Privacy Educators Program

Lesson Plan Outlines

fordham.edu/privacyeducation

Introduction

These lesson plan outlines may be used to guide in-class instruction. The materials presented here track those presented in the accompanying Teacher Training Manual. Privacy educators can feel free to modify these lesson plans to meet their needs or the needs of their class.

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. It will create a baseline for subsequent sessions on more specific privacy and technology issues.

Introduction

- Introduce the team and the course, and explain why privacy interests each team member.
- Explain that over the next few weeks, you'll be discussing and learning about privacy in the context of computers, cell phones, social media, email, and related technologies.
- Encourage the students to contribute, and invite them to communicate their opinions, doubts, and questions. Emphasize that there is no such thing as a "right answer" when it comes to privacy, as each person defines privacy differently and is entitled to personal privacy preferences.

Questions to the Class

Discuss with the class the following questions:

- What is privacy? What are some definitions? What are some pros and cons of different levels of privacy limits?
- Have you heard anyone say that people are giving away too much of their privacy? Give some examples of what you think they might have meant.
- How does technology affect our privacy? Give some examples of what you mean.
    - Example: Danger of posting a public status about your vacation plans
- What would you like to get out these classes?

Brief Lecture

- Remember that there's no "right answer" when it comes to privacy.
- In fact, the reason we value privacy is because it allows us to make *individual choices* that other people might disagree with. What are some examples?
    - A book you're reading, a band you're listening to, a game you're playing, or the people you are talking to online or on social media
- Privacy gives you the freedom to make decisions about who you are and what your interests are free from the pressures that might come from social expectations, peers, and maybe even your in-school identity. Given how you can pursue these interests using technology, privacy and technology together give the freedom to make these personal choices.

LESSON 1: Introduction to Privacy

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

Mini-Group Discussion

If possible, break into small groups to discuss the following questions. Be prepared to recap what each group talked about once the class reconvenes.

- Do you think the information communicated in the following is public or private?
    - *Talking on the phone outside:* Does it matter if you're in a park where you don't know anyone versus 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?

- What if a friend posts something angry about a teacher and someone shows it to the teacher? Is this a violation of privacy? Is everything on social media public? Does it matter that the teacher *could have* found the comment on his or her own, even if they didn't?

- Is posting something on social media more or less private than talking about it with friends at school? 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?

Regroup

Recap and reiterate interesting discussion points made by different groups in response to each question.

Visuals and Discussion

- 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 the items you've stopped to look at.

    - Have you ever seen the loyalty/rewards cards used at the grocery or pharmacy? Why do you think that companies have these programs?

    - What if the store gave customers discounts in exchange for tracking what they buy? Is this worth it? Do you think this is a good thing? Should stores be letting customers know beforehand? What if the store needs this info for stocking inventory or a similar purpose?

- What if you're just looking and do not even buy anything? (Show video of store mannequins with cameras, http://www.youtube.com/watch?v=HSDtTxYxpJY)

    - Would you be okay with what you saw in the video? Why or why not?

    - Is it different when it's online as opposed to a physical store? (Show screenshot from website http://weknowwhatyouredoing.com)

- Street View: Google uses a fleet of cars with equipment on them to drive around and take pictures of public streets. The pictures are then put onto Google Maps "Street View" which can be seen by anyone on the Internet.

    - People are upset they were photographed while walking on street or that pictures of their homes were put online without their permission. Do they have a right to be upset?

    - *Pull up your school on Google Street View*

- People in Germany were so upset that Google stopped taking pictures of their homes (and began blurring photos that it had already taken). Does it matter that a house is put on the Internet for anyone in the world to see (instead of just someone on your street)?

Lecture/Recap

- Privacy is tricky to describe because it means different things to different people.
- What *isn't* private? Think about things as "public" or "shared" to distinguish what isn't private.
- Private versus public: If someone can see or hear it, it's not private.
  - Newspapers are public 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 public.

Wrap-up Questions to the Class

Spend the last few minutes with these questions, which build on the opening discussion by applying some of the issues discussed in this lesson to more general privacy concepts:

- Why might you choose to keep things private instead of making them public?
- Does "private" mean that same thing as "secret?"
- Are there some things that aren't necessarily secrets that you might still want to keep private? What are some examples?
- How does protecting your privacy with respect to other people in your life (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 and will assess the risks involved in sharing passwords. The lesson also addresses behavioral advertising.

