University 101
UNIVERSITY OF SOUTH CAROLINA Programs

Privacy: Campus Living & Technology

Outcome III.3) Describe and demonstrate principles of responsible citizenship within and beyond the campus community.

Outcome III.4) Describe processes, strategies, and resources, and explain the implications of their decisions, related to their overall wellness.

This chapter includes:

Introduction

The concept of Privacy is woven deeply in the fabric of American values and citizenship, established by the Fourth Amendment to the Constitution:

> *The right of the people to be secure in their persons, houses, papers, and effects,[a] against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

Of course, from 1789-1792, when the Constitution was composed and ratified, there was no concept of technology, no internet. But the concept of persons desiring and expecting aspects of their lives – their bodies, their possessions, and their thoughts – to be kept private from others was seen as a basic human right. With the advent of modern technology, the tools by which privacy can be infringed upon grew exponentially.

At the University of South Carolina, the Carolinian Creed speaks to privacy with three phrases in particular:

> *I will respect the dignity of all persons…*
> *I will respect the rights and property of others…*
> *I will demonstrate concern for others, their feelings, and their need for conditions which support their work and development.*

University 101 offers a prime opportunity for students to develop a better understanding of privacy: why they should value it in their own lives, as well as their roles and responsibilities as a member of a community to affirm and uphold the privacy of others.

PLEASE NOTE:
The lesson plans in this packet blend the concept of privacy with technology; in large part this was initiated and inspired by the selected 2014 First Year Reading Experience book, *The Circle.* In that work, author Dave Eggers places a spotlight on the complex and shocking realities that are the intersection of privacy, social media, and technology in general. However, privacy has many dimensions and considerations that are outside the technology domain. Instructors are encouraged to take an expansive view of privacy and develop a comprehensive approach to the topic.

Defining Privacy
Privacy is a concept that is fairly well understood, but difficult to define. People know what privacy means to them, and when their sense of privacy has been violated – but articulating a succinct definition of privacy that can be applied to the many facets of our humanity, is quite challenging. Below are definitions from a few sources. Perhaps one of the best places to start any lesson on privacy is to work with your students in developing a consensus definition of privacy for your section! This gets students thinking right off, engages them in active dialog and negotiation, and provides a shared foundation from which your students will proceed with whatever lessons and activities follow.

Merriam-Webster (http://www.merriam-webster.com/dictionary/privacy, as of 07/2014)
: the state of being alone : the state of being away from other people
: the state of being away from public attention

Privacy International (https://www.privacyinternational.org/, as of 07/2014)
Privacy is the right to control who knows what about you, and under what conditions. The right to share different things with your family, your friends and your colleagues. The right to know that your personal emails, medical records and bank details are safe and secure. Privacy is essential to human dignity and autonomy in all societies. The right to privacy is a qualified fundamental human right - meaning that if someone wants to take it away from you, they need to have a damn good reason for doing so.

Topics & Methods for Teaching Privacy in UNIV 101

Although privacy is not a required module in UNIV101, it is implicitly related to two Goals and Learning Outcomes:

III.3) Describe and demonstrate principles of responsible citizenship within and beyond the campus community.

III.4) Describe processes, strategies, and resources, and explain the implications of their decisions, related to their overall wellness.

Savvy instructors can leverage a few other goals and learning outcomes in designing solid lessons on privacy; in particular, consider lessons that:

- *Use written and oral communication to discover, develop, and articulate ideas and viewpoints* (Foster Academic Success, I.4)

- *Develop and apply skills that contribute to building positive relationships with peers, staff and faculty* (Help Students Discover and Connect with The University of South Carolina, II.2)

- *Describe what it means to be a Carolinian in context of the history, traditions, and culture of the University* (Help Students Discover and Connect with The University of South Carolina, II.3)

These and other goals and learning outcomes have been purposefully incorporated into the lesson plans and activities that follow.

References

Included where appropriate throughout this document.

Foundational Activities

Activities: Defining Privacy

In this section, the suggested approach is to conduct the in-class activities first, with a follow-up assignment to blog/journal or otherwise reflect on the definition of privacy your section constructs in class.

- In-class activities
  - Working individually, define "Privacy," in both sentence form and a bulleted list of related concepts and principles.

    - Learning Outcomes I.4, III.3

  - After individual definitions are complete. Working in small groups, or as the entire course section, develop a consensus definition of privacy. Adopt this as *the* meaning of privacy for your section in all the activities that follow should facilitate understanding, and empower students to hold each other accountable for their shared use of the term.

    - Learning Outcomes I.4, II.2, III.3

- Assignment / Homework
  - **Individual Blackboard blogs/journals, or multimedia**. Have students respond to the following items in writing. Due to the potential for students to feel pressured by the assignment, students should be encouraged to share the generalities of their experience, and to a share only the level of detail they are comfortable with. The assignment is *not* intended to further undermine the person's sense of privacy.

    - Briefly describe the circumstances of a time when your privacy was violated by someone.
    - What did the loss of privacy feel like to you?
    - Was there any actual damage or risk done to you or your reputation
    - What did the experience do to your sense of trust for the person or organization that infringed on your privacy?

    - Learning Outcomes I.4, III.4

4th Amendment – Basis of Privacy in the U.S.

Background

What is the Fourth Amendment?
"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

- Fourth Amendment, U.S. Constitution

Did you notice something?

It may be obscure, but the word "privacy" appears nowhere in the Constitution, including the 4th Amendment. Yet many scholars and civil liberties groups – of all stripes – hold that the 4th Amendment is the *basis* for the right to privacy. While the focus of this lesson is on the 4th Amendment, be aware that other Amendments (comprising the Bill of Rights) also pertain to privacy:

- 1st Amendment – right to keep beliefs private
- 3rd Amendment – privacy of home, (free from demands to quarter soldiers)
- 4th Amendment – privacy of person and possessions, freedom from unreasonable searches
- 5th Amendment – privacy, as freedom from self-incrimination
- 9th Amendment – broad statement that the fact that certain rights are enumerated in the Bill of Rights does not mean that other (unlisted) rights are not retained by the people

Suggested approaches

- Be sensitive to conservative/liberal differences of opinion regarding constitutional interpretations
- Present a mix of perspectives. Note that the resources below include unaligned as well as organizations that are purportedly left and right; it is up to the instructor to be aware of any potential political agenda or funding bias of organizations whose materials are used for this lesson, including those below.

Additional resources

Preparatory Homework: Have students browse one or more of the following sites prior to class.

University of Missouri – Kansas City, page on Right to Privacy
http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html

New York Times: Search and Seizure news, commentary and archival articles.
http://topics.nytimes.com/top/reference/timestopics/subjects/s/search_and_seizure/index.html

What does the 4th Amendment Mean? [US Courts}
http://www.uscourts.gov/educational-resources/get-involved/constitution-activities/fourth-amendment/fourth-amendment-mean.aspx

Bill of Rights Institute (Additional lesson plans available here; includes the "Background Essay", which is Appendix A of this document)
http://billofrightsinstitute.org/wp-content/uploads/2012/11/Are-They-Watching-You-PDF-Lesson-Teacher-and-Student-Pages.pdf

Activities

For this lesson, it is recommended to assign the reading as preparation for in-class activities.

- Assignment / Homework [Simple]
  - **Read the Background Essay** (found in Appendix A) as a reading assignment before the in-class activities.

    Impress upon students that in addition to reading, they should allow themselves time to digest and *reflect on the essay in advance*, giving special consideration to what privacy is and what it means in their lives both as college students and as adolescents who are transitioning into adulthood.

