cybertipline/ or 800-843-5678).
- Take advantage of parental controls whenever possible. Options and functionality differ from source to source, but generally parental controls can help you monitor your children's online activities and limit what

they are able to do, read or view online. Many websites, apps and devices/hardware offer built-in controls. There is also stand-alone parental control software/apps. Learn more about parental controls from the Family Online Safety Institute (www.fosi.org/good-digital-parenting/) and in the Google Safety Center (www.google.com/safetycenter/).

- Check children's website and app reviews/ratings before allowing your child to visit/use them. www.BeWebSmart.com is a website for parents who want to keep their families safe online. It includes tips and resources, 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 app reviews (https://www.commonsensemedia.org/app-reviews).
- Tell your kids not to share their social media logins/passwords or to ever impersonate anyone online.

➡SLIDE #8

Introduction: All social media users can benefit from following some simple dos and don'ts.

Go over slide notes.

Slide notes: Obeying the dos and don'ts of social media will help you protect your privacy and stay safe.

Do protect your accounts from outsiders:

- Create strong account passwords and log out when you're finished with your social media session, especially on a shared or public computer. Don't share your logins with anyone. Visit Google Support (https://support.google.com/accounts/answer/32040?hl=en) or ConnectSafely (http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/) to learn about creating strong passwords. You can also use an online tool such as PasswordsGenerator.net (http://www.passwordsgenerator.net/) for help coming up with a strong password.
- Check the company's privacy policy before opening an account or downloading an app.

Do adjust your account and device privacy settings:

- Adjust the privacy settings for your accounts and/or apps as well as your device.
- Keep an eye out for changes in policies and/or settings that might require you to take additional steps—readjusting your settings or deleting your account/app—to achieve the level of privacy you're comfortable with.

Don't overshare:

- Think twice about everything you share. Consider how it could be used by someone else and how others (family members, employer, lender, etc.) might perceive it if they saw it.
- Avoid announcing your location, and don't share your current (real-time) whereabouts or information about where you will be in the future.
- Don't ever share sensitive personal information such as your address, full birthdate, mother's maiden name, Social Security number, etc.
- Talk to your kids about social media sharing and what is and isn't acceptable.
- Comply with your employer's social media policy, if it has one.

Don't let your guard down:

- Ignore communications, requests and invitations from strangers. If necessary, adjust your settings so that you cut ties with anyone you don't want in your network.

- Don't respond to spam, even to "unsubscribe"; don't click on unknown links and downloads; don't feel obligated to fill out every field when creating your profile; and don't respond to quizzes, games, etc.

GOODBYE, TMI (EXERCISE) (10 minutes)

Assign participants to work on the four social media "shares" on page 18 of the lesson plan. Ask for volunteers to share their answers. (Answer key is on page 19.)

"BIG DATA" AND INDIVIDUAL PRIVACY (20 minutes)

Learning objective: Understand what "Big Data" is, how companies collect and use consumer data, what negative consequences there might be and how to exercise some control.

Key points (slide 9):

- There are pros and cons to "Big Data" for consumers.
- Virtually every digital exchange is tracked.
- Consumers have some options for trying to restrict the information gathered about them.
- It is virtually impossible for a consumer using the internet to avoid having data collected about him or her.

Questions to generate discussion:

- Why do you think many things with "Big" in their name—"Big Data" or "Big Pharma," for example—sound menacing? What does "Big" imply relative to consumer rights?
- How do you think Big Data could be used to benefit consumers? How could it be used to disadvantage or harm consumers?

➡SLIDE #9

Introduction: Your audience isn't the only thing you should try to exercise some control over. The companies that play a role in your social media use—from the social media company itself to app developers and other third parties—want your personal data. If you want to reduce their intrusiveness, you need to understand what to look for and what your options are for exercising some control.

Go over slide notes.

Slide notes: "Big Data" refers to the large volume of consumer data that is collected, aggregated and summarized for purposes such as statistical analysis. Virtually every online and social media exchange is tracked. While Big Data helps to detect fraud and customize the user experience, targeted advertising is probably the most visible use of it. Many consumer advocates argue that this data also enables companies to use it against consumers—say, by increasing price based on a person's online activities. They also are reasonably concerned that the de-identified, or anonymized, data could be re-identified using "hidden" personally identifiable information (PII). Big data isn't going away, so the best consumers can do is understand something about data collection and then exercise control wherever possible.

