Sample Lesson in Computing Ethics: Privacy Principles and Regulations

This lesson is the second of a three-session unit on privacy and information technology. The first session introduced some general considerations in the philosophy of privacy, and how different ethical theories (namely, utilitarianism and deontology) can be used in arguments defending or denying that we all have a moral right to privacy. This lesson introduces further details from privacy regulations in the USA, Canada, and the EU, then asks students to apply these concepts to a specific case in information technology ethics. The lesson is broken into three parts: [1] Lecture (20 min), [2] Small Group Discussion (40 min), [3] Class Discussion (20 min).

Pre-Reading

- Deborah G. Johnson & Keith W. Miller, 2009, *Computer Ethics* (4th ed.), Ch. 4: Information Flow, Privacy, and Surveillance, pp. 81–108.
- Office of the Privacy Commissioner of Canada, "What are my business's responsibilities under PIPEDA?", YouTube video (14 min), https://youtu.be/VK2rDI04oDQ
- Ben Wolford, "What is the GDPR, the EU's new data protection law?", Proton Technologies AG, https://gdpr.eu/what-is-gdpr/
- "Fair Information Practice Principles," International Association of Privacy Professionals, https://iapp.org/resources/article/fair-information-practices/

Lecture Notes

In this session:

- Lecture
  - Overview of the history of privacy legislation
  - Summary of modern privacy principles and regulations
- Team Exercise
  - Applying the privacy principles to a case of education technology

The Invention of Privacy

- Privacy *isn't* included in any early treatises defending human rights, or any laws written before the 20th century.
- The very idea of a right to privacy first appears in the 19th century:
  - Newspapers and photography are becoming more common, cheaper, easier to use.
  - Recall (from a previous unit) James Moor's account of computer ethics: new technologies make new actions possible, which necessitates ethical reflection.
  - Several high-profile events where celebrities' privacy was invaded.
    - 1883: Boston lawyer Samuel Warren marries Mabel Bayard, the daughter of a Delaware senator. The local newspapers are eager to report on Mabel's personal life—they start asking for gossip and send reporters to snoop on her social gatherings.

        - 1898: an unauthorized photo of Otto von Bismarck on his deathbed was offered for sale to the press. His family sues and prevents publication of the photo until 1952.
- "The Right to Privacy" (1890)
    - Possibly inspired by dealing with nosy reporters, Samuel Warren, with his classmate from law school Louis Brandeis, write an article in the *Harvard Law Review* defending a right to privacy.
    - Warren and Brandeis define the right to privacy as "the right to be let alone."
    - They argue that even though the law of the time didn't list privacy as a right, it seemed to recognize a right to privacy in protecting *other* rights.
    - Example: Private diaries and property law
        - Property rights were well-established in US law.
        - There were cases of property rights being invoked to defend the contents of a private diary. The "property" in question is the writings in the diary.
        - Warren and Brandeis argue that, properly understood, what's being protected is actually the *personal information* the writings contain, which doesn't fit easily into the concept of property.
- Timeline of laws on electronic personal data
    - 1960s–80s: Governments start keeping electronic records. Electronic privacy regulations focus on the public sector.
        - 1960s: US government agencies start using electronic databases.
        - 1970: State of Hesse, Germany, passes the world's first data protection law.
        - 1973 onwards: US agencies develop the Fair Information Practice Principles (FIPPs). These are guidelines, not laws, and are interpreted and applied differently by various agencies.
        - 1983: Canada passes the *Privacy Act*, which applies to government agencies.
    - 2000s–10s: Privacy laws regulating how private companies can collect and use electronic data are developed in response to the growing role of for-profit data processing, online commerce, and smart phones.
        - 2009: Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) enters full force. This law applies to *for-profit* organizations conducting business in Canada.
        - 2018: EU's *General Data Protection Regulation* (GDPR) enters full force. This set of regulations applies to organizations *worldwide* who collect and use EU citizens' personal data.
- Today: an alphabet soup of information principles
    - The exact list of FIPPs changes depending on the source.
        - Original 1973 report lists five principles.
        - Federal Trade Commission (FTC) lists five slightly different principles.
        - International Association of Privacy Professionals (IAPP) lists eight principles.
    - PIPEDA lists ten fair information principles.
    - GDPR lists seven data protection principle and eight privacy rights.
    - For our purposes, we'll focus on what's in common among these regulations.
    - You'll need legal advice to navigate these regulations if you're starting a business. But day-to-day, you can get by with the following general concepts.