    - Learning Outcomes I.4, III.3

- Alternative Assignment / Homework #1 [Complex]
  - **Library research.** Have students conduct research, using the library, to construct definitions of the following terms, in contemporary U.S legal jurisprudence:
    - Searches
    - Seizures
    - Reasonable vs. unreasonable
    - Surveillance

- Learning Outcomes I.2, III.3

- Alternative Assignment / Homework #2 [Complex]
  - **Online research.** Have students research the capabilities of smartphones, and how using one can raise privacy concerns and bear legal complications. Have students submit a written one-page paper via Blackboard on their findings. They should consider:
    - How does a smartphone track your activities?
    - What does your smartphone know about you?
    - What does your smartphone report to others about you?
    - How can smartphone tracking have consequences for you if you get in trouble or break the law?

    - Learning Outcomes I.2, I.4, III.3

- In-class activities
  - **Discussion.** The focus of discussion is the "Background Essay." If you had your class previously develop a consensus definition of privacy, incorporate that into the discussion. Suggested open-ended questions for discussion:
    - How does our section's definition of privacy gel with the essay?
    - Could you have privacy if there was no warrant requirement from unreasonable searches and seizures?
    - What are the benefits of consenting to a search of your dorm room without a warrant? What are the cons?
    - Discuss one of the key questions posed in the essay: Has technology changed the meaning of the Fourth Amendment.
      - *Context matters!* Today's traditional entering freshmen do not relate easily to a world that didn't have the Internet and wide-spread technology. The Internet began broad public access in 1990, 6 years before most 2014 freshmen were born. Handheld mobile phones (as opposed to those installed in cars and "bag phones") began spreading widely after 1995. Texting started to blossom between 1995 and 2000. In 2007, when Apple released the first iPhone, these students were about 10 years old.

        So, don't be surprised if their cultural concepts and values surrounding the intersection of privacy and technology is different from your own.

    - Learning Outcomes I.4, II.2, III.1, III.3

- **Video and Factsheet.** Watch the TED Talks video "Your phone company is watching", http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching, which takes about 15 minutes. Also, have students explore the Privacy Rights Clearinghouse Fact Sheet (2b) on "Privacy in the Age of the Smartphone", located at https://www.privacyrights.org/smartphone-cell%20phone-privacy and discuss key aspects of both afterward.
    - What are the common themes between the Background Essay and the TED talk?
    - Is privacy important?
    - Why should you be concerned and/or defend your privacy

    - Learning Outcomes I.4, II.2, III.3

Carolinian Creed – Your Guide to Privacy on Campus

Background

What is the Carolinian Creed?
The Creed is a complement to the University's conduct code. It explains why we regulate and restrict what we do. It forms the basis for and serves as "a summary of what's expected by the institution." The Creed emphasizes integrity, openness and the general principles of civility. By defining the common values of our community the Creed helps create expectations that students should strive to live up to.

Source: http://www.sa.sc.edu/creed/creedhistory/

As a Carolinian…

I will practice personal and academic integrity;

I will respect the dignity of all persons;

I will respect the rights and property of others;

I will discourage bigotry, while striving to learn from differences in people, ideas, and opinions;

I will demonstrate concern for others, their feelings, and their need for conditions which support their work and development.

Did you notice something?

It may be obscure, but just like the Constitution, the word "privacy" appears nowhere in the Carolinian Creed. But you'd be hard-pressed to argue that three lines in particular don't speak emphatically to privacy and related concerns:

- I will respect the dignity of all persons;
- I will respect the rights and property of others;
- I will demonstrate concern for others, their feelings, and their need for conditions which support their work and development.

Suggested approaches

- Be sensitive to the fact that students may not yet be familiar with the Creed or if they are familiar, they may still regard it with apathy or disinterest.
- The President and key leaders of USC Columbia have placed an emphasis on "civility" – consider how that ties into respecting the privacy of others.
- Encourage honest, open discussion – and put the emphasis on "community values" and individual responsibilities.
- Carolinian Creed & Diversity Day is a fall event, usually in early November. Creed Week is held each spring semester. Consider discussing privacy, in the context of the Creed, around these times. For details, visit http://www.sa.sc.edu/creed/creed-programming/
- The Office of Student Conduct and Academic Integrity offers scheduled presentations upon request – outside of the U101 Campus Partner Presentations. For details, visit http://www.sa.sc.edu/creed/request-a-presentation/

Additional resources

Visit the full Creed website at http://www.sa.sc.edu/creed/
Look for sections on

- Creed History
- Resources & Articles
- Creed on Campus

Activities

For this lesson, it is recommended to assign the Carolinian Creed reading as preparation for in-class activities.

- Assignment / Homework [Simple]
  - **Creed Prep.** Have students read the Carolinian Creed, as well as the Creed History and Essay Contest sections – and come to class prepared to discuss.
    - Learning Outcomes II.1, II.3

The following assignment may be best given as *follow-up to class discussion*.

- Assignment / Homework [Complex]
  - **Invasion of Privacy and Bullying on Campus**
    - Step 1. Assign students to read a comprehensive article about Tyler Clementi, a Rutgers University freshman who killed himself in September 2010 after discovering that his roommate had secretly used a webcam to stream Mr. Clementi engaged in a romantic interlude. The article is available in Appendix B.

    - Step 2. In addition, have students listen to the song "Make It Stop (September's Children)" by the band Rise Against, which was written in part as a response to Tyler's suicide, and other similar cases.

    - Step 3. Have students journal/blog about the abuse of privacy in a dorm room, and the unintended consequences. Consider the following in their reflection:
      - What would it be like to have your activities in your dorm room video recorded without your knowledge?
      - What would it be like to have those recordings released publicly?
      - While this is an example of extreme consequences, it is a factual case – and sadly not the only one of its kind. What is it like to consider that violating someone's privacy could lead the person to take their own life? What would you feel afterward if you had been the one to set the chain of events in motion?
      - Can you think of behaviors, including pranks, which have the potential to go too far? Do these often involve compromising someone's privacy?

    - Learning Outcomes I.4, II.2, III.1, III.2, III.4

- In-class activities
  - **Creed Discussion.** Stimulate a dialogue between students about the relationship of the Creed to privacy. As much as possible, use open-ended questions to encourage students to avoid one-word responses. (If you haven't assigned the simple homework – reading and reflecting on the Creed in advance – then budget time at the beginning of this lesson to do so.)
    - Is there a link? How so?
    - Which tenets of the Creed speak most directly to privacy?
    - Describe some behaviors or activities you've observed since arriving at USC that violated someone's privacy.
    - Describe the impact on the person whose privacy was violated.
    - Describe an instance when you were asked in public for more information than you felt comfortable disclosing at the moment. Why did you feel uncomfortable?

    - Learning Outcomes II.1, II.2, II.3

  - **Privacy Barometer.** Clear the area of furniture as much as possible, with central standing area, flanked left and right by free area that students can walk to. On the left side have a large poster on the wall that reads "Agree" and on the right a poster that reads "Disagree." To start, have all students stand in the middle of the floor space.

    As you read each item, students should move toward either the Agree or Disagree side of the room to the extent that they feel strongly about the item. Students may be middle of the road, or lean one direction or the other, and that is perfectly fine. These issues are not black and white, so permit students to put themselves where they truly feel they belong.

    The idea is to stimulate thought, reflection, and reconsideration of one's position. So after each item, ask a few students why they placed themselves in the spot they occupy.

    Emphasize that students are not being asked whether something is or should be legal, but rather where they would evaluate the item from a privacy perspective. Don't expect to cover all of these items.