- **Read the company's privacy policy.** "How to Read a Privacy Policy," from the Calif. Depart. of Justice Privacy Enforcement and Protection Unit, helps consumers nationwide understand what to look for (http://oag.ca.gov/privacy/facts/online-privacy/privacy-policy). In 2015, Time Magazine and the Center for

Plain Language analyzed the privacy policies of seven well-known tech companies. Read the results to get an idea of what to expect and what to look for (http://time.com/3986016/google-facebook-twitter-privacy-policies/). Take advantage of opportunities to opt out of (or not opt in to) data collection.

- **Consider activating "Do Not Track" (DNT).** Most browsers allow you to select this setting, which tells websites that you want to opt out of third-party tracking (typically used for advertising purposes). However, honoring users' DNT preference is voluntary, and most companies have not committed to do that. (If a company/site ***has*** made the commitment, it is legally required to do so.)
- **Consider activating "private browsing."** When you surf the internet, your web browser stores data about your browsing history. With private (or "incognito") browsing turned on, your browser won't retain "cookies" (small tracking files installed on your computer or device), your browsing history, your online searches, passwords you've saved or files you've downloaded. This means that anyone else using your computer or device wouldn't see that information. It also means that sites you've visited wouldn't remember you, which is not ideal if, for example, you saved items in a "shopping cart." Be aware that while private browsing provides some added privacy by not saving any information about the sites and webpages you've visited, it doesn't prevent third parties from tracking you ***while*** you're browsing. To learn how to enable private browsing, visit How-To Geek (http://www.howtogeek.com/269265/how-to-enable-private-browsing-on-any-web-browser/). Lifehacker's "The Best Browser Extensions that Protect Your Privacy" makes recommendations for "plug-ins" that improve the privacy functions of your browser (http://lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034). And TechWorld offers a list of "The best 8 secure browsers 2016" (http://www.techworld.com/security/best-8-secure-browsers-2016-3246550/). (The types and level of protection provided by private browsing varies among browsers, so choose the one that best meets your needs.)
- **Consider a 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. 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).
- **Manage your "cookies."** First-party cookies are placed on your computer by the sites you visit to remember things like your preferences or what's in your shopping cart. Third-party cookies are placed by someone else, such as a partner advertising network. These cookies can follow you and place ads even when you visit other, unrelated sites. Various browsers have different ways to let you delete or limit cookies, and some allow privacy plug-ins—separate tools that help you block, delete, or control cookies. (Check the links directly above for more information and options.) If you block cookies entirely, you might lose functionality, so choose to block only third-party cookies. Be aware that cookies might be placed on your computer again the next time you visit the site or view an ad. And new technology, such as "device fingerprinting," which identifies you based on your browser's configurations and settings, can track your activity without using cookies.
- **Block ads.** There are many software programs for blocking ads, though businesses—including social media companies—sometimes find ways around them. Tom's Guide (http://www.tomsguide.com/us/pictures-story/565-best-adblockers-privacy-extensions.html) is one source for information about specific ad-blocking software options. For mobile apps, the FTC's "Online Tracking" page (https://www.consumer.ftc.gov/articles/0042-online-tracking) provides instructions for resetting the identifiers on your device and limiting the use of identifiers or your geolocation for ad targeting (all accessed via Settings). As the Tom's Guide site explains, though, ads are the way many sites are able to provide free content; blocking them could prevent the site from working for you or could ultimately limit the free content available.
- **Avoid online surveys,** polls, games, contests, etc.—often these are just ploys for collecting consumer data.

- **Sites must obtain parental consent** for the collection or use of any personal information from children under 13. Report violations to the Federal Trade Commission (www.ftccomplaintassistant.gov or 877-FTC-HELP).

PRIVACY IMPLICATIONS AND CONTROLS FOR ONLINE VIDEO (20 minutes)

Learning objective: Be aware of the privacy risks inherent in internet-based video and what you can do to try to protect your viewing history and other personal data.

