Embedded EthiCS @Harvard: S20 Repository Entries
Lyndal Grant

1. **Course**. CS1: Great Ideas in Computer Science

2. **Course Level.** Introductory undergraduate

3. **Course Description.** "An introduction to the most important discoveries and intellectual paradigms in computer science, designed for students with little or no previous background. Explores problem-solving using high and low-level programming languages; presents an integrated view of computer systems, from switching circuits up through compilers and GUI design. Examines theoretical and practical limitations related to unsolvable and intractable computational problems, and the social and ethical dilemmas presented by such issues as software unreliability and invasions of privacy."[1] (Course description)

4. **Module Topic.** Electronic Privacy

5. **Module Author.** Lyndal Grant

6. **Semesters Taught.** Spring 2019-2020

7. **Tags.** social networks (CS), anonymization (CS), privacy (both), consent (phil), public interest (phil)

8. **Module Overview.** This module introduces the concept of electronic privacy and asks *Why is electronic privacy valuable?* Students are introduced to what Solon Barocas and Helen Nissenbaum call "the traditional privacy protection paradigm", according which tech companies can adequately protect users' privacy through a combination of informed consent and data anonymization. We explore a number of challenges to this paradigm. Are lengthy and complicated terms of service agreements an effective way to secure informed consent, for example? How does the fact that machine learning allows highly sensitive personal information to be inferred from seemingly mundane user data complicate questions about consent? Is de-identification an effective way to ensure data remains anonymous, given that a small number of datapoints are often adequate to re-identify particular users (as Latanya Sweeney has shown)? We also discuss why we should care about our own electronic privacy, and whether robust privacy protections are in the public interest.

9. **Connection to Course Material.** This module follows up on class sessions in which students learn simple data encryption techniques. Since encrypting user data is one way to protect user privacy, this sets us up for a discussion of how user privacy has traditionally been understood in the tech industry, as well as recent challenges to that understanding.

---

[1] http://sites.fas.harvard.edu/~cs1/no1.cs1.2016.pdf

Marginal note: CS 1 is an introduction to computer science for students who do not plan to major in the discipline. Since students in the course have limited technical training as well as an unusually diverse set of backgrounds and interests, it makes sense to focus on a relatively nontechnical topic that will resonate with a broad audience. This topic fits the bill.

10. **Module Goals.**

1. Encourage students to consider a variety of explanations for the value of electronic privacy.
2. Help students to think critically about whether systems put in place by social media companies, online retailers, and the like genuinely protect their electronic privacy.
3. Discuss necessary and sufficient conditions for informed consent when it comes to giving away private information.

11. **Key Philosophical Questions.**

1. Why is electronic privacy valuable?
2. Does a person who feels that they have "nothing to hide" nonetheless have self-interested reasons to care about electronic privacy?
3. Are strong electronic privacy protections in the public interest?
4. Does the fact that companies can use personal information that you have intentionally given them to infer personal information about you that you have not intentionally disclosed complicate questions about informed consent to data collection?

12. **Key Philosophical Concepts.**

- Privacy
- Self-interest
- Public interest
- Informed consent

13. Assigned Readings.

- Salon Barocas and Helen Nissenbaum, "Big Data's End Run Around Procedural Privacy Protections," *Communications of the ACM.*
- Erica Pandey, "I'm being Watched at Amazon Go and I Don't Care," *Axios.* https://www.axios.com/amazon-go-privacy-big-tech-instagram-971eafc2-c37f-406d-a0a6-d4bab5976f1c.html

Marginal notes: Barocas and Nissenbaum's article introduces students to what they call "the traditional privacy protection paradigm," according to which informed consent and anonymization are sufficient to protect user's electronic privacy. The authors argue that informed consent and data anonymization are not merely difficult to achieve, but, in the age of big data, unsuited to the job of protecting privacy. The authors draw a parallel to the role of informed consent in biomedicine to argue that companies' approaches to protecting user privacy ought to be informed by review processes that assesses "the substantive values at

stake in these informational practices" (p.33) While the article is dense, it is accessible to a general audience (which makes it a good fit here).

Pandey's article expresses the common view that the value of electronic privacy for individual users is usually trumped by the convenience of services companies like Amazon and Google offer in exchange. The article thus sets us up to discuss whether we have self-interested reasons to demand stronger privacy protections from companies that collect our data, as well as whether we have reasons to care about privacy that go beyond self-interest (narrowly construed).

14. **Class Agenda.**

    1. What is privacy? Defining informational and electronic privacy.
    2. The traditional privacy protection paradigm: informed consent + anonymization.
    3. Challenges to traditional paradigm.
    4. Case studies: Amazon Kindle's terms of service agreement; Strava fitness app and US military bases; Samaritan's RADAR suicide prevention program.
    5. Do we have self-interested reasons to care about privacy if we have nothing to hide? Are there public interest reasons to care about privacy?

15. **Sample Class Activity.** After discussing ways in which informed consent and anonymization might fail to protect privacy in the era of big data, students are encouraged to think about why we should care whether our electronic privacy is protected if we have nothing to hide. In small groups of 3-4, students briefly discuss the following questions, followed by a full-class debrief:

    1. Do those of us who have "nothing to hide" have self-interested reasons to care about privacy?
    2. Are there other, non-self-interested reasons to care about privacy?

Marginal note: We find that getting the students to generate as much of the module content as possible both promotes broader engagement and helps the instructor get a better feel for what students already understand and how they are thinking about the ethical issues under discussion. By conducting this activity at the start of the segment on why electronic privacy matters, the Embedded EthiCS TA gives students the chance to introduce arguments and ideas that will be discussed in more detail later in the module (as opposed to introducing them by lecturing).

16. **Module Assignment.** In the follow-up assignment, students are asked to write a short essay in response to an excerpt from a *New York Times* article about the sale of user data by telecommunications firms and mobile apps. The excerpt and essay prompt appear below.

    Excerpt: "Telecommunications firms and mobile-based apps make billions of dollars per year by selling customer location data to marketers and other businesses, offering a vast window into the whereabouts of cellphone and app users, often without their knowledge.

That practice, which has come under increasing scrutiny and criticism in recent years, is now the subject of a proposed ban in New York City […]
The Bill would restrict cellphone companies and mobile apps from sharing location data to situations where they were "providing a service explicitly requested" by the customer. The language is designed to challenge the vague agreements customers click on when signing up for an app or a cellular service. The legislation would also exclude the collection of location data in 'exchange for products or services.'"
-From a July 23, 2019 article in the *New York Times*, "New York City to Consider Banning Sale of Cellphone Location Data" Jeffrey C. Mays

Essay prompt: Do you think New York City should pass the legislation? Please support your answer using ideas from the lecture and/or readings, and make sure to consider at least one reason based in public interests. (Your response should be approximately two to three paragraphs in length.)

17. Lessons Learned

Student reaction to the module was very positive. However, the class was on the larger side (around 60 students), and participation was initially limited to a relatively small number of students until a small-group discussion activity encouraged more voices to join in. This reinforced our view that it helps to include a short active learning exercise as early as possible in the module – even a two- or three-minute pairs discussion activity can be an effective way to draw more students into the conversation and ensure the whole class is engaged.