Privacy Educators Program

Teacher Training Manual

fordham.edu/privacyeducation

Introduction and Contents

This Teacher Training Manual is designed to instruct privacy educators. Privacy educators can consult this handbook to educate themselves on the topics covered by the Privacy Educators curriculum. The materials presented here suffice to supply a privacy educator with knowledge adequate to successfully teach the curriculum to others. Of course, privacy educators need not limit their study to the materials presented here—they can feel free to further edify their knowledge by using any additional resources that they may desire to use. Supplemental lesson plan outlines provide roadmaps for in-class presentation. Here, the materials appear as follows:

LESSON 1: Introduction to Privacy

Objective

This session will introduce the concept of privacy and discuss its importance. Students will investigate what privacy means to them and how it is relevant in their daily lives. The lesson will create a baseline for subsequent sessions on more specific privacy and technology issues.

Introduction

What is privacy? Have you heard anyone say that people are giving away too much of their privacy, or how technology is reducing our privacy? What do you think they mean?

There's no "right" answer when it comes to privacy. In fact, we value privacy because it allows us to make individual choices that other people might not agree with. Think about it: people often talk about wanting privacy so that they can do things, think things, and talk about things that they don't want others to know about. As we'll discuss, there are many reasons that you might not want other people to know these kinds of things. One example is that you may anticipate that others might disapprove: they might think the book you are reading is inappropriate, that the blog you read is too nerdy or too feminine or too masculine, or that the people you talk to online are not the type you should be friends with.

By anticipating this, and by avoiding that kind of judgment, limitation, or censorship, privacy and technology can provide a very useful kind of freedom: the freedom to make decisions about who you are and what your interests are. Technology, coupled with privacy, can allow you to do this free from the pressures that might come from social expectations, peers, or in-school identity.

The idea behind this program is to get students to think about what privacy means for them, to question how some of their behaviors impact their privacy, and to give them some tips that will help them achieve the amount of privacy that they want.

Privacy is a tricky concept to describe, as it can mean different things to different people. It may be easier to describe privacy by talking about what it *isn't.* For instance, it can sometimes be helpful to think about things that are public or shared as a way of distinguishing what is *not* private.

Typically, when we say that information is public, we mean "not private." "Public" doesn't necessarily mean that everyone in the public *actually* sees or hears something, but rather that they *could* see or hear it without much effort. Facts printed in a newspaper article are considered public information because even though not everyone reads the newspaper, theoretically anyone could pick one up and read the information contained therein. Messages printed on billboards are clearly public. Things posted on websites that can be accessed without a password are also considered public.

Scenarios for Discussion

Think about whether the information being communicated in the following scenarios is public or private. Integrate a discussion of these scenarios into your lesson plan.

- ***Talking on a cell phone in public.*** Does it matter if you are talking on your phone in a park where you don't know everyone, as opposed to outside of your school where you do know everyone? What is different about those situations?

- ***Talking on a phone in your room with the door closed.*** What if people in the hallway can hear you? What if the door is open? What if you share that room with another relative so that it is also their room—is it possible to have privacy there?

- If you and a friend are talking on the sidewalk outside of a store, is it ok for someone else to overhear you as they walk by? What if they stop and stand next to you and listen? What if they record your conversation and post it on the Internet?

    - Do your expectations about whether or not anyone is listening affect how you feel about the privacy of a situation?

    - Even when someone is listening, does whether or not you think they care about what you're saying influence how you feel about the privacy of the situation?

    - When you can hear someone talking on their phone, do you listen to what they are saying? Do you repeat it to others?

    - If you do, how does that affect the phone-talker's privacy? What about the person on the other end of the phone call who may or may not even know that people are listening on your end?

- When you get a text from a friend, do you feel ok showing it to other people? Does it depend on what the text message says?

- You send someone a text and they get it while hanging out with a group of other people. Is it still private? Can they show it to everyone? Can they talk about it?

- Is this different from what happens when you respond to someone on social media?

- **Google Maps:** To make its Google Maps, Google uses a fleet of cars with specialized equipment on them to drive around and take pictures of public streets (i.e., streets that everyone can drive on—not people's home driveways). The pictures that the cars take are then put onto Google Maps "Street View" and can be seen by anyone on the Internet. Some people are upset that they were photographed by the cars while walking down the street. Others are upset that pictures of their homes were put online without their permission. Do they have a right to be upset?

    - People in Germany were so upset that Google stopped taking pictures of their homes (and began blurring photos that it had already taken). These houses were

all visible to the public. Does it make a difference that they were being put on the Internet where anyone on Earth could find them (as opposed to only the people who happened to be walking down that street)?