    Barometer Items

    - Privacy is a privilege in the United States.
    - Privacy should be a right in the United States.
    - I don't mind telling people how much money my parent(s) make.
    - It's okay that my mobile phone provider knows where I am.

- It didn't bother me to share personal information with my University 101 classmates at the beginning of the semester.
- Dorms with hall-style bathrooms don't give you privacy.
- I have a right to know my girlfriend/boyfriend's whereabouts.
- I have a right to know my roommate's sexual orientation.
- I have a right to know whether my roommate smokes cigarettes or not.
- If your roommate smokes pot in the room, you are responsible for *not* letting others know – keep their secret for them.
- Police should be able to stop and question people who are acting suspiciously.
- I don't mind swiping my CarolinaCard to get into special programs like guest lectures, movies, and musical performances.
- Being an open, outgoing person means you're not as private about things as some people.
- My instructors should be able to have students join a Group on Facebook for the course sections.
- My instructors should be able to have their students "Friend" them on Facebook.
- It's okay for instructors to talk in class about how certain students did on a quiz or test.
- My RM should be able to enter my room when I am not there.
- It's okay for my mobile number to be published in the online student directory.
- It's okay for another student to ask me what religion I am.
- It's okay for a staff member to ask me what religion I am.
- It's okay for a faculty member to ask what religion I am.
- It's okay to tell a friend that you think someone you both know is pregnant.
- It's okay to tell your parent(s) about your roommate routinely skipping class for no good reason.
- It's okay to search through a friend's Facebook friend list to find someone you might want to ask out on a date.
- The benefits of security cameras around campus outweigh the cons.
- I feel like this activity "outed" my feelings about certain topics.

- Learning Outcomes I.4, II.2, III.4

Online Privacy

Background

For activities about Online Privacy we will use the term "vendor" as a general label for technology companies and organizations that either make web browsers (Internet Explorer, Firefox, Chrome, Safari, etc.) or search engines (Google, Bing, Yahoo, Ask, etc.).

In many parts of the world vendors are capitalist organizations, often motivated by a desire to produce a good or service they hope people find useful and from which they can derive a profit. So, in exchange for providing you a good or service (like a browser or search engine), they get something in return. That 'something" may be:

- information about you (biographical, demographic, contact information), and/or
- information about what you go looking *for* (search), and/or
- what you look *at* (browsing history), and/or
- transactions you take (e.g. purchases, creating accounts, etc.).

Vendors collect this information by tracking and cataloging data on your activities, through various tools and databases, sometimes working in partnership with other vendors, including companies that you buy products from (Amazon, eBay, Gap, etc.), or services you use (bill payments, banking, etc.).

Then vendors analyze the data to derive patterns about your behavior, combine it with information about the behavior of people who are somehow similar to you, and transform that knowledge into business intelligence (BI). They may use that BI themselves to improve their efforts at marketing to you over time, or they may sell that BI, charging other companies for useful information about you that those companies can then use to help make a sale to you. Either way, the company has gained some value from collecting and analyzing data about you. When a vendor uses your data for their profit, they have "monetized" your data.

Suggested approaches

- Online privacy issues are challenging to address – most people go about their activities without actively considering the consequences of where they browse, even though they are vaguely aware that there are threats out there.

- Doing a lesson about online privacy runs the risk of stoking paranoia, suspicion and distrust. Your intent should be to educate and heighten awareness – state that objective flatly to students.

- Expect that some students may be highly vocal about certain topics, especially if they or someone close to them has had a negative experience.

- Give the above background information to students ahead of the activities. Then talk in general with the students about browsing/surfing online, and the variety of activities people engage in online. Don't shy away from real behaviors and be sure to encourage general responses *without* intricate details or TMI (too much information). These lessons are about privacy – so we don't want to unintentionally encourage too much disclosure from students.

- Understand that some students will be very tech-savvy and know exactly how to answer the technical questions, while others may have strengths in other areas.

- If there are questions students don't know how to answer, it's okay to allow time for them to find out what the question means – this activity is designed to be a true learning experience, so having to research what something means isn't a bad idea. (e.g. the question "What are cookies?" may be a top-of-head simple response for some students, but others may need a few minutes to search the term and make meaning of the results.)

- Intent: the activities are purposefully designed to make students actively consider and reflect upon their online behaviors in the hope they can avoid making poor choices with negative, potentially lifelong consequences. As they emerge through adolescence into adulthood, their behavior will have more and more lasting consequences – both legally and socially. For better or worse, any and all behaviors can be permanently recorded and posted or transmitted online. We want to raise awareness about this, so students can make decisions in their college years that will hopefully avoid fallout later in life.

- The following activities can be done either as in-class discussions or homework, or a combination of the two.

Activities

- <u>In-class discussion -OR- Independent research with written response</u>

  - **What am I doing online?** The items below may be used to facilitate in-class discussions or as written research assignment. Because of the more technical nature of this topic – which may be beyond the skills of some instructors – many of the items are immediately followed by a short list of valid responses in square brackets [e.g.]. But don't be discouraged from this activity if you're less technical – the intent is to facilitate purposeful reflection on the items.

    1. What kinds of data does your web browser collect and report to the vendor when you surf online?

[Geographic location, IP address, Internet Service Provider ("ISP" such as Time Warner Cable, Comcast, USC (on-campus connections) and wireless service providers such as AT&T, T-Mobile, and Verizon), personal info (name, email, etc.), unique identifier of your computer, history of sites you visited before, etc.]

2. Who do you think captures your data and/or tracks your activity online?

   [Website owners, Internet Service Provider, search engine vendor, browser vendor, governments at various levels, persons with malicious intent, etc.]

3. What do vendors do with the information they collect about you?

   [Collect and store it, attempt to match it up with other information about you, analyze it, combine it with data of other people, use it to target you for further activities, sell it to other vendors for a profit, etc.]

4. Why do vendors want this information?

   [To give themselves an advantage in earning your business in the future, improve their site, or otherwise monetize your information]

5. Why would non-vendors want this information?

   [Depends on who the person/entity is. Could be a friend, family member, or other person trying to pry into your business for some reason, or could be a person with malicious intent looking to steal your identity for any number of reasons.]

6. What are cookies?

   [Basic answer: small files of data stored on a user's computer that help deliver tailored web pages based on places the computer has browsed before]

7. Do you like targeted advertising or does it creep you out? Do you understand that cookies are, generally, the "magic" that makes your browser aware of who you are and what you might be interested in seeing?

   [Item is discussion oriented – no right/wrong answer]

8. Can you point to and describe an example of when targeted advertising has gone too far for your comfort?

   [Item is discussion oriented – no right/wrong answer]

9. To some degree, "getting hacked" and having "your data mined by a company" both involve your personal data being used by someone else, quite possibly without your full awareness of how it is being used. So, what's the difference?

   [There is really no end of valid responses to this item – e.g. "a company that mines my data is trying to figure out what I might buy, so they show that to me the next time I'm on their site. I like it because they make me aware of their latest products so I can stay fashionable. Getting hacked means someone stole my identity and might pretend to be me online, or might use my information to get into my bank account or open up a credit card account."]

- Learning Outcomes I.4, III.1, III.4

- **From Class assignment to Watch list?**

  As a college student you will periodically conduct research on topics that are unfamiliar to you but are related to something that you are studying in one of your courses. The upside is that this opens your eyes to new fields of study, career opportunities, techniques and subject matter. But there may be some downsides as well. Some of these topics may be controversial, politically sensitive, or even a bit uncomfortable.

  Consider: depending on who is monitoring your online activities, could researching some topics get you placed on a terrorist watch list? Thought of as a potential active shooter? Could a health insurance company deny you coverage if they knew your browsing history?