Introduction

Today we are going to talk about how some different technologies work and how they can affect your privacy. We're going to be talking specifically about passwords and sharing passwords, and also a little bit about how online advertising can impact your privacy.

Ask the class a few introductory questions:

- How many people have at least one password that they use on a daily basis?
- How many people have more than two passwords that they need to remember? More than five?
- How many people know another person's password?

How Passwords Work

Ask the class when and why you might need to use a password:

- When do you usually have to create a password?
    - 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. When you log into 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.

- Why do you think accounts have a user name and a password?
    - It's more secret and private. If your user name is the only thing you need to sign in, other people might see it and could access your account by using it.

- What do you notice that is different about a user name and password?
    - Typically, the password characters are not displayed when you type them.

- Why would you want to prevent people from seeing a password?

Password Activity

Break the class into small groups, if possible. Have each group come up with a list of possible passwords for fictional characters (for example, write fictitious names, birthdays, interests, etc. on the board). Once the groups have finished, have each group share some examples of what it came up with.

LESSON 2: Passwords & Behavioral Ads

Crafting a Good Password

Discuss how to construct a good password. But first, give a few examples of some *bad* passwords: 1234, password, 12345678, qwerty, abc123, iloveyou

- What makes these passwords bad?
- What else might make passwords weak?
    - They are easy to guess or obvious (e.g., variations of your name)
    - They have been shared
    - They are used on multiple sites
    - They are too hard to remember

- What makes a good, secure password?
    - Show the website, http://makeagoodpassword.com

Passwords should be unique and difficult for a stranger or someone who knows you well to guess. How can you accomplish this? By:

- Adding numbers and uppercase letters
- Using symbols for letters, such as $ for S
- Avoiding things like name, birthday, or favorite sports team
- Using different passwords for different accounts or services
- Changing passwords often
- Being able to remember your password

Four random dictionary words may make a more effective password than a random string of characters!

- Test some examples at www.howsecureismypassword.net

Saved Passwords

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?"

- How do you think the sites are able to remember this information?

Cookies

Websites remember your password information by using cookies. Cookies are small files that a website stores on your computer. When you choose to have a site remember your password, your web browser adds the website address and your password to the cookie file. When you visit the site again later, the cookie reminds the website who you are.

- What do you think are some of the reasons you might let a site, or your browser, remember your passwords?

- Are there reasons you might not want to do this?

- Are there certain computers, devices, or sites where you are more comfortable saving your passwords with cookies?

- How many people share a computer with at least one other person, either at home or at school?

- If you do share a computer, do you let that computer remember and save your passwords?

Social Engineering

Social engineering is one way people might access your accounts even *without* knowing your password. Through social engineering, people might compile small bits of information about you. This process might enable someone to guess your password, if it's not secure enough. It can also be used to hack your email, your social networking accounts, and your financial accounts. One of the most common ways access is accomplished through social engineering is by guessing or learning answers to security questions.

- *Tip: Use opposite answers when answering security questions*

- Can you think of any problems with allowing someone to access an account by answering one of these questions?
    - Friends might know the answers to security questions—you might be giving the answers away on social network accounts!

Mini Group Discussion Questions and Hypotheticals

Break into small groups, if possible. Discuss the following questions, and have students report back to the class once they've come up with responses.

- Your mom or dad says you can sign up for a social networking site or app, but only if you give them your password. Would you agree, and would this change the types of things you post and who you decide to "friend?"

- Your best friend suggests swapping passwords for your social media accounts. Weeks later you get into a fight, and now people are sending you messages asking why you've been acting so mean towards them. You're not sure what they are talking about. What should you do now?

LESSON 2: Passwords & Behavioral Ads

- A boyfriend and girlfriend choose to share their social network passwords. They say it makes them feel closer and shows they trust each other. Now the girlfriend is starting to worry that her boyfriend is checking her private messages too often. She is not sure she wants him to be able to access her account, but she is worried about starting an argument with him. What might she do?

- If you would consider sharing a password, would you also consider sharing a credit card number? Giving out your credit card number allows other people to make purchases online (or over the phone) that get charged to you. This is called credit card fraud. Giving your password out allows people to do other things under your name that will be attributed to you.