- A friend writes something angry about a teacher on a social network, and someone shows it to the teacher. Is this a violation of privacy?
    - Consider that many things posted on social media are available to the public. Does it matter that the teacher *could have* found the comment on his or her own, even if he or she didn't?
- You're shopping at a pharmacy and notice that a store employee is following you around and making a list of not only the things you've put in your basket, but also the items you've stopped to look at.
    - Do people need privacy for the things they buy? What might be some of the downsides of having other people know about what you are buying?
    - The pharmacy often keeps track of things people purchase to figure out what products are the most popular with different kinds of people. Even if you think this violates their privacy, would it change your view if you found out the pharmacy gave its customers discounts in exchange for tracking what they buy? Is this a fair trade-off ?
- Is posting something on social media more private or less private than talking about it with a group of friends at school in the cafeteria? Are there differing degrees of privacy across social media platforms? How does the *form* of communication impact privacy?
- If you post something to a social network and limit it to "private" or "friends only," do you expect many people to see it? Do you feel as though you have control over who will see it and what they will do with the information in your post?
- Why might you choose to keep things private versus public?
- Does private mean the same thing as *secret*?
- Are there some things that aren't necessarily secrets that someone might still want to keep private? What are some examples?
- How does protecting your privacy with respect to other people in your life (like friends, "friends," parents, and teachers) relate to creating healthy boundaries and relationships with those people?

LESSON 2: Passwords & Behavioral Ads

Objective

This session will explain how passwords can be used to protect privacy. It will provide students with practical tips for creating secure passwords. Students will discuss the risks involved in sharing passwords. There will also be a discussion about behavioral advertising.

Introduction

This lesson discusses how some different technologies work and how they can affect your privacy. The lesson specifically addresses passwords, sharing passwords, and a little bit about how online advertising can impact your privacy.

Passwords

What is special about passwords? Your computer, phone, and even your Internet service provider (the company you pay to connect to the Internet) all employ technical safeguards that are used to maintain different levels of privacy. Those safeguards keep you from being able to listen in on other people's phone calls and from using your computer to see what your neighbors are looking at on their own computers. But those safeguards are largely out of your control: someone else designed them and someone else makes sure they are working.

Passwords are different because it is left to you to design and maintain them. The better you design your password and the better you maintain its security, the better it will be at performing its job. But what is the job of a password? Let's start by talking a little bit about how they work.

Technology Background—How Passwords Work

Passwords are created at the time that user accounts are created. Websites, apps, and online stores issue accounts so that they can keep track of who is who. For example, when you log in to your email, you are telling the email host who you are so that your inbox is full of emails for you and not for someone else.

Accounts are meant to ensure that the person who creates an account on Monday is able to access the same information on Tuesday, Wednesday, Thursday, and 5 years from now. Millions of different people use sites like Gmail, Facebook, Twitter, and stores like Zappos.com and Amazon.com. Those businesses want to keep track of who is who. This means they need to identify you somehow—by remembering your user name and password.

Typically, any account has two parts: a user name and a password. The user name is usually the first thing you type when you are signing in. It is often a nickname, a screen name, an email address, or your actual name. It is typically also how that site or app will refer to you. A password is a code that you enter along with your user name to verify that you are the user who owns the user name that you're trying to log in with.

LESSON 2: Passwords & Behavioral Ads

Crafting a Good Password

First, let's consider what makes a bad password. Passwords that are easy to guess or obvious, such as variations of your name, "1234," or "password" are weak, as are passwords that have been shared or recycled on multiple sites. Passwords that are too hard to remember might also be weak: if you need to write it down somewhere, someone might find your note and learn your password.

So what makes a good, secure password? Your password should be something unique to you that would be difficult for a stranger, or someone who knows you well, to guess. Computers can do a decent job of guessing generic, simple passwords, so the more unique yours is, the better. Adding numbers and mixing uppercase and lowercase letters also helps.

Avoid using things that would be easy to know about you, such as your name, birthday, or favorite teams (if you are a sports fan) and activities (for instance, "ballet" if you are a dancer).

Even good passwords can sometimes be compromised (e.g, when someone figures out your password or gets access to it). Using different passwords for different accounts will help contain the damage if this happens.

Another great way to protect the security of your passwords is to change them from time to time. This is because you might not be able to know right away that someone has accessed your passwords and is snooping on your accounts.

In summary, make sure your password is something easy enough for you to remember, but not obvious enough for your friends or enemies to guess.

Sharing Passwords

Generally, it's not a good idea to share your passwords with other people—especially people that you can't be certain you trust. Sometimes, though, you might need to share a password. For instance, parents or guardians might condition social media use on their having access to the account. Similarly, they might need to know your password to access an online learning system that your school uses.

Remember, though, that even if you never share your password with another person, there is always someone else who knows what it is: the website where you created the account. An actual person working there may not be looking at your password, but for the password to work it must be stored somewhere on one of the website's computers. This is how police (or the government) can find out about information stored in people's accounts even when the person does not give them the password. Police can get a note from a judge, called a warrant, that tells the website to hand police information about a specific person—including information in their account and their password.

Hackers can also sometimes break into a website (and its computers) and steal passwords. This is called a data breach, and when it happens, usually the website will let its users know right away. If you ever get notified that a website you use has been breached, you should change

your password immediately, because now someone you don't know—someone who enjoys committing computer crimes—has it. This is even more important if you use the same password for multiple accounts.