  Consider if you were conducting research on topics such as:

  - Personal bankruptcy
  - Genital warts
  - Uses for fertilizers
  - Oversees adoption
  - Alcoholism treatment
  - Pre-surgical hormonal preparation for sex reassignment surgery
  - Methods of suicide bombers

Questions for Reflection

1. What are the potential ramifications when vendors collect and analyze your browsing history?

2. What would be potential consequences if the government was tracking your browsing history?

3. Do you think trackers can distinguish your search reasons from those of a non-student? Do the things you search for online in college become part of your permanent data identity?

4. Does privacy matter in your life as a college student? How so?

- Learning Outcomes I.4, III.3, III.4

- In-class videos – to be followed by facilitated discussion

  - **1. Hot on Your Trail: Privacy, Your Data, and Who Has Access to It. (Short – 5 minutes)** A YouTube video that explains the range of tracking, information gathering, and information exchange that occurs when individuals search, browse, and execute transactions online. Produced by the Center for Investigative Reporting (CIR), The I Files selects and showcases the best investigative videos from around the world. Major contributors include The New York Times, ABC, BBC, Al-Jazeera and the Investigative News Network. The I Files is supported by The John S. and James L. Knight Foundation. http://www.youtube.com/watch?v=bqWuioPHhz0

    - Learning Outcomes I.4, III.1, III.4

  - **2. Terms & Conditions May Apply. (Long – 58 minutes)** Staff of the University Information Security Office will facilitate discussion and screen a documentary film that spotlights the ways in which vendors and websites collect and leverage user data, and look at how people move through websites and social media without regard to the digital footprint they leave behind…. And the consequences that can result.

    To schedule a screening and discussion, please contact Kyle Brown at 803-777-8823 or BROWNKS4@mailbox.sc.edu

    An 80-minute long version of the film is available in streaming format through Netflix, Vimeo, and Amazon. Instructors may wish to view the trailer to get a sense of the film, but the trailer is not recommended for class viewing in lieu of the film; browse to http://tacma.net/

    - Learning Outcomes I.4, III.1, III.4

Workplace and Employment Privacy

Background

Accessed 07/2014 adapted from:
https://www.privacyrights.org/workplace-privacy-and-employee-monitoring

Employers want to be sure their employees are doing a good job, but employees don't want their every sneeze or trip to the water cooler logged. That's the essential conflict of workplace monitoring.

New technologies make it possible for employers to monitor many aspects of their employees' activities: telephones, computers, email, voice mail, and when employees are using the Internet. Such monitoring is virtually unregulated. Therefore, unless company policy or laws specifically state otherwise, employers may listen, watch and read most of your workplace communications.

Various technologies can provide insight into individual employee behavior based on the trail of "digital footprints" created each day in the workplace. This behavioral modeling technology can piece together all of these electronic records to provide behavior patterns that employers may utilize to evaluate employee performance and conduct.

A majority of employers monitor their employees in some manner. They are motivated by concern over litigation and the increasing role that electronic evidence plays in lawsuits and government agency investigations. And they also want to maximize worker productivity, by encouraging employees to stay focused on work-related activities.

Activities in which employers might engage include, but are not limited to:

- Monitoring employees' web site visits in order to prevent inappropriate surfing
- Using software to block connections to web sites deemed off limits for employees (Employers are concerned about employees visiting adult sites with sexual content, as well as games, social networking, entertainment, shopping and auctions, sports, and external blogs.)
- Monitoring e-mail, both internal and external.
- Monitoring phone calls – frequency, contacts dialed/received, listening into conversations and voicemail content
- Tracking content, keystrokes, and time spent at the keyboard.
- Tracking text messaging for content sent or received on an employer-provided phone
- Opening and inspecting postal mail.
- Monitoring blogs to see what is being written about the company.

- Monitoring social networking and media sites, especially posts by employees.
- Using video monitoring to counter theft, violence, sabotage, and performance.
- Firing workers for misuse of technology.

Suggested approaches

- Be aware that while many traditional university freshmen have given thought to their future career field, it's unlikely they've considered deeper issues of the relationship between an employee and an employer, beyond how much they will get paid, benefits, and leave time.

- There is a ton of legal background involved in workplace privacy, way too much to go into with UNIV101 lessons unless you decide to have students do an extensive research project. Don't be discouraged from doing activities that involve legal principles! Rather, have students focus and reflect on how they would feel and react in certain scenarios, and point out that the law may speak clearly in some cases as to who's in the right and who's in the wrong. Keep in mind that laws may change, and what is considered "constitutional", especially around the topic of privacy, is subject to change – especially in response to emerging technology.

- Even if they haven't realized it, many students who have held after-school jobs through high school have already been subjected to some form of workplace monitoring. Point this out and have them think about it. Examples:

    - Having to disclose personal information on an employment application
    - Choosing to Friend their employer or supervisor on Facebook (think: did this ever limit their ability to post something, or limit when they called in "sick" to work?)
    - Having coworkers who wanted to know more about them than they wanted to disclose
    - Whether they worked at a fast food restaurant, a neighborhood lawn mowing job, or retailer in a mall, chances are they've been monitored and recorded on video at work

Additional resources

- Privacy Rights Clearinghouse, Workplace Privacy and Employee Monitoring
  https://www.privacyrights.org/workplace-privacy-and-employee-monitoring

- Privacy Rights Clearinghouse, Background Checks & Workplace
  https://www.privacyrights.org/Background-Checks-and-Workplace

- American Civil Liberties Union (ACLU), Workplace Privacy
  https://www.aclu.org/technology-and-liberty/workplace-privacy

- Electronic Privacy Information Center (EPIC), Workplace Privacy
  http://epic.org/privacy/workplace/

Activities

The activities for workplace and employee privacy are designed to be done in sequence: assigned reading outside of class first, followed by the in-class activity.

- Homework/Preparatory activities
  - **Online reading.** In preparation for the in-class activity, students should be required to read the following sections of NOLO Law for All, self-described as "one of the web's largest libraries of consumer-friendly legal information." The articles and FAQs listed below should be very accessible and cogent to the average traditional college freshman. Students should budget 60-90 minutes for the reading.
    - Workplace Electronic Monitoring, addressing email, texting, blogging and social media, phone calls, voicemail and secret recordings.
      - http://www.nolo.com/legal-encyclopedia/electronic-monitoring
    - Workplace Privacy FAQ, addressing searches, cameras, and access to one's personnel file.
      - http://www.nolo.com/legal-encyclopedia/right-privacy-work-faq-29112.html
    - Off-Duty Conduct and Employee Rights, addressing privacy of off-hours behavior, drug testing, political and religious activities, marital status, and illegal activities.
      - http://www.nolo.com/legal-encyclopedia/off-duty-conduct-employee-rights-33590.html

  - Learning Outcomes I.2, I.4, III.3

- In-Class activity
  - **What Would You Do?** Print each of the following scenarios and pass one out to each student in the class. Give them directions, and five minutes to consider their response, and then go around the room and have each student report their scenario, and how they would handle the situation. Depending on how talkative students are, and how much discussion ensues, you may not get through more than half of the scenarios in class. You can always give a follow-up reflection assignment to ensure each student actively reflects on the activity.

  - Learning Outcomes I.4, III.1, III.3, III.4

    Directions: each of you will be given one scenario related to the topic of workplace and employee privacy. Based on your understanding of privacy rights, laws, and common practices – as well as your personal values – consider how you would respond if you found yourself in the situation described. Take 5-10 minutes to consider your scenario and how you would respond. We'll then go around the room asking you to articulate your scenario and what you would do. Consider:

    - Does the scenario pose issues of legality, ethics, or morals?
    - Would your privacy potentially be compromised, and if so, in what ways?
    - What would your employer and coworkers have access to about you?
    - What would be the possible consequences of your response?
    - Could the scenario – or your response - limit your perceived freedoms in the future, and if so, how?