Key points (slides 10-15):

- New ways of watching TV and video present new privacy risks along with the advantages they offer viewers.
- There typically are a few middlemen between you and the video you are watching via the internet, all of whom are likely to have access to some data about you.
- Technology offers viewers some tools for protecting their privacy, but some collection and use of viewer data is virtually unavoidable when connected to the internet.
- Consumers have some limited rights to privacy when it comes to online video.

Questions to generate discussion:

- What are some advantages and disadvantages of modern viewing options like YouTube, Netflix, etc.?
- What are some scenarios in which you would not want your viewing history to be monitored or shared? What about scenarios in which you wouldn't want a video you're in to be shared?

➡SLIDE #10

Introduction: How we watch video has changed dramatically—from a few TV channels that can only be watched at home at the times designated by programmers to almost limitless options delivered anywhere, at any time. That gives us a lot more choices of what to watch, as well as a lot more ways that our viewing history and personal data can be collected and used.

Go over slide notes.

Slide notes: How we watch TV and video content has advanced in ways that few would have predicted. Here's an overview of some of the new ways to watch:

- **Streaming (on demand):** This refers to watching (YouTube, Netflix, etc.) or listening (Pandora radio, etc.) to content as it is sent to you via the internet. Streaming video allows us to watch whatever we want, whenever we want, wherever we want—"on demand." You can stream video on any screen that is connected to the internet, either directly (computer, mobile device, smart TV, etc.) or through external equipment (streaming media players such as a Roku, Blu-ray player, Xbox, etc.).
- **Smart TV:** These televisions have internet connectivity built into them, so no external streaming media player is needed. Different makes and models will have different interfaces (what you see onscreen when you are controlling the TV) and pre-installed apps (streaming services).
- **Video sharing:** This refers to uploading and sharing video clips online (on YouTube, for example). Like other social networks, video sharing networks typically allow users to share their videos with the

audience they select. Going “viral” refers to achieving huge popularity through widespread internet sharing.

- **Livestreaming:** This allows people to broadcast live video content (as it happens). Formerly only an option for newscasters, sporting events and similar professional video sources, the average person can now livestream right from their smartphone.

  These new viewing and sharing options provide a lot of advantages, including convenience, choice and savings, but also raise new privacy concerns.

➡SLIDE #11

Go over slide notes.

Slide notes:

- Often when you stream video content (i.e., watch via the internet), you are required to set up an account, including personal data such as your name, email, credit card number, login, etc. This puts your data out there, to potentially be used or breached—no different from the many other types of accounts you set up online or off. Even if you don’t set up an account, your viewing activity can be monitored by middlemen such as the video source (through online tracking tools), your internet service provider, the device/TV manufacturer, etc., and the collected data could be used or shared in ways you don’t like, such as targeted advertising.

- The law provides some limited protections for viewers. First, the Video Privacy Protection Act (VPPA), which was designed to prohibit “video tape” service providers from disclosing users’ personally identifiable information to third parties, has been updated to require streaming video providers to obtain customers’ consent in order to share information about their viewing preferences on social networks. However, blanket permission obtained online (not to exceed two years or until consent is withdrawn by the consumer, whichever comes first) is allowed instead of requiring it on a case-by-case basis. (This was pushed by Netflix to allow its users to share their viewing history via social networks such as Facebook.) In order to qualify for the protections provided by the VPPA, you must be a “customer,” which generally means registering for an account. The VPPA allows individuals to sue and collect damages of $2,500 or more per violation, plus attorney fees. The Cable TV Privacy Act requires cable television operators to protect subscribers’ personally identifiable information and notify customers annually about what PII is collected and how it’s used, how long the information is maintained, where and when the subscriber can access it and what legal limits and consumer rights exist. Cable and satellite service providers also are prohibited from using the cable system to collect or disclose PII for advertising purposes without a subscriber’s written or electronic consent. 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. New rules under the Federal Communications Act have been proposed that would require broadband internet service providers to get explicit opt in consent from customers before using or sharing their data in certain ways (not related to the provision of service or some affiliate marketing efforts). (The proposed rules had not yet been voted on by the Federal Communications Commission (FCC) as of September 2016.)