Saved Passwords

Sometimes when you return to a website or an app that you've used before, it will remember you and either have your user name or password already filled in. How are the sites able to remember this information?

You have probably seen this before when you sign up for a new account, log on to a site for the first time, or log in on someone else's computer or phone: your web browser or phone may ask you, "Would you like me to save this password/log in information?"

When you say yes, your browser adds the website address and your password for the site to a small file so that it can be recalled when you go back to the site. That file is called a cookie—a small file that is saved on your computer in a place you probably never look that communicates with the website each time you visit. The cookie reminds the website that you've authorized it to recall your password, and the next time you visit, the cookie reminds the site who you are and that no password is necessary to enter your account.

We're not sure exactly why these files are called cookies, but it might have something to do with the fact that your web browser is constantly asking your computer if it has any and if it will share them (the way you might keep asking for more cookies).

When you go onto your web browser's settings and delete the cookies, websites will no longer have access to username or password information about you. That means they won't be able to remember who you are or what your password is.

Cookies can be useful ways to save time, especially on sites where you have indicated many preferences (for instance, your favorite bands on a music listening site). Instead of re-entering your preferences each time you visit, cookies allow a website to remember exactly how you left things on your last visit.

But enabling sites and your devices to remember you is also potentially risky for your privacy. Consider what happens if you allow a site like Gmail to remember you on your laptop. When you lend that laptop to someone else (or, even worse, if it is stolen) he or she will be able to access your account by simply opening up that site.

Opting to not have a site remember your password gives you the ability to sign in and out after each visit to the site. This prevents other people from accessing your accounts and possibly manipulating them in ways you might not like (for instance, impersonating you to send messages on social media accounts or looking up other passwords you have saved in your email account).

This is even truer when you log in on public computers, such as the ones at a school library. It is almost certain that after you leave, someone else will be sitting down at the computer and

logging in to similar email and social networking sites. Even if they don't have bad intentions, many people become naturally curious when they find they have the ability to peek at other people's private things. Should friends, classmates, and teachers have the ability to sort through students' email messages?

Social Engineering

We've talked about how bad passwords and using passwords carelessly can lead to other people getting a hold of your accounts and your information. Now we are going to talk about ways that people can get into your accounts even when they don't know your password.

Social engineering is the process of using small pieces of information that people learn about you to get *even more* information about you. They start small and build up more and more with the goal of obtaining as much private information about you as they can. It can enable them to hack into your email or social network account, assume your identity, use your credit cards, and more. They might even be able to change your password for you and lock you out of your own accounts.

How does social engineering work? As one example, many password-protected accounts have security questions that you can use in place of a password. These are often questions such as, "What is the name of your first pet?" or "What street did you grow up on?" or "What was your 1st grade teacher's name?"

For adults, the answers to these questions come from things that happened so long ago that it's unlikely anyone else will remember the answer. But for young people, many of their friends may know the answers to those questions.

Further, you may be unknowingly giving away those answers to the public when you post information about yourself online. Imagine that someone sees a picture you've posted of your dog with the caption "Me and Rooster." Next, they go to one of your email or social networking accounts and try to sign in as you, but they don't know your password. Instead, they click "Forgot My Password." The site then prompts them with a security question. If that question is "What was your first pet's name?" then this person will have a very good guess and may be able to get into your account.

To prevent this, it is good to pick security questions and answers that are not things that will come up frequently in either online or offline conversations. Think of choosing a security question and answer the way you think about creating a password: the more obscure and harder to guess, the better.

Scams

Hackers and scam artists can steal your passwords and your information. When this happens, it's called a *data breach*. Sometimes when this happens, a website will notify you. If you think your information has been compromised, you should change your passwords immediately.

LESSON 2: Passwords & Behavioral Ads

One way scammers get your information is through "phishing"—a process by which the scammers pretend to be trustworthy so that you give them valuable information. Often, these come in the form of emails from people telling you that you've come into a great deal of money and that they need your bank information before giving it to you. Other times, imposter versions of real websites try to get you to enter valuable personal information.

Behavioral Advertising

Now we are going to talk about something different: the ways that we are sometimes secretly followed around when we are on the Internet and the reasons for why this happens.

Recall the scenario where an employee follows someone through a store and watches the things they browse and put into their shopping baskets. That is a metaphor for how behavioral advertising works—you're followed around as you browse the Internet.

Have you ever bought something online, or even just browsed through merchandise in an online store, only to later see ads for the same things you were looking at on a completely unrelated website? This is behavioral advertising at work. Advertising companies try to keep track of who you are, what you are interested in, and what you have been looking at. They then use that information to show you ads that they think will appeal especially to you. It is called behavioral advertising because it focuses on keeping track of your online behaviors in order to learn about you.

Behavioral ads work by using cookies to create a digital log about your online activities. That cookie, placed on your computer when you visit most websites, will contain information about the name of the sites you visit, how often you visit them, what you click on, and how long you stay on each site. Based on your web browsing habits, these logs can be used to make guesses about who you are—your age, gender, interests, and even how much money you make.