Fair Information Principles

- Defining Personal Data/Information

    - Recall (from the previous lesson): having privacy means having control over the flow of information about you.
    - This information includes facts that can be used to identify you, such as:
        - Your name
        - Your appearance
        - Your voice
        - Etc.
    - Also included: information about where you are and what you're doing:
        - Your geographic location
        - Your device's MAC address
        - Your device's IP address
        - Applications you're running
        - Websites you've visited
        - Purchases you've made
        - Recordings of you
        - Etc.
    - "Sensitive" data are intimate or exploitable facts about you:
        - Information about your health
        - Information about your relationships
        - Banking or credit card details
        - Passwords
        - Usernames
        - Government-issued ID numbers
        - Etc.
    - Recall (from the previous lesson): You might still have privacy even if some of these data are shared. You lose privacy when these data can be associated with you as an individual.
- Principle 1: Consent
    - You need *free and informed consent* before collecting personal data at all.
    - "Free" means "given willingly." If the user cannot decline or was tricked, they haven't given consent.
    - "Informed" means not just telling the user *which* data will be collected, but also *how they will be used.*
    - You need to ask for consent again before using personal data for a new purpose.
    - Consent can be withdrawn: you may be required to destroy or stop using data if asked (cf. GDPR's "right to be forgotten").
- Principle 2: Justification
    - You need a *good reason* collect, retain, and use personal information.
    - When getting consent, you must explain these reasons.
    - When asked, you must explain these reasons again.
    - You may not collect personal data just on the off-chance they might be useful later. You need a good reason at the time of collection. *Do not collect data if it is not necessary.*
    - If you no longer need personal data (e.g. the purpose for which you needed them is complete), they must eventually be destroyed.
    - The more sensitive the data, the stronger your justification for collecting it must be.
- Principle 3: Accuracy
    - You must ensure the data are *accurate* when collected.
    - You must keep the data reasonably up to date, for example, by asking users to periodically update their profiles.

    - When asked by the person the data are about, you must correct any errors.
    - The more sensitive the data, the more important that they are kept accurate.
- Principle 4: Security
    - You must keep the data *safe.*
    - Protect the data from hackers and leaks.
    - Do not reveal the data to anyone who is not authorized.
    - Protect the data for people in your own organization who don't have a good reason to access the data.
    - The more sensitive the data, the tougher your security measures must be.
- Principle 5: Accountability
    - Someone at your organization needs to be *responsible* for ensuring the privacy principles are followed.
    - Large organizations need a specific Privacy Officer (and assistants). Smaller organizations might manage by training all staff on how to follow the principles.
    - When challenged, you must show how you've done your best to follow the principles.
    - When there's a breach, leak, or error, you must disclose it to the people affected.
    - Data protection by design and by default (GDPR).

Team Exercise

Now that we've discussed the ethics of privacy in general (see previous lesson) and some specific privacy principles, let's get some practice applying these concepts to a real case.

Case: Attendance-Tracking Apps

SpotterEDU is an education app for smartphones with the following features:

- Integrates with college registrar records to import students' schedules, with room locations.
- Using Bluetooth beacons installed in classrooms, the app automatically records when students enter and leave class their classes.
- The app uses these data to generate attendance reports. Profs use these to assign attendance grades, and advisors use them to identify students who may be struggling.

The company claims that their app improves student success. But student advocates have argued that it violates their privacy and autonomy.

Team Exercise: Part 1

Imagine that you're working to develop an app with the same features as SpotterEDU. In your teams, discuss and answer the following questions from this perspective.

1. List all the different types of data the app *could* collect from students while operating normally. Identify those that are *needed* for the app's purposes. Note any that are particularly *sensitive* kinds of data.
2. Pick one of the privacy principles, and explain how your company will ensure that it is followed in developing this app.

Team Exercise: Part 2

Imagine now that a university wants to make the use of your app *mandatory* in all of its first-year classes.

3. Consider the perspective of a student at this university. How might they argue that making this app mandatory violates one or more privacy principles? Refer to either a utilitarian argument or a deontological argument in your answer.
4. Think of a rebuttal to the student's argument. Can you provide a good reason to think they are mistaken?
5. As a team, decide which perspective you find more convincing: the pro-privacy student argument, or the rebuttal from the perspective of the tech company.

Class Discussion

Questions to guide discussion of the team exercises as a class. The poll can be done by show of hands, with iClickers, or with a classroom response app (e.g. Top Hat).

Classroom Response Poll

What was your conclusion—Is it unethical for a university to make the use of an attendance monitoring app mandatory in first-year classes?

- Yes
- No
- Depends on circumstances (be prepared to explain)

Lines of Questioning

1. What data *can* the app collect? Which data does it *need* to collect? Which data are *sensitive*?
2. Which privacy principle did you choose? How did you indicate you would comply with it? (If some principle wasn't chosen by a team: how would you comply with *that* principle?)
3. What arguments might a student advocate make against making the app mandatory? How do these relate to the ethical theories we've been studying?
4. What arguments can be made in response? How do these relate to the ethical theories we've been studying?
5. Why did you find the answer you chose more convincing? Are there any other arguments you considered? If the circumstances matter, which ones, and why?