- If you don’t want to share your viewing history, avoid using “Like,” “Share” and similar buttons when accessing video. And don’t use your Facebook or Google account to sign in to sharing services if you don’t want your viewing or search history to be tied to those accounts.

➡SLIDE #12

Go over slide notes.

Slide notes:

- Smart TVs have some important similarities with computers and mobile devices: They run on software (or apps), they are connected to the internet, they may have a built-in camera and microphone, you can sign in to online accounts, your viewing history could be gathered and shared, there is the potential to be hacked, etc.
- As with computers and mobile devices, you can't achieve absolute privacy on a smart TV (unless you disconnect it from the internet, but then why have a smart TV?), but there are some steps you can take to reduce some of the privacy risks related to being connected to the internet:

--Download apps only from trusted sources.

--Check the software/app and device "Settings" to find out whether you can reset them to limit ad tracking.

--Install software/app updates as soon as they're available (or automatically) so that you have the latest security patches.

--Avoid entering sensitive information into the TV's browser or apps.

--If possible, connect the TV to a "guest" account you create on your Wi-Fi network—that will keep it separate from your computer and other devices if a hacker ever got in.

--Opt out of (or don't opt in to) content tracking and/or data sharing, if that option is offered.

- Some consumers express concerns about smart TVs' ability to see or hear them, but these capabilities are not much different from your smartphone's ability to respond to your question or command (Siri) or allow you to video chat. You can turn off these functions in your TV (most likely through the Menu button on your remote control) but this will remove much of the functionality of your high-end TV.

➡SLIDE #13

Go over slide notes.

Slide notes: According to its website, the YouTube social network has over a billion users—almost one-third of all people on the Internet!—and every day people watch hundreds of millions of hours of video and generate billions of views. And YouTube's not even the only video sharing option! Based on those statistics, it's very likely that you or someone in your family watches shared video and/or shares video with others. If so, you should be aware of your privacy options.

Privacy settings: As with all social networks, there are ways to exercise some measure of control over who you share video with. 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.

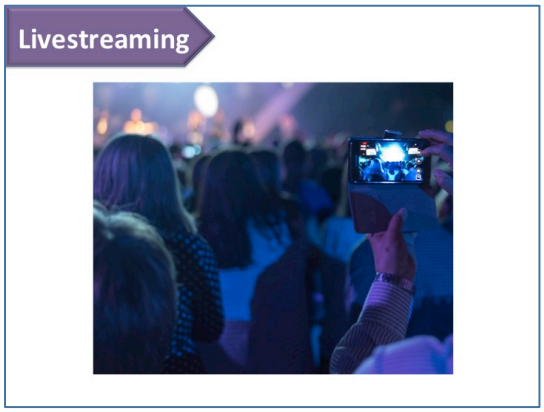
- **Requesting removal:** What recourse do you have if you do not want a video in which you appear to be shared? That depends. In many cases, the best place to start is by asking the video poster to remove the

video. The next step is to appeal to the social network. Each has its own procedure for reporting, or "flagging," offensive or undesirable content, and its own criteria for removing content. For example, YouTube has a system that allows you to "Report" a video by clicking on the flag icon (under the word "More" below the video when viewing in a browse). You will be asked to explain why you think the video should be removed, 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 someone is posting unwanted comments regarding a video *you* posted, you have the option to delete them so they can't be seen by the rest of your audience, and you can "block" the user so they can't view your videos or leave more comments. You can also turn comments off for any video, or manage comments by requiring pre-approval before they get posted. Check the policies of the social network to find out what types of content qualify for removal and the process for requesting removal or changing settings.

- **Legal action:** It is illegal for your image to be used for commercial purposes without your permission. Whether or not a non-commercial video of you is illegal will depend on a variety of factors, which might include where it was taken (in public or private) and what the content of the video is. Contact an attorney if you think you have a case.

➡SLIDE #14

Go over slide notes.