Cookies also frequently log your IP address. This is a number assigned to every computer by your Internet service provider. Every device that connects to the Internet has its own IP address. That address is critical to how the Internet functions. It is how websites know where to send the text, videos, and images that appear on your computer screen.

Behavioral advertisers associate their log of your behavior to your IP address. This is because behavioral advertising is typically operated by special companies that create and post ads for lots of clients. They might run ads for shoe companies, car companies, political campaigns, and restaurants. Their job is to make sure that the ads for each client reach the Internet users to whom they are most likely to appeal. For instance, a car company would not really want to spend money showing car ads to 12 year olds, but a video game company certainly would.

Many websites sell advertising space on their sites to these ad companies and frequently let the ad company choose which ads to display. Instead of showing the same ad to everyone who visits a site, behavioral ad companies use cookies already on your computer to figure out who you are when you visit one of the sites that they work with. Once they do this they can look at the log file they've created about you and decide which ad they want to show to you

specifically. Because they have your IP address, they can make sure to send that ad directly to you. Other people who visit the same site on the same day will see different ads based on who they are and what they are interested in. If you've been looking at sneakers on a shopping site and later that day you start seeing ads for those same sneakers on a completely different site, this is why.

LESSON 3: Dealing with Social Media

Objective

This session will give students practical tips for navigating tricky social situations that can arise as a result of social media use. Discussions in this session will focus on privacy tradeoffs, managing privacy settings, maintaining a healthy balance between online and offline relationships, maintaining a healthy relationship with social media, and ways to disengage from social media.

Introduction

Networks, including social networks, are ways of linking objects or information together in useful ways. Social networks operate by linking people's profiles together based on a particular set of factors. For instance, you might be connected with other people who list that they have an interest that you also have.

Probably the most common way that profiles get linked together, however, is when users actively choose to be connected to other people. On different social networks, this could be called "making a friend request" or "following." When users' profiles are linked together they become "friends" or "followers."

But designating someone as a "friend" for the purpose of a social network does not necessarily indicate how close you are with a person or how well you know them. All it does is alert the social network that you want your profile linked to that person's profile.

Friending and following also has privacy implications because you can adjust your privacy settings to allow friends or followers to see certain material that others cannot. In this way, friending or following someone tells a social network to give another user permission to see certain content in your profile.

If you have adjusted your privacy settings to "friends only" or "private," determining who you want to designate as a "friend" becomes very important. Whether or not you are actually friends with (or even know) the people you link your profile to, those people will have access to the things you post about yourself and others.

Friends of Friends

Now let's talk about sharing not just with friends but with "friends of friends."

When you choose to share only with people you have actively connected with (i.e., "friends"), you have some grasp on who you are sharing with (though not the people they might share with by showing them your information on their phone or saving screenshots of photos).

When you enable sharing with friends of friends you cede some control over your privacy to your friends. You are sharing with the people that they determine they want to share with. Can you imagine why this might be a problem for someone trying to keep tabs on who is seeing their information?

In fact, a recent study showed that on average, people who choose to share with "friends of friends" end up giving access to over 150,000 people.

Gaming

Gaming implicates privacy as well. For one, gaming consoles are computers, much like your laptops, desktops, or mobile devices are. Many of the topics studied here that apply to computers apply to game systems with equal thrust.

Additionally, popular game systems typically enable user cooperation and interaction. When you interact with other people through these game systems (whether through a chat feature, headset communication, video chat, or some other means), it is important to be careful about what information you disclose. Even if these people are your "friends" in the context of the game, they could potentially jeopardize your privacy if they have access to your private information.

Privacy Policies

Websites and apps usually have a privacy policy. A privacy policy is a document that describes the ways that the site or app collects, uses, and shares a user's information. Different websites or apps have different policies, so it's important to review the policy for each site or app you use. Privacy policies often change, so it's also important to check to see if a site or app you use updates its policy. Privacy policies can usually be viewed by clicking on a link provided by the site or app.

Social Network Privacy Settings

The popular social networks and apps you use usually allow you to adjust your privacy settings. Some adjustments you might make could include limiting who can see your posts and photos, disabling location settings, or changing what other networks or apps the particular service shares your content with. You can usually find these settings by clicking or tapping an icon that looks like a gear. Each social network or app is different, so explore the settings on your favorite services to see what changes you can make.

Drama, Haters, Bullies, and Flame Wars

Now we are going to discuss what can happen when drama, bullying, or embarrassing things happen online.

Reporting Hate and Bullying

If drama, bullying, or embarrassing or inappropriate content appears online, you can report it to the website or app. Reporting bad content to a social network will not guarantee that they remove it, however. Most sites have a set of criteria that they use to make determinations about whether to remove content. For example, Facebook will remove content that contains hate speech (like racial slurs, anti-gay slurs, anti-woman slurs), pornography, harassment, and information about self-harm (like suicide, cutting, or eating disorders). But mean comments

about you, while very upsetting to you, may not rise to the level of a site's own definition of these things.