    1. After applying for your first job out of USC, the Human Resources department at the company where you applied calls to schedule you for an interview. During the call they tell you that if you pass the first round of interviews, you will be asked for your usernames and passwords for Facebook, Twitter, Instagram, and any other social media sites to which you subscribe. This is a precondition for the interview.

    2. Three weeks after starting a new job, your manager tells you she's noticed that you haven't yet Friended the company's official Facebook account, and that you need to in the next couple days.

3. You've been working at a multinational company with 11,500 employees for 4 years, when senior management decides the company will launch a Twitter account and an active feed. All employees are asked to make sure they too have a Twitter account and follow the company; in turn, the company will follow them.

4. You've just secured a marketing internship at a trucking and logistics company for the spring semester of your final year. That's great, because your major requires you to complete an internship in order to graduate! While filling out the hiring paperwork, you are presented a consent form for a criminal background check, which indicates a clean record is required for all employees. (Rationale: the company's truck drivers must have no criminal records in order to drive and make deliveries to customer sites, so all employees are held to the same standard.) You are concerned because you have an assault and battery conviction, stemming from a fight in Five Points you got into one Thursday night in your sophomore year. You also have a charge for simple possession of marijuana.

5. You are mowing lawns around town for the summer to make money for school. Midway through the summer you notice that one of your customers has a residential alarm system installed, which includes outdoor monitoring cameras that are motion tracking. As you mow, you notice the camera is following your every move.

6. It's your first day of work at a technology firm that is known for innovative and groundbreaking designs. Today is new employee orientation. After completing paperwork and getting the basic info about benefits, parking, work hours, and leave policy, it's time to have your employee ID card made. In the process you discover that a retinal scan (eyeball) is required for access to all facilities, and your eye will be scanned today to establish your identity.

7. You've been working at the company for 7 years, and love your job. You and your colleagues spend most of your day on computer work stations dealing with email and management programs. One afternoon, a coworker comes back to your area, saying he has been fired for shopping online during the workday. Neither of you knew it before now, but in his termination meeting, he was told that the company routinely tracks all web activity of its employees and had flagged some of his activity as being not work related. The company doesn't disclose this practice to employees.

8. You work as a loan manager for a nation-wide bank at a local bricks-and-mortar location. You're a solid employee, generally keeping your personal life out of your work day. On Tuesday afternoon your boss calls you to her office, and says the bank has flagged your work phone line as having been used for personal calls. A monitoring system that logs the frequency of in-bound calls from the same number detected that you receive daily calls from the same number; the number belongs to your elderly and frail grandmother. After flagging your number, the IT department retrieved some of your voicemails from that number and forwarded them to Human Resources. You are written up for misuse of the bank's communications systems.

9. It's a routine Monday morning when your boss walks into your office and sits down. He has a grim look on his face as he tells you he's concerned about a Facebook post – with pictures and a 24 second video clip – that you were tagged in over the weekend by one of your friends. You were at a pool party, and things were a little wild – scant clothing, heavy drinking, and some yelling that included profanity. Your boss tells you the posting reflects poorly on the company, because you list your employer in the About section. You and he became Facebook friends by your own choice a couple years ago.

10. You recently did some shopping on Amazon.com and had the delivery sent to your office instead of home, because you've had a couple packages stolen off your porch recently. The company's mailroom delivery person brings the daily work mail, including your package. You are surprised to find it's been opened, and you ask about it. The mailroom manager calls you a little later and tells you that while company policy allows you to have personal deliveries sent to the office, the policy also allows the mailroom to open any in-bound packages. This package contained a racy romance novels, some fashion underwear, and blood testing strips for your diabetic monitor.

11. You manage a team of fifty staff members for an insurance company. One of your employees, Joan, just came to you, complaining that she'd just found out that one of her colleagues – Teresa, another of your employees – had taken a photo of her the previous day, without her knowledge or permission. To make matters worse, Teresa posted the picture on Instagram, with a caption mocking Joan as her "worst dressed colleague." Your company has no policy on the use of personal digital devices in the workplace.

12. You manage a team of twelve marketing account representatives who work all over town soliciting radio ads for your station. Due to the nature of their work, your reps each are issued a company smartphone, so they can communicate with the station and customers rapidly. Tony, who owns a local furniture store, has had Andres as her account rep for seven years. Tony called you this morning, irate because at 12:16 a.m. (last night) he had received a "sexually explicit photo," via text from Andres's work-issued mobile phone. Tony believes he was not the intended recipient, but you summoned him to your office and asked him to hand over his phone for inspection because it is station property and his actions reflect on the station. After he hesitantly handed it over, you scrolled through the texts and discovered he and two other account reps routinely exchanged naked photographs of themselves and others.

13. It's Monday. Without any warning whatsoever, the Human Resources direct fired you this morning from an investment broker job you have held for 8 and a half years. You were stunned. You've always been a top performer, routinely yielding your clients and your firm earnings well above market performance, and receiving commendations from your manager based on client praise for your service. In your termination meeting, the Director offered no explanation. At 6:17 p.m. you learn from one of your friends at the firm that over the weekend, another colleague had discovered a YouTube video in which you briefly appeared, along with several hundred other customers in the crowd. It was taken last Friday night at a local mostly-gay nightclub. Nothing other than dancing occurred in the video. You did not post the video, and did not knowingly appear in it. You don't even know the person who posted the video.

14. You supervise 17 front-line sales associates at the local store for a big-name, internationally known fashion clothing store. Your regional manager just called to tell you that there's a problem with one of you employees, Leroy, and he should be fired. The corporate office has a crawler program that searches social media for postings about the company, to protect the brand name. The crawler located an Instagram posting from last Tuesday, in which Leroy posted a picture of a clothing item currently selling in stores with the caption, "$73? Really? I won't pay $7.30 for the crap we sell." The brand label was clearly visible in the picture, and the corporate IT department was able to track the user account to your employee. Leroy has a "public" account, allowing anyone using Instagram to view his content.

15. You're at your second interview for your first real job out of college – you advanced from the first round which had about 12 candidates, and you are now one of three finalists for the position. You graduated five months ago, and while this isn't your dream job, the position suits your interests and abilities, the salary sounds reasonable and the benefits are solid; it's a Fortune 1000 company. During the interview the hiring manager tells you that, if hired, you must accept a document called "technology terms of employment." She summarizes it for you: your email, phone calls, voicemail, and documents are all subject to constant monitoring. The company also does "keystroke logging" randomly of a few employees at a time – and you will never know when it's your keyboarding that's being recorded and analyzed. Personal smartphone use is allowed, for up to 15 minutes twice each day, plus a full hour lunch break. She explains these measures are implemented to assure employees do not abuse workplace technology or stray off task during the work day.

16. You've been working at a hospital as a nurse for three years, love your occupation, and like most of your colleagues you occasionally post on Facebook about really awful days (and patients), and the really good ones, too. You never use names or disclose much detail. One day your shift supervisor hands out an announcement to everyone advising that the hospital is adopting a new policy on use of social media. The policy permits employee termination in cases where their use of social media, whether for work or personal purposes, could incite violence, disclose confidential patient information, release protected data, or say anything contrary to the best interests of the hospital.