Slide notes:

- Livestreaming means broadcasting—or sharing—video live, as the filmed event or activity happens. No longer exclusive to sporting and news events, today anyone with a smartphone, a livestreaming app such as Meerkat or Periscope, and a video social network account can share live video.
- What rights do you have to privacy in the case of livestreaming? Privacy laws generally don't apply in public places. However, it's illegal for video of you in a public place to be used for commercial purposes without your signed release. In private settings—places where you have a "reasonable expectation of privacy," such as your home or a public restroom—it is generally illegal to photograph or record you without your permission.
- It's impossible to ensure that you won't appear in video of a public place—you could be walking down the street while a tourist just happens to be filming the scene of his visit and then posts it online—but you can reduce the chances of being included by avoiding being in a particular public place when the likelihood of filming is high (at a protest rally, for example).
- If someone keeps their live video posted/shared for later viewing, you can follow the same process to have an offending video you're in removed: Ask the owner of the video to take it down, and if that doesn't work, ask the social network to remove it. As with any request for social media content removal, success will depend on the social network's content policies and judgment of the shared item.
- As with prerecorded (non-live) video, it is illegal for your image to be used for commercial purposes without your permission (for example, a photo or video showing you working out that is used in an ad to sell gym memberships). Whether or not a non-commercial video of you is illegal will depend on a variety of factors, which might include where it was taken (in public or private) and what the content of the video is. Contact an attorney if you think you have a case.

➡SLIDE #15

Go over slide notes.

Slide notes: Despite many consumers "cutting the cord"—giving up cable or satellite TV in favor of streaming options—millions of Americans still pay traditional sources for their television service. For those customers, the FCC requires cable television operators to protect subscribers' personally identifiable information and notify customers annually about what PII is collected and how it's used, how long the information is maintained, where and when the subscriber can access it and what legal limits and consumer rights exist. Cable and satellite service providers also are prohibited from using the cable system to collect or disclose PII for advertising purposes without a subscriber's written or electronic consent. 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. If a service provider violates your privacy rights, you can sue.

If you experience a problem you cannot resolve with your cable, satellite or internet service provider, file a complaint with the local or state public utility commission. Find your state's office in the directory at https://transition.fcc.gov/wcb/iatd/state_puc.html.

PRIVACY, PLEASE! (EXERCISE) (10 minutes)

Assign participants to work on the exercise on page 20 of the lesson plan. Ask for volunteers to share their answers. (Answer key is on page 21.)

RESOURCES (10 minutes)

Learning objective: Be aware of the various resources that provide consumer information on the topics of internet safety, social media and online video privacy and consumer data collection.

➡SLIDE #16

Introduction: Governmental and non-profit organizations offer countless resources for consumers who want to learn more about staying safe and protecting their privacy online. In addition to these sources of assistance, consumers can look to social media networks, service providers and other businesses for their specific privacy policies, usage guidelines and account management instructions.

Go over the resources on slide per slide notes. *(Note: If you can project your computer screen, visit one or more of the sites to show participants what they will find.)*

Slide notes:

- **Consumer Action:** Learn more about online and social media privacy in Consumer Action's "Put a Lock on It: Protecting your online privacy" (http://www.consumer-action.org/english/articles/put_a_lock_on_it) and "Privacy and control for social media users" (http://www.consumer-action.org/english/articles/privacy_and_control_for_social_media_users). Learn more about modern TV and video technology and privacy in the Changing World of TV and Video issue of *Consumer Action News* (http://www.consumer-action.org/news/articles/canews_spring_2016#streaming_privacy).
- **FTC:** The Federal Trade Commission (FTC) offers consumer publications on many topics, including "Understanding Mobile Apps" (https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps),

"Online Tracking" (https://www.consumer.ftc.gov/articles/0042-online-tracking) and "Kids and Socializing Online (https://www.consumer.ftc.gov/articles/0012-kids-and-socializing-online).

- **FCC:** The Federal Communications Commission (FCC) is in charge of making rules for communications by radio, television, wire, satellite and cable in the U.S. Get details about cable service provider subscriber privacy requirements (https://www.fcc.gov/consumers/guides/cable-companies-record-retention-and-cable-subscriber-privacy) and proposed rules to protect broadband consumer privacy (https://www.fcc.gov/document/fcc-releases-proposed-rules-protect-broadband-consumer-privacy). 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.
- **PRC:** The non-profit Privacy Rights Clearinghouse offers a large library of information on privacy, including a section on online privacy and technology (https://www.privacyrights.org/topics/11) and one on social networking privacy (https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social).
- **ConnectSafely.org:** ConnectSafely offers a plethora of resources, including some in Spanish, and many regarding safe blogging and social networking targeted to a parent/teen audience, as well as a newsletter you can subscribe to (http://www.connectsafely.org/safety-tips-advice/).
- **EPIC:** The "EPIC Online Guide to Practical Privacy Tools" offers a long list of web browsers, software, message services and other tools to increase your privacy online (https://epic.org/privacy/tools.html).