Beyond Reporting

Since reporting content will not always give you the successful resolution you are looking for, there are some other steps you can take:

- Unfriend or unfollow the user in question. This will prevent them from commenting on your account or contacting you.

- Block the user. This will prevent them from seeing any of your information, even if they are friends of friends. Usually, sites and networks will refrain from alerting the person you've blocked that you have blocked them. But that person may be able to figure this out on their own. If your account was set to public, consider changing your account to a private one so you can place clearer limits on who will see what you post. As we've discussed, sharing only with approved friends doesn't guarantee that one of your friends won't pass along something you've posted, but it does give you a bit more control.

- Don't respond publicly to hateful comments with more anger. This will only serve to motivate someone seeking to get a rise out of you. Instead, consider sending the person a private message explaining why you are upset. Another option is to simply ignore that person.

- Document and save what has been said.

LESSON 4: Mobile, WiFi, Facial Recognition

Objective

Rather than discuss abstract notions of privacy and expectations, this session will focus on how the technologies we use every day may be compromising our privacy in unexpected ways. Students will learn the basics of how certain information technologies work and will be able to discuss the costs and benefits of data collection. We will discuss how these technologies impact their privacy and how they can have an effect on those outcomes. Topics include mobile phones, GPS, WiFi encryption, and facial recognition.

GPS & Mobile Technology

Let's talk about cell phones. Almost all of us have them. And we know that cell phones are capable of figuring out where we are. Smartphone apps that use your current location to provide you specialized information are called "location-based" services. Because of the nature of how mobile phones work, your phone is constantly making calculations about your current location and sharing that location with your phone company. When you use location-based apps (like maps that give you directions or apps that recommend restaurants and movies that are near you), you are allowing your phone to share that information with the companies that run those apps.

Mobile Phones

There is actually an important reason your phone and phone company need to know where you are. Mobile phones make calls by sending out and receiving radio waves. Although your phone does not need to be connected to wires to make calls, those waves do need to reach your phone company, who in turn needs to pass them along to the person you are calling (or the website you are trying to visit if you are browsing the Internet on your phone). This works through the use of cell towers. These towers are set up in tens of thousands of locations around the country and act as receivers for the waves coming into and going out of your phone.

When you make a call, your phone sends a signal to the nearest tower, which is connected to wires in the ground. Those wires are maintained by phone companies. They relay your call signal to the cell tower (or land line, or computer) that is nearest to the person you are calling. That tower sends out radio waves that get picked up by the other person's phone.

In order to know which cell tower to connect to, your phone is constantly picking up signals from nearby towers and sending back signals about how far away it is from those towers. By combining your phone's distance from the nearest three towers, your phone, and your phone company, can get a pretty good idea (within a few hundred feet) of where your phone is at any given time. This happens even when you are not making calls so that when you do decide to place a call, your phone already knows where the nearest tower is located so that the signal transmission can begin. The only way to prevent your phone from transmitting your location to the phone company is to turn it completely off.

LESSON 4: Mobile, WiFi, Facial Recognition

GPS

In addition to cell towers, location can also be tracked via GPS (global positioning system). GPS is a technology that relies on satellites orbiting the earth, rather than cell towers, to calibrate your location.

Who might want to know your location information? There are many possibilities:

- ***Your phone company:*** That is, the company you pay each month to provide you phone and data service.

- ***The company who makes your phone:*** In 2011, researchers discovered that secret computer programs had been incorporated into Apple iPhones and Android phones that kept logs of the phones' locations and sent the information back to the manufacturers without customers' knowledge.

- ***Parents:*** Parental monitoring services allow parents to install apps on your phone that can allow them to track your whereabouts. If the apps use GPS coordinates, they may even be able to measure the time it takes for your phone to move from one point to another. This means that if you are driving, GPS can tell how fast you are going even without being connected to your car.

- ***Companies whose location-based apps you use:*** Those companies take the geographic coordinates of your phone and match them to data that they have (which could be coordinates of a map, coordinates of a particular store, or the coordinates of other people who are using the app). Typically, these apps ask for permission to use your location when you first download and install them.

  Often, you can go into your phone's settings and disable the location-based functions of these apps (which will limit how useful they are), but you should realize that for most location-based apps, once you initially agree to allow them to use your location they do not come back and ask your permission each time you use them. You provide consent once.

- ***Advertisers:*** Behavioral advertisers might buy your location information to target area-specific ads to you.

- ***Lawyers and police***: Law enforcement might use location data when trying to find out information about you in relation to a criminal investigation or lawsuit. If they want to know where you were at a particular time, it is very helpful for them to ask your phone company or an app company. In 2011, phone companies responded to 1.3 million requests from law enforcement about phone users' text messages, locations, and lists of who they called and when.

LESSON 4: Mobile, WiFi, Facial Recognition

Choosing to Share Your Location

In addition to all the different people and groups listed above, people can learn about your location when you do things to actively share it with them. This kind of sharing requires you to make a decision about revealing your location not just to an app or a company but to other people—sometimes people you know, but possibly to ones you do not know.