- Do you have passwords that lock your laptop or phone? What might be some of the benefits of using a password to lock these devices (as opposed to just using passwords on website and app accounts)? How might password protection come into play when your device is lost or stolen? If you choose to use passwords on your devices, what would you do when you want to let a friend use your laptop or phone?

- Has an app or social website ever asked if it could access your contacts to send invites to or locate people you may know? Why might this be good? Why might it be bad? What do you think the app or website is doing to retrieve and send the contact information? How would you feel if a friend's app asked if it could have your contact information?

- Has a public computer ever asked you if you would like for it to remember you the next time you log on (for example, in a library or a school)? Have you ever noticed that a box is already checked "yes" when this question is asked? Why might it be a good idea to uncheck the box or answer "no" when asked if you would like the public computer to remember you? Why might it be a good idea to log-out of webpages that required a password to sign-in?

- Do you share your passwords? Why? With whom? What are some good reasons to share a password? What are some of the consequences that could come from sharing a password? Would sharing a password affect what you do on that account?

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.

- Example: Fake "Prince" emails, http://wafflesatnoon.com/2012/11/26/email-alert-fake-fbi-warning/

Behavioral Advertising

Behavioral advertising refers to when companies advertise to you based on your interests. How do they do this? Advertising companies keep track of your online behavior and activities using cookies, as we talked about earlier. The companies use the information in these cookies to figure out what you browse for and what you like. They then send you advertisements for similar products and services.

- Do you think this kind of tracking and advertising is a good thing?
- Does it help you to find the kinds of things you want to buy?
- Do you ever click on the ads? Is there a downside to this kind of tracking?
- Do you think it is fair to keep track of what people like and what they do online so that they can be shown advertisements?

Recap

End with a brief recap of the lesson's topics, and open the floor for any questions or comments.

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 section 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.

Optional Materials: *Friend Request Worksheet*

Introduction

Today we are going to talk about social networking and some of the tricky situations that can come up when dealing with people online and offline as a result.

Visual Poll

Poll the class and use Excel (or some other visual mechanism) to display the results of the following questions:

- Who uses a social network?
- Which social networks do you use?
- Who has a friend on a social network that they've never met in person?

Technical Background

Spend a few minutes discussing the technical background driving social networks. Then describe the implications of having your profiles set to "private," or set to be viewable by "friends only," as opposed to by everyone. Ask some or all of the following:

- Why do you think a social network might use the word "friend" even though you may not actually be friends with the people you connect with?
- Do you agree to every friend request or follow that you get? Should you? How do you decide?
- Do you friend request or follow everyone you meet?
- Do you friend request or follow people you have never met in person?

Friends of Friends

Discuss the implications of sharing your online posts with "friends of friends" or a similar set of users. Explain what this means in terms of how many people you are actually sharing your information with, and the costs and benefits of this approach.

LESSON 3: Dealing with Social Media

Gaming

Discuss how the topics covered today might apply to gaming on popular gaming systems. Such systems typically enable user cooperation and interaction. Because gaming technologies rapidly develop, it might be a good idea to let the students' input drive this conversation.

Privacy Policies

Discuss website and mobile app privacy policies. If possible, show students how to locate them on a webpage or app, and show examples.

Social Network Privacy Settings

Show students how to manipulate privacy and sharing settings on the popular types of social media. Note that technologies and networks in use among students vary greatly, and older apps or networks become obsolete as new ones emerge. To stay abreast of new trends, ask students about which services are popular and tailor this discussion to meet their interests.

Drama, Haters, Bullies, and Flame Wars

Discuss what can happen when drama, bullying, or embarrassing things happen online:

- Reporting hate and bullying to websites or social networks

- Beyond reporting:
    - Unfriend, unfollow, or block the user in question
    - Don't respond publicly with more anger
    - Document and save what has been said

Questions and Hypothetical Scenarios for Discussion

Break into small groups and discuss the following hypothetical scenarios. Make sure each group will be able to recap its responses when the full class reconvenes later.

- Your 11-year-old cousin asks for your help in setting up an account on a social network for kids. The website asks your cousin for his parents' email address so it can get permission for him to use the site. Your cousin wants to use your email address and asks you to give permission (pretending to be one of his parents). Do you think this is a good idea? Do you think anything bad could come of this?