17. You just graduated with a degree in secondary school teaching with a concentration in history. Teaching jobs are scarce (especially in subjects like history), and you'd like to return to your home city of Cincinnati, Ohio. You've just been scheduled for an interview with a Catholic school – which you think is awesome because you're Catholic, and somewhat involved in the church, attending services at least a couple times a month. In talking with a group of your closest friends about your upcoming interview, one of them asks if you've lost your mind, or if you've just not heard of the teaching contract. She shows you on her iPhone that teacher contracts in the Catholic schools now refer to teachers as "ministers," and the contract forbids them from living together with another person or having sex outside of marriage, using in-vitro fertilization, leading a gay lifestyle, or publicly supporting any of those things. The friend discloses that she was conceived through in-vitro, and your lesbian friend gives you the stink-eye.

18. You are in the break room at work for lunch one day, sitting with some colleagues. Two of them are friends, but the other three aren't your kind of people and one of them – Kat, who also happens to be your team leader – is known for spreading gossip (sometimes viciously). She's fiddling around on her smartphone, and next thing she blurts out is "why are you friends with these two but not me?" And with that she sends you a friend request. Up til now, you've had a personal policy of only friending your actual friends, in part because you don't want people you don't know very well able to see everything you post or your friends post about you.

19. Walking back into your office from lunch, you find your manager inside your semi-private cubicle, looking through your file drawers. She received a call from one of your customers while you were eating, and didn't want to disturb you because she thought she could find the invoice in question pretty easily. In the course of going through your drawer, you know she must have observed a flask of gin that you keep hidden away.

Privacy and the Internet of Things

Background

Often abbreviated "IOT" or "IoT", Internet of Things is the concept where objects that are uniquely identifiable by an "address" are virtually represented in an internet-like structure, or in reality are present and connected on the Internet. A related concept is the Internet of Everything (IoE).

When IOT was first conceived, tech professionals assumed that some form of radio frequency identification (RFID) would be built into or tagged on items, objects, and people, so that they could be inventoried and monitored. You may have heard of big box stores (like Target, Wal-Mart, BestBuy, etc.) that place an RFI inside each item's packaging, so they can electronically monitor inventory inside huge warehouses.

More recently identifying items has expand into several forms of what's called "machine-readable tracking": near-field communications (such as Bluetooth or Wi-Fi), bar codes (which have been around for a long time), QR codes (the square blocks that looks very digitized and are usually printed in black and white), and a form of low-power radio devises (known as "chirp networks").

What kinds of objects are we talking about, already or potentially in the future?

- Security system components
- Cars, motorcycles, trucks
- iPads and other tablets
- Computers
- Wireless headphones
- Clothing
- Coffee makers
- Smart watches
- Scale for measuring body weight
- Bikes
- Bike locks
- Lamps
- Pacemaker
- GPS locator

- Game stations
- Video cameras
- Thermostats
- Water heater
- Vending machines
- Biometrics reader
- Mind tracker
- Fitbit and FuelBand
- Alarm clock
- Dishwasher
- Sprinkler
- Milk cartons
- Orange juice containers
- Indoor air purifiers
- Jewelry
- Soccer balls and other sports equipment
- Outdoor weather monitors
- Apple TV or other Smart TV device
- Integrated Bluetooth lightbulb/speaker for lighting-enhanced music
- Key finder (when you loose your house and car keys)

Applications of the Internet of Things include:

- Milk cartons containing sensors that send signals to the homeowner or grocery store when they are nearly empty. A refrigerator may even have a smart sensor that reads the full/empty status of all the packages grocery items contained inside the fridge. Imagine being able to walk into the grocery store and use a smartphone app to talk to your fridge and discover in real-time whether you need to buy more sour cream, orange juice, sports drink, or string cheese!

- Computer chip under the skin that provides real-time vital signs to self-trackers and medical providers, including some pacemakers that can now self-report to medical professionals.

- Remote control smartphone, tablet, and web apps that allow users' phones to monitor and control household activities, from pre-heating the oven, to arming your burglar alarm, to starting your clothes washer.

- Smart cities, where sensors and GPS tracking facilitate smoother flows of traffic by detecting surges in vehicle traffic and adjusting traffic light timing accordingly.

- Sensors on infrastructure – like bridges, tunnels, elevators, escalators, and subway cars – that give regular readings on wear and tear and provide alerts when repairs are needed.

- Smart appliances, working with smart electric grids, which run themselves or perform their chores after peak electric demand subsides.

- A smart cup that can detect what you are drinking, how fast you consume it, how many calories you consumed, how much protein you've received, and how hydrated you are – and can report out to your fitness/activity tracker

- Garden sensor that can trigger a sprinkler system to come on based on rainfall, temperature, and other weather factors

- Smart jewelry that can alert you with different color lights or light patterns when you receive a text message, email, or have been tagged in a social media posting

Sources

- http://www.livescience.com/45579-experts-predict-the-future-of-the-internet-of-things-infographic.html

- http://iotlist.co/

Suggested approaches

- Relax. There's a lot of technical stuff here, and it may seem over your head even if you are technically inclined! The idea is to get students thinking about the connectedness of devices and services, and what that means for their lives.

- Emphasize the key point: each of the devices described and discussed in this lesson is not only delivering a service or other benefit, it is also producing data and recording it – most likely recording it somewhere forever. That data may say a whole lot about the person who's using the device: their detailed whereabouts, their activities, who they are in proximity to, their health and safety, etc.

- Don't stoke paranoia. The point is getting students to think about unintended consequences.

- Consider: if the device user were the only one with access to the data their devices produce, perhaps this is no big deal. But the point is that the generated data is transmitted through the Internet and/or radio waves, and goes somewhere. That could be a trusted company, or it could be intercepted, analyzed, used or sold for some advantage – perhaps by someone with nefarious intentions. For instance, what happens if your in-home monitoring camera gets hacked, and someone halfway across the world can watch you and your family move around inside your home?

Activities

- In-Class activity
  - **Cool or Creepy.** This activity works just like the familiar "social barometer" activity, except the labeled sides of the room are "Cool" and "Creepy." You can either run through the list of devices above, or you can pull up the website http://iotlist.co/ in real time, and scroll through the list (which is continuously updated with new and emerging devices). As you stop on each device, have students move to one side of the room or the other, depending on whether they think the device is "more Cool than Creepy" or "more Creepy than cool." Students who are torn can stand in the middle.

    Instigate discussion among students by asking thought provoking questions after each item:

    - What makes you feel it's Cool or Creepy?
    - What privacy implications does this device have?
    - How can you see this being used other than what was intended by the manufacturer?
    - What happens to your privacy if the data gets stolen?
    - Do you trust the manufacturer with your data?
    - What happens if the data never goes away?

  - Learning Outcomes I.4, III.1, III.3, III.4

Appendix A: Background Essay

How Have the Protections of the Fourth Amendment Been Interpreted, Applied, and Enforced?

Source: The Bill of Rights Institute
Accessed 07/2014
Excerpted from materials located at http://billofrightsinstitute.org/wp-content/uploads/2012/11/Are-They-Watching-You-PDF-Lesson-Teacher-and-Student-Pages.pdf

The Founders knew that some of the most vulnerable people in our society are those suspected of crimes. Suspected criminals tend to be disliked, and almost all lack the vast resources of government. The Fourth Amendment was added to the Constitution to protect the rights of accused persons -------- and all citizens -------- from abuse by government.

Due process protections are evident in the Fourth, Fifth, Sixth, Seventh, and Eighth Amendments to the Constitution. The principle of due process means that, in going about the business of enforcing laws, government must follow established rules and procedures that respect all citizens' rights. (In other words, it is not enough for the laws to be followed. The principle of due process requires that laws themselves are constitutional.) The Fourth Amendment's warrant requirement provides for one of the most important individual protections: freedom from unreasonable searches and seizures. If the police want to search someone, they must first get a warrant by convincing a court that there is probable cause to believe that an individual has committed a crime. If the court agrees, they will give the police the okay to act.