This can be done through "check-in" apps, where users self-report their current location. This location is then shared with other application/social network users who have been authorized, typically by being your "friend" or follower. Before using these services, be careful that you have checked your settings and read their privacy policies. If you are sharing with the public, anyone will be able to find out where you are each time you check in. Be aware that you may unknowingly give away your location, even without clicking "check in," based on other things that you post (for example, "Going to soccer practice and then to the mall").

Even where your settings are not shared directly with the public, if you have them linked to another account, then you may be sharing with a very wide range of people.

In addition, public location sharing can also be combined with other public profile information to allow people to learn about you and approach you without actually knowing you.

WiFi and Encryption

Other than using a smartphone, another way of getting online is with a wireless Internet connection—often referred to as "WiFi." In the same way your phone uses radio waves to connect to cell towers, computers (and smartphones) can use radio signals to connect to the Internet.

When you log in to free or open WiFi hotspots (generally, Internet connections that do not require a password) you are connecting to the Internet using an "unencrypted connection." Encryption is a technology that helps ensure privacy and security by taking the bits of information sent over a network and encoding them. Only computers (and other devices) that have the correct encryption key are able to unscramble the data and put it back together in a way that makes sense. Encryption is commonly used in online commerce, such as banking and shopping where there is a risk of someone getting their hands on very valuable information (like credit card numbers).

Google's map-making cars (Discussed in week 1 lesson "Introduction to Privacy") were gathering more than just photos while they were driving around cities and neighborhoods. They also used very specialized equipment that detects WiFi networks (the way your phone or laptop asks if you want to join new networks when you are in a new place). The German government discovered that when Google's cars encountered an open WiFi network (one that was not protected by a password) they were intercepting information that was passing through the network. This meant Google could see parts of people's email messages and find out which websites they were browsing.

Do you think it's ok to do this when people do not protect their networks? Google has argued that what they were doing was no different than listening to radio signals on a car radio. What do you think?

In multiple instances, people with open, unencrypted WiFi networks have found themselves in trouble because the bad behavior of others. Unscrupulous strangers have logged onto the Internet via their open WiFi networks and engaged in illegal activities like trafficking in child pornography or engaging in credit card fraud. When police investigators track them via their Internet connection they end up at a house with an open WiFi network and a very confused and scared Internet user. Do you think people should be required to put passwords on their networks to prevent this type of thing? Are there any good reasons for keeping your WiFi network open and password-free? One reason is generosity—you may like the idea of providing free access to passers-by or people who need to connect quickly while they are away from home.

Facial Recognition

Now let's talk about something a little less technical and a little more personal: your face. Besides our names, our faces are one of the most basic ways that we identify each other. As computers become more and more advanced, however, they are starting to acquire the ability to identify our faces as well.

How does this happen? Facial recognition technology is software that analyzes digital images to look for a particular set of patterns—patterns that indicate the image is a human face. For instance, software can locate clusters of dark dots and measure how far they are from similar clusters of dark dots. If they are within a certain distance, the software will make a guess that those dark dots are actually eyes, at which point it can look for other shapes that might be a nose, mouth, ears, etc.

Being able to distinguish between a picture of a face and one of a chair is not necessarily a privacy concern. However, since this software recognizes faces by taking very precise measurements of facial features, once a computer has a name to attach to a face, privacy suddenly becomes very relevant.

When you tag your face, or a friend's, in a photo, the recognition software remembers to append that name to that set of measurements. So when the software encounters another photo, finds a face, and measures the distance between, say, the nose and the mouth, it can remember that "Jessie Maxwell" has about the same distance. Maybe this photo is also her.

This means that every time you tag photos with people's names, you are helping the software learn how to better recognize those people. The software can eventually become so accurate that it is able to recognize people in photos even where no one tags them.

LESSON 5: Reputation

Objective

This session will challenge students to think about how to actively manage a digital reputation. It will introduce the concept of audiences and highlight the multiple audiences involved in digital communications. This session will emphasize the permanent, searchable nature of online communications and how this impacts reputation management.

Introduction

Students are the best managers of their own reputations. Thinking about how information might impact that reputation is a useful activity to engage in before posting or sharing. It might be useful to have some non-threatening ways to approach others about content concerning you that makes you uneasy about your reputation.

Audiences

So far, we've been talking about different technologies that we use and the relationships between technology and our privacy. Now we're going to talk about the relationship between privacy and our own reputations. You might think that privacy and your reputation have little to do with each other—reputations are about what others think of us and privacy is about what we want to keep to ourselves.

But thinking about which information to keep private and which information to share has a direct impact on how others will shape their opinions of us. Because of that, it's important to think about who is seeing our information as an audience. Once you figure out who that audience is, you will have a better idea about what information you might want to share with it and what you might want to keep private.