- What if there's a rumor circulating online that a friend likes a classmate? Should you respond? How? Should you respond on social media? Or in person? How about over phone?

LESSON 3: Dealing with Social Media

- Should parents be on social networks?
- Should middle school teachers be on social networks?
- Do you think social networks are appropriate for kids younger than you (say, 7-10 year olds)?
- Talk about what drama or offensive things may be posted online and how to block or report someone

Recap

Spend a few minutes discussing as a class the small groups' responses to the above questions.

Suggested Activity: Debate

Explain to students that you are going to split them into two groups. Half the class will argue why kids under 10 should be on social networks, and the other half will argue why they should not. Students will have 2-3 minutes to develop their arguments within their group, and then one student from the group will be called on to share the arguments. After both groups have made their case, take follow-up comments and rebuttals from the class.

Review

Use this time to review what you've covered about social media and privacy.

Wrap-Up Questions

End the lesson by getting class input on the following:

- What is something you learned today that you didn't know before?
- Are you going to change anything in your social media profile now that you know all these new things? Why or why not?

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.

Optional Materials: *GPS & Mobile Technology Worksheet*

Intro Poll

Raise your hand if the statement applies to you:

- I have a cell phone.
- I understand how my phone knows where I am when I use it.
- I have signed on to wireless Internet either at my home, another person's home, or at school.
- I know how wireless Internet works.
- I've seen a website or a computer tag my face in a photo by guessing who I am.
- I understand how it figured out who I was.

Mobile Phones

Poll the students to see how many use their cell phones to make calls. Describe how cell phones work, including how the devices use GPS systems and cell phone towers to determine your location, send and receive signals, and transmit calls.

- **Visual:** Show supplemental animation of how the cell phone systems work

- **Visual:** Weird cellphone towers (http://twistedsifter.com/2012/08/examples-of-cell-phone-tower-disguises/)

GPS

Discuss GPS technology and how it works. Solicit student answers for the following questions:

- Given that phones need to know exactly where they are in order to work, can you think of who, besides you, could get that information and figure out where and when you're holding your phone? Why would they want that information?

LESSON 4: Mobile, WiFi, Facial Recognition

Choosing to Share Location

First, poll the class: How many of you choose to share your location with others on apps, social networks, or in some other way?

Describe how location sharing works and its implications for privacy—including how sharing location information enables others to physically pinpoint you by combining location information with other publicly-shared information.

Split the class in half to facilitate a debate (or alternatively, break the class into small groups for discussion). Have one side advocate for the "pro" side, and the other argue for the "con" position, for the following questions:

- What do you think are some of the benefits and drawbacks of sharing your location with just your friends?

- What do you think might be some good and bad reasons to share your location with the public?

- Would the fact that you knew your parents were seeing all of your location check-ins on a social network affect whether or how you might use that service?

WiFi

Discuss WiFi, and remind the class that just as phones and devices use radio waves to connect to cell towers, the devices can use radio waves to connect to the Internet, too. Also discuss encryption and the dangers of not securing devices and networks.

Provide the following anecdotes and solicit student feedback on the questions that follow:

- Google's map-making cars (discussed in the 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 (like 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 intercepted 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 of 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

As computers become more and more advanced, they are starting to acquire the ability to identify our faces.

- Who has ever had an experience where a computer was able to guess their name or someone else's name in a photo?

Briefly describe how facial recognition technology works, and provide some examples of botched attempts at facial recognition (available online). Use the following questions to facilitate a class discussion:

- Some social media allows you to put tags on the photos you upload. Do you think there is a difference between tagging yourself and tagging someone else in a photo?

- Do you have your privacy settings set so that you have to approve tags when someone else tags you? Why or why not?

- Do you ask others for permission before you tag them or do count on social media to do that for you?

- Because of the millions of tags people have put on photos in Facebook, its facial recognition software has the ability to tag peoples' faces on its own, with good accuracy. That is, even if you don't tag the faces in a photo that you've uploaded, Facebook can probably do it for you. Do you think they should?

- In some cities, the police set up security cameras on public streets that are connected to computers with facial recognition technology. The camera looks at everyone walking by and sends pictures to a computer that tries to match the faces with names. Where do

you think those computers get the names to match the faces? (Some Answers: public social media profiles, pictures posted to websites, police databases with mugshots).