QUESTIONS AND ANSWERS (10 minutes)

Preparation: Review the *What's not to 'Like'? Protecting your privacy on social media* and *Watch out! Online video and your privacy* publications and the *Questions & Answers: Social media and online video privacy* backgrounder.

Open the floor to questions.

WRAP-UP AND EVALUATION (5 minutes)

➡SLIDE #17

See page 22 of this lesson plan for the course evaluation form and instructions.

Thank participants for joining you today and ask them to fill out the evaluation form and leave it on a table or in a large envelope you provide. If you will be conducting other trainings at a specific future time, announce that now and encourage everyone to attend.

Goodbye, TMI (exercise)

For each of the following social media "shares," identify how someone could use the information against the person who shared it. Then determine if there are changes they could make to share safely.

1) YouTube: A "hidden camera" compilation of children enjoying the toys in the store posted by Tom's Toy Town on the business's YouTube channel.

_____

_____

_____

_____

2) Facebook: "As a lot of you know, Jenny and Josh are entering 6th grade in September. I'm looking for someone to pick them up from Hoover Middle School (on MacArthur Street) at 3:15 on Tuesdays and Thursdays and drop them at home. (No babysitting needed…they can take care of themselves until I get off work around 5:00.) Thanks!"

_____

_____

_____

_____

3) Twitter: "Anyone want to call in sick with me today? Beach? Movie? #HateMyJob"

_____

_____

_____

_____

4) Instagram: Photo of 18-year-old student at a bar, with drink in one hand and fake ID in the other.

_____

_____

_____

_____

Answer key: Goodbye, TMI

1. Tom faces two potential issues. First, while there's no federal law making it illegal to photograph or videotape children playing in a public space without a parent's consent, parents who see video of their child being shared online without their consent could object, contacting Tom to request removal, flagging the video for removal by the social network or even attempting to take legal action. Even if none of these steps were successful, the unapproved video sharing could foster distrust among parents—the last thing a child-centered business would want. Second, even if the video itself is not illegal, it is illegal to use anyone's image for commercial purposes without that person's consent (or in this case, a parent's consent). If Tom did not receive written consent from the parents of all the children in his "hidden camera" video to be used to promote the business on the store's YouTube page, he could be sued. Tom's best course would be to obtain parents' signatures on consent/release forms *before* videotaping and only record and share video of those children whose parents have already consented.

2. This parent just shared all the information anyone would need to get to her children—their names, their school (including the street, so someone who didn't know what city the school is in can look it up), what days and times the kids will be expecting someone to pick them up, and how long they'll be home alone. Conceivably, someone with bad intentions could show up at the school and say that they are picking them up because the person they were expecting had an emergency and couldn't make it. By calling them by their first names (provided in the post) and knowing the schedule, the imposter can establish legitimacy and gain the kids' trust. While the parent probably shared this only with his or her chosen audience, there is always the possibility that the information could get out. For example, maybe a friend of the parent cross-posts to her own network because she knows some parents who also have kids going to Hoover Middle School. You just can't be sure that the information will stay out of the reach of a predator. The parent would have been better off to post to a select audience something limited, such as "As a lot of you know, my kids are switching schools in September. I'm looking for someone to pick them up and take them home a couple of days a week. Private message me for details and to discuss."

3. Because of the ability to retweet, this employee's message could get shared much more widely than he intended. If any of his followers are also coworkers, any one of them could inadvertently—or purposely—expose the tweet to their boss or another decision maker in the company. Even if that doesn't happen, what if he needs to find a new job one day and expects to tap his network of friends and family for leads. Would you feel confident hiring or recommending him? Not everyone loves their job, but it's best not to share that on social media.