Think of all the multiple audiences of a sporting event: there are people sitting in the stadium, people watching live on TV, people listening to the radio, and people following scores on their phones. The next day, even more people will be reading about the game in newspapers and blogs, and some will go back to watch recordings of the game on DVR. Think of a player who makes an embarrassing play during the game. He doesn't just have to worry about the fans in the stadium laughing—they are only one audience. The blooper will be shown on instant replay to everyone watching on TV at home and most likely uploaded to YouTube, where sports and humor websites can link to it. When something like this happens, multiple audiences can multiply a player's embarrassment. On the other hand, when a player does something good (both on or off the field), technology allows that message to be spread quickly to many people as well.

Because there are so many possible audiences for these things, it can be very tough to *control* who learns about what is happening. Think about the twist ending to a great movie, or the final score of a baseball game: even if the people putting on these events wanted to keep those things secret, or just limit them to the people sitting in the actual audience, it would be very, very tough to do.

LESSON 5: Reputation

Information—particularly juicy information—is difficult to contain and manage. Once it is known by even one person, it often spreads quickly.

If you have a phone with a camera and have ever witnessed something exciting, strange or funny, you can probably relate. How often do you take a picture of something like that and keep it to yourself *without* ever sharing it? Think about times you've received such a picture or video taken by a friend.

Think about the things you communicate with your devices. Typically you have at least one audience in mind, but remember—that's not the only audience who might see what you have written, posted, or shared. There are many other potential audiences out there who might come across your information. We are going to spend some time talking about who the different audiences are when we communicate in different ways.

Thinking About Audiences in Popular Technologies

Text Messages

- Who is the audience?

- Besides the person you send it to there might be other audiences who might see your message: the recipient of your text could forward it, show their phone screen to someone, or take screen shots and post them online.

Social Media Posting

- Who is the audience when you post on social media?

- You have control over who your friends are, but no control over who *their* friends are. They might include family members and employees of your school. Further, you have very little control over what other people say about you, or whether they post photos of you.

- When you add a comment to a discussion happening on someone's social media account, that comment is viewable by the original poster and their friends, even if those people are not connected to you as friends. Be aware that they will be able to see your comments, just as you are able to see comments of people with whom you are not friends.

Monitoring Your Reputation

Other people in your life will use search engines to find out more information about you after (or even before) meeting you. What they find when they enter your name, good or bad, is going to impact how they think of you. If you want to be able to have control over how they perceive you it is important for you to know what information they are likely to see.

LESSON 5: Reputation

Maybe you've Googled yourself before out of curiosity. The next time you do it, try looking at the results from the perspectives of other people: a friend you've just met, an employer with whom you've just applied for a job, a college admissions officer, your teacher, your parents. For these people, your Google results are a like a resume: they will help form their impression of you. If someone has never met you but has your name and runs a search, the results will be forming their *first* impression of you.

When you Google yourself, ask yourself these questions: What comes up first? Is it something to be proud of? Is it something neutral like a link to your social media profile (typically only your name will be visible from the Google results page, and not the content of your profile)? Is your name part of a list (like a list of participants at a sporting event or members of a club at school)?

Think about someone who is scanning this page very quickly, perhaps without clicking the links. What kind of impression do you think they would get about you?

Managing Bad Results

If a search about your name turns up some unpleasant or unflattering results, do you feel like there is anything you can do about it?

Having unpleasant or undesirable search results is not the end of the world. For one thing, as you get older, more and more websites associated with your name will start showing up online and some of that will replace what are now the top search results for your name.

Tips for Handling Other Uncomfortable Content

It is a good idea to have some strategies for handling comments, photos, or other information that could affect your reputation. What might you do if:

> ***You come to regret something you have written?*** You always have the option of deleting content that you have posted. However, you don't have control over what other people do once they've come into contact with that material.
>
> For instance, if you've written a comment on someone's photo in which you used language that you now regret, you can go back and delete the comment. However, the person about whom you've written it has likely seen it, and many of their friends have, too. If they've made a copy of the text or taken a screen shot of the photo comments, then they will have a permanent record of what you've done.
>
> If someone you've written about has seen or heard about what you've said, consider reaching out to them directly and apologizing. Be honest and direct: "I wrote something about you the other day. I'm not sure if you saw it, but I realize that it was mean and/or wrong and I'm sorry." This could help prevent the situation from escalating.
>
> ***Someone else finds something objectionable written by you or about you?*** This scenario is slightly different than changing your mind about something you've posted and going back to delete it. When someone else (a friend, teacher, parent, etc.) approaches you (either

online or in person) to express concern about something you've written, you know for certain that at least one other person has viewed the material and has found it off-putting. You may feel an impulse to delete the content as quickly as possible to make it go away, but remember: things don't disappear from the Internet as easily as we'd like them to.

Keep in mind that if someone is upset by something you've posted they may well have saved a copy of it before reaching out to you. That means that deleting it yourself will not only fail to make it go away, but you may be drawing greater attention and embarrassment to yourself for attempting to cover up a mistake.

Instead of trying to hide the post or erase it immediately, think about *why* the other person was upset by it (or why it gave them concern) and consider offering a direct, private apology to them (and possibly the person your comments were about, if that is a different person), along with an explanation that you plan on removing the material. Additionally, if the comments you made were public, you may want to follow up with a post explaining that you regret what you said and now understand that it was inappropriate.