Recap

Recap the major topics covered during the lesson. Open the rest of the time to any additional questions the class may have.

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.

Optional Materials: *Managing Your Reputation Worksheet*

Introduction

For the last few weeks we've been talking all about different technologies that we use and the relationships between technology and our privacy. Today we're going to talk about the relationship between privacy and our own reputations.

What Does Reputation Mean?

Have a general discussion with the class about what reputation is and what it means to the students. Use the following questions to prompt discussion:

- What does "reputation" mean?
- Do you care about your reputation? Why or why not? Does the answer change depending on who might be thinking about you?
- Can you think of any examples of good and bad reputation?

Which information we choose to keep private and which information we choose to share has a direct impact on how others will shape their opinions of us.

Audiences

Discuss the concept of audiences. With the class, try to define what an audience is. Emphasize the idea that your reputation might reach multiple audiences.

Use the following video clips to demonstrate that your reputation can carry over to multiple audiences over a long period of time:

- Mark Sanchez's Famous "Butt Fumble:" http://www.nfl.com/videos/nfl-network-total-access/0ap2000000286025/One-year-anniversary-of-the-butt-fumble

- Tony Romo's Botched Snap: http://deadspin.com/5839408/we-could-watch-tony-romo-take-a-snap-to-the-gut-over-and-over-again

- John Travolta Butchering Idina Menzel's Name: http://www.vulture.com/2014/03/watch-john-travolta-flub-idina-menzels-name.html

LESSON 5: Reputation

Use the following questions to discuss the implications of managing your reputation across multiple audiences:

- How often do you take a picture of something exciting, strange, or funny and keep it to yourself?

- What are some of the possible audiences for things you've posted and shared online?

- What makes it so difficult to control who sees this information or keep it secret?

- Who is your audience for the following?
  - Texts
  - Facebook
  - Kik
  - Instagram
  - Email
  - Snapchat

Monitoring Your Reputation

Now that you've discussed the meaning of reputation and audiences, use this time to provide some tips on how students can manage their reputations online. Use the following questions as prompts:

- Have you ever met someone and gone home and Googled them? Why? What were you trying to find? What did you find?

- Have you ever Googled someone whose name you've seen (on Facebook, Twitter, tagged in a friend's photo, mentioned on a blog, etc.), but whom you've never met? Why? What were you trying to find? What did you find?

- How would you feel if someone knew things about you already because they Googled you? Creepy? Flattered? Embarrassed? Is that different than telling someone about a friend before they meet them?

- Who has done a search of their own name? What kind of things might you see?

When students think of their online reputation, they should think of it as a "first impression" that people will get of them in the future. These people might include teachers, college admissions officers, employers, parents, friends, family members, and others.

LESSON 5: Reputation

Managing Bad Results

Discuss what steps one might take to prevent unwanted information from appearing online.

Handling Uncomfortable Content

Tell students that unfortunately, uncomfortable content about them might appear online.

As a class or in small groups, solicit student responses and discuss what you can do when:

- You come to regret something you've written or posted online, either about yourself or someone else
- Someone else comes to you to tell you that there's something you've posted that *they* think is bad or upsetting
- You find something bad that someone else has posted *about you*
- Asking someone to remove the bad material doesn't work

Sexting

Discuss the serious legal and reputational consequences of sexting or sharing inappropriate pictures.

Discussion

Use each of the following hypothetical scenarios to prompt class discussion. Have students apply what they've learned from this lesson in their responses.

- A student applies for job at mall. After applying, the store's social media account sends him a friend request. He loves this store. Should he accept the request?
- A student posts photos of herself at a party on one of her social media accounts. She later applies for a job (or to college) and is turned down because the employer (or college) saw the photo after doing a search for that student's name. Do you think it's OK for someone who is thinking about hiring you (or admitting you to school) to try and find out information about you on the Internet?
- How does thinking about all the potential audiences (present and future) for a post or text affect what you might want to share?

LESSON 5: Reputation

- Is there a downside to going back and deleting something you've written that you now think is inappropriate or bad for your reputation?

- Have your views about which people care about your reputation changed?

Recap

Use any remaining time to recap the major points of the lesson. Open the floor to student questions, if time permits.

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