When is a Warrant Required?

Warrant requirements are not always clear----cut. In general, a search of someone's home requires a warrant, stating the person and place to be searched, and the items to be searched for. The Supreme Court has ruled, however, that many types of searches can be considered "reasonable" even if conducted without a warrant. If a police officer is in a place where he is allowed to be and sees an illegal item in plain sight, the item may be seized without a warrant. Police may also conduct a warrantless search if they believe there is an immediate danger to his life or the life and property of others. In these "exigent circumstances," a search is considered reasonable, so long as there is no intent by the officer to either arrest or seize evidence. Cars, the Supreme Court has ruled, can be searched without a warrant, provided the officer legally stopped the vehicle in the first place and has reasonable

suspicion that a crime may have been committed. Finally, no warrant is required if an individual voluntary allows a search request.

What is the Exclusionary Rule?

All searches are subject to the Exclusionary Rule, which holds that evidence obtained through unconstitutional means may not be used against defendants at trial. The Court first interpreted the Fourth Amendment this way for federal trials in 1914, and applied it to the states in the 1961 case of *Mapp v. Ohio*. Police must be certain their warrant is correct and complete, as the Court ruled in *Groh v. Ramirez* (2004) that an incorrectly written search warrant could also lead to evidence being excluded from trial.

The Exclusionary Rule can be controversial. The text of the Fourth Amendment does not require it, and critics argue there are others ways to discourage police from conducting illegal searches that do not threaten public safety by setting guilty people free. Other critics claim the rule does not actually stop officers from conducting illegal searches because they face no personal punishment. Supporters tend to agree with the Court that allowing the government to punish people using evidence it obtained in violation of the law would be unjust and violate the principle of due process.

Like the warrant requirement of the Fourth Amendment, however, the Exclusionary Rule is not absolute, according to the Court. If the police can prove the evidence would surely have been found through legal means, it may be presented in court. This is called "inevitable discovery."

Has Technology Changed the Meaning of the Fourth Amendment?

Technological advances, surveillance technology, and the use of military----grade equipment by police have dramatically enhanced the government's power to search. In many cases, these developments have forced citizens and the Court to wrestle with finding the constitutional balance of liberty and security.

In 1965, Charles Kar was suspected by the FBI of being involved in illegal interstate gambling. He would often use a pay----phone near his apartment to place his bets, so police attached a listening device to the outside of the phone booth to record his conversations. He was arrested and later convicted. He challenged the search on the basis that his conversation, though in a public location, was private and protected

by the Fourth Amendment. The Supreme Court agreed in *Katz v. United States* (1967), reasoning that the Fourth Amendment protected "people, not places," and that Kar had a "reasonable expectation of privacy" that was protected from an unreasonable government search.

The case of *Kyllo v. United States* (2001) also concerned issues of technology and privacy. Police believed Danny Kyllo was growing marijuana in his home. They used a heat---sensing device to look for the telltale signs of heat lamps that are commonly used to grow the illegal plants. The Court found that the police actions were an illegal search, as the government "use[d] a device…to explore the details of the home…[which is] unreasonable without a warrant."

The widespread use of GPS devices has prompted constitutional questions about privacy and the Fourth Amendment. Antoine Jones was suspected of possessing and dealing drugs. In 2005, police attached a GPS----tracking device to his car without a warrant. They traced his movements for nearly a month. In mapping his whereabouts, along with other evidence, police were able to tie Jones to locations where drug transactions were known to occur. In *United States v. Jones* (2012), the Supreme Court unanimously agreed that the warrantless GPS tracking was an unreasonable search. The Court further argued that while Jones drove on public streets, he did so with a "reasonable expectation" of privacy. This ruling may prove an important precedent in future cases, as many Americans now carry GPS---
-enabled cell phones as they go about their daily lives.

How Does the Fourth Amendment Apply in Public School?

Public schools have long been considered by the Supreme Court as a special place. The Fourth Amendment does protect you in school, but at a much lower threshold than would be the case for adults in the "real world."

Tracy was a high school student in New Jersey, and exited the girl's bathroom smelling like smoke. A teacher took Tracy to the principal's office, where an Assistant Vice Principal searched her purse, finding not only cigarettes, but rolling papers, a pipe, and other evidence of marijuana use. In *New Jersey v. T.L.O.* (1985), the Supreme Court upheld the constitutionality of the search, adopting a lower standard than is applied to police in criminal situations. The court held that school officials only needed "reasonable suspicion" to search students.

While the Court found this lower standard met in T.L.O., it found in 2009 that Arizona school officials went too far in strip----.--------searching a 13 year old student who they thought might be distributing ibuprofen (Advil). In *Safford Unified School District v. Reading* (2009), the Court ruled that while schools have search authority to root out contraband, the search cannot be "excessively intrusive," in light of the age and sex of the student, and the nature of the items being searched for.

Drug tests can also be a kind of "search," and the Supreme Court has weighed in on the use of them by public schools. In the 1995 case of *Vernonia School District v. Acton*, the Court ruled that schools may force athletes to submit to random drug tests. In *Board of Education of Pottawatomie County v. Earls* (2002), students fought a school rule that required drug testing for all extra----curricular activities, not just sports. The drug test was even a condition to take courses such as band or choir. The Court upheld the policy because it "reasonably serve[d] the School District's important interest in preventing drug use among students." The principle of due process, like other constitutional principles, is a means to an end. In other words, as the Constitution's Preamble states, it is a way to ensure our government establishes justice and secures the blessings of liberty for future generations. While technologies and threats to security change, the inalienable rights protected by the Constitution belong to us by nature. This means it will always be important to understand the protections in our Bill of Rights, and the reasons for them.

Appendix B: Invasion of Privacy & Bullying on Campus

The New York Times

The following article is a Times Topics piece on the subject of Tyler Clementi, subject to periodic updates. The content below was captured in July 2014 from
http://topics.nytimes.com/top/reference/timestopics/people/c/tyler_clementi/index.html

Tyler Clementi

Clementi Family, via Associated Press

Updated: March 16, 2012

Tyler Clementi was an 18-year-old Rutgers University freshman who killed himself in September 2010 after discovering that his roommate had secretly used a webcam to stream Mr. Clementi's romantic interlude with another man over the Internet.

The suicide of Mr. Clementi, who jumped off the George Washington Bridge, focused national attention on the victimization of gay, lesbian, bisexual and transgender youth. Public figures including Ellen DeGeneres and President Obama spoke out about the tragedy, and New Jersey legislators enacted the nation's toughest law against bullying and harassment in January 2011. Rutgers also responded in several ways, among them a plan to introduce gender-neutral housing — co-ed dorm rooms for gay, lesbian and transgender students who request it — and training staff in suicide awareness.

In late February 2012, Dharun Ravi, 20, his roommate, went on trial at Middlesex Superior Court, charged with 15 counts, including bias intimidation — a hate crime that was based on the victim's sexual orientation — and invasion of privacy. He was not charged in Mr. Clementi's death.

On March 16, Mr. Ravi was found guilty on all counts, including tampering with evidence and a witness and hindering apprehension. The jury found that he did not intend to intimidate Mr. Clementi the first night he turned on the webcam to watch. But the jury concluded that Mr. Clementi had reason to believe he had been targeted because he was gay, and in one charge, the jury found that Mr. Ravi had known Mr. Clementi would feel intimidated by his actions.