It will not guarantee that the person won't attempt to remind others of the deleted posting, but it could go a long way to ensuring that a conflict does not escalate into something greater.

Remember that aside from the emotional consequences that demeaning, derogatory, or insulting comments can have on another person, being identified as a bully is something that can haunt your reputation for years, even if you end up becoming a very different person.

You find something objectionable that someone posted about you? We talked a bit about this in the social media lesson. Think about the person who did the posting: who they are might affect how you want to approach the situation. If it is a friend who is maybe just using poor judgment, or someone who maybe doesn't know you very well and thus may not understand how what they've done affects you, perhaps you can simply ask them to remove the material. If you think the person is a bully, this strategy might not be the best move. Bullies want to get a reaction out of you, and pleading with them to stop might be playing into their hands.

If the person is someone you know and is perhaps just using poor judgment, consider sending a private message directly to the person in a calm, non-threatening tone. Calling them out publicly might make them defensive or less willing to help you. If someone has posted or written something embarrassing about you, you may feel the urge to try to embarrass them back. But however good that feeling of revenge might be in the short run, in the long run it is probably not going to help your reputation.

Sending a private, direct message will send a signal that you are serious about the matter. Explain to them why what they've written is upsetting to you. Was it hurtful? Is it simply embarrassing? Are you worried that it makes you look bad? Focus on how the material affects you rather than pointing out their poor judgment. For instance, if they've posted a

photo of the two doing something inappropriate, focus on how *you* are embarrassed about having the picture of yourself out there, and not on how you think *they* should be more embarrassed.

When Asking the Poster Fails

If you've reached out to the person who posted material about you and asked them to remove it and they refuse, is there anything else you can do? There are a few possibilities:

Reach out to someone at school like a teacher, counselor or principal. Teachers and other adults at school may be able to help resolve the problem, particularly if it involves someone else at the school. Additionally, talking to an adult may help you figure out what your options are or what you can do next.

***Reach out to parents*.** This may seem like a strange option if it's your parents whom you don't want to see the bad material about you in the first place! However, if you are involved in activity that could be seen as sending inappropriate pictures (sexting) or verbal abuse (cyberbullying) there may be legal implications. This means the police, your school, and lawyers could be getting involved.

Flirting and Inappropriate Pictures

It is important to understand the serious implications that can result from sending inappropriate photos or content to others, either online or by using your mobile devices.

Naked Pictures and the Law

Sending sexual pictures of people becomes illegal when the people in the pictures are underage. This is the case even when you take and send a picture of yourself if you are underage. In fact, even if you didn't take the picture or send it, just having sexual images of minors on your phone or computer can bring legal trouble.

In situations like that, even though it may be embarrassing at first, your parents will want and need to be involved and to support you. What's more, because of the highly sensitive and illegal nature of these images, websites where they are posted will likely be more motivated to help you get images of yourself removed and get the people who are circulating them blocked or suspended from the sites.

How Flirtatious Photos Affect Reputation

There are few things more private, more personal, and more worth thinking about protecting than your body. The reputational costs of sending naked or explicit photos include possible humiliation and embarrassment among peers who have seen photos of you. Even when other students at your school haven't seen pictures they may simply find out that such pictures exist.

If the photos get posted online, they could be labeled with your name and become searchable so that even when you start at a new school or college your classmates may be able to find them.

LESSON 5: Reputation

While parents, teachers, and principals may be eager to get these pictures deleted from your friends' and classmates' phones as soon as possible, the damage to your reputation may have already been done.

Tips

If a boyfriend, girlfriend, or anyone else is asking you to send a revealing or flirtatious photo, consider the strong possibility that many other people will see it before you take the picture. It is a good idea to have a response ready. If the person insists that they will not share the picture with anyone else, don't feel that you have to relent. Even if the other person doesn't ever intend to share the photo, their friends or parents could end up seeing it if they borrow the phone, computer, or device. And don't forget that the person who is being flirty with you today may turn into someone who wants to embarrass or shame you in the future.

Acknowledgements

Fordham CLIP would like to thank the following people for their help with the development and implementation of this curriculum.

Fordham CLIP Privacy Fellows Jordan Kovnot, Thomas B. Norton and Andrea Flink developed this program during the course of their fellowships with assistance from Fordham CLIP's former Executive Director Jamela Debelak, Executive Director Cameron Russell and Academic Director Joel Reidenberg.

Fordham CLIP would like to thank Sandra Perez, Nichole Gagnon, Celia Kim, Shawn Mitchell, and the rest of the staff at PS 191 in New York City for their cooperation, assistance and support of our program.

Fordham CLIP's Board of Advisors provided suggestions and advice on shaping this project.

The development of this program was supported by *cy pres* funds from the *NebuAd* Class Action Settlement awarded to Fordham CLIP by the U.S. District Court for the Northern District of California and by a grant from the Digital Trust Foundation.

CLIP Center on Law and Information Policy
AT FORDHAM LAW SCHOOL