4. There are so many things that could go wrong for this student. First, the use of fake identification is a crime; drinking in a bar under the age of 21 is another crime. Second, assuming some of this student's schoolmates are also his/her Instagram followers, it's not too farfetched to think that one or more of those students' parents might see the photo (or be told about it) and report it to the school. Third, since there is no guarantee of privacy on the internet, it's not inconceivable that a college admissions officer and/or current or future employer could find the photo and make an unfavorable decision based on it. This student's best decision would be to not use a fake ID and to not go to a bar. If he is determined to do those things, he should, at the very least, not provide evidence of his bad choices.

Privacy, please! (exercise)

Select from the choices at the bottom of the page to complete the following statements.

1) The first thing you should do after opening a social media account is adjust these to match your privacy preferences.

2) Social networks typically allow you to do this when you feel that content is inappropriate and should be removed.

3) These help consumers evaluate, or "vet," an app before downloading it themselves.

4) Apps/companies that display these must meet certain minimum privacy standards.

5) This makes it illegal for companies to collect certain information from children under 13 without a parent or guardian's permission.

6) These help parents monitor their children's internet activity and limit what they are able to do, read or view online.

7) These are used to lock intruders out of your accounts and devices. Don't reveal yours!

8) If an app or website doesn't have one of these posted, it's a red flag.

9) This can help companies detect fraud—a good thing—and target their advertising efforts—not always such a good thing.

10) This can be used to tie data directly to a specific individual.

11) These are small tracking files placed on your computer by websites you visit.

12) This browser setting tells websites you do not want to be tracked from site to site—but it's not always honored.

13) Using this means your browser won't save any information about the websites you've visited—but that doesn't mean those sites can't track you while you're there.

14) This is intended to prevent advertising—particularly nuisance pop-ups and banners—from showing up while you're surfing the web.

15) This acts as a middleman between your computer and the internet so that your online activity is no longer associated with your personal IP address.

16) Creating this for connecting your smart TV to the internet can help to protect the other devices on your Wi-Fi network if your television were to be hacked.

17) This requires streaming video providers to obtain customers' consent in order to share information about their viewing preferences on social networks.

18) This prohibits cable and satellite service providers from using the cable system to collect or disclose PII for advertising purposes without a subscriber's written or electronic consent.

COPPA	Reviews and ratings	Flag it	Privacy seals	FTC
Passwords/passcodes	Big Data	DNT	Ad-blocker	VPN
Private browsing	Parental controls	Settings	Privacy policy	Cookies
Cable TV Privacy Act	Guest account	Remote control	VPPA	PII

Answer key: Privacy, please!

1. Settings
2. Flag it
3. Reviews and ratings
4. Privacy seals
5. COPPA
6. Parental controls
7. Passwords/passcodes
8. Privacy policy
9. Big Data
10. PII
11. Cookies
12. DNT
13. Private browsing
14. Ad-blocker
15. VPN
16. Guest account
17. VPPA
18. Cable TV Privacy Act

Training evaluation:
Social media and online video privacy

Please help us improve future presentations by giving us your opinion of today's class.
Circle the response that best reflects your feelings about each statement.

1. I have a better awareness of the privacy risks associated with online sharing.

Strongly agree Agree Disagree Strongly disagree

2. I feel better prepared to protect myself and my family when using social media.

Strongly agree Agree Disagree Strongly disagree

3. I have a greater understanding of how consumer data is collected and the privacy tools available to me.

Strongly agree Agree Disagree Strongly disagree

4. I have a better awareness of the privacy implications of online video and my options for avoiding my image or viewing history being shared.

Strongly agree Agree Disagree Strongly disagree

5. I know where to find additional information and assistance regarding online privacy.

Strongly agree Agree Disagree Strongly disagree

6. The instructor was well informed.

Strongly agree Agree Disagree Strongly disagree

7. The materials I received are easy to read and understand.

Strongly agree Agree Disagree Strongly disagree

8. I would like to attend another class like this.

Strongly agree Agree Disagree Strongly disagree

On a scale of 1 to 10 (10 being the best), how would you rate the training? _____

Please let us know how we could improve future trainings (use back, if necessary):

_____

_____

_____

_____

Thank you for attending!