Mr. Ravi could get years in prison — and could be deported to his native India, even though he has lived legally in the United States since he was a little boy — for his part in an act that cast a spotlight on teen suicide and anti-gay bullying and illustrated the Internet's potential for tormenting others.

Prosecutors said Mr. Ravi, motivated by antigay sentiment, intentionally set out to embarrass Mr. Clementi.

Mr. Ravi's lawyers portrayed him as a young man who may have acted foolishly, but was not homophobic and did not intend to hurt his roommate. They said he was suspicious of Mr. Clementi's boyfriend and was worried that the man might steal his computer, so he set up his webcam to keep an eye on his belongings. His lawyers said that he was "a kid" with little experience of homosexuality who had stumbled into a situation that scared him. Mr. Ravi, they argued, was being sarcastic when he had sent messages daring friends to connect to his webcam, or declaring that he was having a "viewing party."

But prosecutors argued that his frequent messages mentioning Mr. Clementi's sexuality proved that Mr. Ravi was upset about having a gay roommate from the minute he discovered it through a computer search several weeks before they arrived at Rutgers in fall 2010.

The star witness in the case was "M.B.," the young man whose date with Mr. Clementi was captured by Mr. Ravi's webcam. The full name of M.B., who appeared to be in his late 20s or early 30s, was withheld to protect his privacy.

M.B. testified that as he and his new boyfriend lay naked on Mr. Clementi's bed, he sensed he was being spied on. "I just happened to glance over," the man said. "It just caught my eye that there was, you know, a camera lens looking directly at me."

As he left the room that night, he testified, a group of students were standing nearby, joking and looking at him in a way that unsettled him. He wanted to see his new boyfriend again — they had been exchanging e-mails for weeks now, but had had only three dates, and were texting furiously in the hopes of setting up another one. But he was not sure he would return to the dorm. "I felt a little uneasy about it," he said.

Ravi Posted Twitter Feeds and Texts

An investigator testified that as Mr. Ravi posted Twitter feeds about using a webcam to see Mr. Clementi in a sexual encounter with another man, one of those reading intently was Mr. Clementi. In the two days before he jumped to his death from the George Washington Bridge, Mr. Clementi checked Mr. Ravi's Twitter account 38 times, said the investigator, Detective Gary Charydczak of the Middlesex County Prosecutor's Office.

Detective Charydczak said that in the early hours of Sept. 21, Mr. Clementi saved a screenshot of a Twitter post that Mr. Ravi had sent two days earlier; it read: "Roommate asked for the room until midnight. I went into molly's room and turned on my webcam. I saw him making out with a dude. Yay."

That night, Mr. Clementi saved a screen shot of another Twitter post from Mr. Ravi, which read: "I dare you to chat me between the hours of 9:30 and midnight. Yes, it's happening again."

Detective Charydczak testified that Mr. Ravi's hard drive showed that he later edited that post to read, "Don't you dare chat me." After Mr. Clementi died, Mr. Ravi added a Twitter post in response to the one he had sent on Sept. 19. The new post read: "Everyone ignore that last tweet. Stupid drafts."

Michelle Huang, who had known Mr. Ravi in high school and was also a student at Rutgers, testified that he had sent her a text message about "keep the gays away" and urged her to watch a feed from a webcam that he had trained on the bed where he expected Mr. Clementi to have a tryst with another man.

Earlier in the trial, a Rutgers employee testified that Mr. Clementi had submitted a request online to be transferred to a single room. On the form, which was sent electronically around 4 a.m. on Sept. 21, 2010, Mr. Clementi wrote that he wanted to move because "roommate used webcam to spy on me." However, Judge Glenn Berman did not allow that statement into evidence, ruling that it was hearsay.

Other Rutgers Students Testify During the Trial

Molly Wei, a friend of Mr. Ravi who joined him in spying on Mr. Clementi, was originally charged in the case. Her charges were dropped in exchange for testifying for the prosecution, performing 300 hours of community service and attending counseling for cyberbullying.

During the trial, Ms. Wei said that three days before Mr. Clementi leapt to his death, she twice watched him on her laptop computer kissing another man inside the dorm room that he shared with Mr. Ravi.

Ms. Wei said Mr. Ravi was concerned that his iPad might be stolen from the room because Mr. Clementi had asked him to leave for a few hours while he was alone with a man, whom Ms. Wei recalled Mr. Ravi describing as "an older, shabbier-looking guy." From Ms. Wei's room across the hall, they turned on Mr. Ravi's webcam and for a few seconds saw Mr. Clementi kissing the other man before they turned off the camera.

Ms. Wei, who had known Mr. Ravi since middle school, testified that she had never before seen two men kissing. She said that despite being "freaked out" over viewing "something we shouldn't have seen," she later turned Mr. Ravi's webcam back on to show the scene to her roommate and three female friends.

Ms. Wei testified that Mr. Ravi had told her that he suspected his roommate was gay.

Lokesh Ojha, another student, testified that Mr. Ravi pulled him away from a game of foosball in a dormitory lounge on the university's Piscataway campus on Sept. 21 and told him that his webcam had captured Mr. Clementi kissing a man.

The two then went to Mr. Ojha's room, he said, where Mr. Ravi, knowing that Mr. Clementi had invited his date over again that night, set up the iChat function on Mr. Ojha's laptop to test that the webcam was directed at Mr. Clementi's bed.

Mr. Ojha said that Mr. Ravi encouraged him to send text messages to other friends to alert them to watch his Twitter feed, where he told them to turn on their computers to watch the webcam feed.

Background

Mr. Ravi was initially charged with invasion of privacy. The grand jury also charged him with a cover-up. The Middlesex County prosecutor's office said he had deleted a Twitter post that alerted others to watch a second sexual encounter that Mr. Clementi planned and replaced it with a post "intended to mislead the investigation." Prosecutors said Mr. Ravi had also tried to persuade witnesses not to testify.

Mr. Ravi was charged with additional counts of attempted invasion of privacy for trying to carry out a second live transmission. The authorities said he tried to use the camera a second time and boasted on Twitter that he had seen his roommate “making out with a dude.” That attempt was thwarted after Mr. Clementi found the camera aimed at his bed.

After discovering that his roommate had spied on him, authorities said, Mr. Clementi jumped from the George Washington Bridge on Sept. 22, 2010.

Anonymous postings that appear to have come from Mr. Clementi, identified after his death in the forums of a gay chat site, show a student wrestling with his rising indignation over a breach of privacy and trying to figure out how best to respond.

Classmates say Mr. Clementi, an aspiring violinist from Ridgewood, N.J., mostly kept to himself. Danielle Birnbohm, a freshman who lived across the hall from him in Davidson Hall, said that when a counselor asked how many students had known Mr. Clementi, only 3 students out of 50 raised their hands.

The Star-Ledger of Newark reported that Mr. Clementi posted a note on his Facebook page the day of his death: “Jumping off the gw bridge sorry.” Friends and strangers turned the page into a memorial.

Notes and Credits

The information and lessons that comprise this packet were researched and compiled in summer 2014 by staff in the Division of Information Technology at the University of South Carolina. The content is designed to serve as a general resource for instructors in USC's University 101 (UNIV 101) course, and to supplement pedagogical discussions of the 2014 First Year Reading Experience book, *The Circle*, by Dave Eggers, © 2013.

Background and Research

Andrew Grimball, MLIS
Project Coordinator
grimbala@mailbox.sc.edu
803-777-8088

Author

Mike Kelly, Ph.D., PMP
Chief Data Officer
kellymc2@mailbox.sc.edu
803-777-5230