Education before Regulation: Empowering Students to Question Their Data Privacy

We need to be taught to study rather than to believe, to inquire rather than to affirm.

—Septima Poinsette Clark

Data from the core academic processes of teaching, learning, and scholarship is estimated to be a potential multibillion-dollar (perhaps multitrillion-dollar) market.¹ Not surprisingly, privacy concerns around this data have become an increasingly hot-button topic. In an ever-increasing array of examples, data privacy violations have whittled away consumers’ trust.² Higher education institutions, experiencing their own trust crises, have a duty to protect data privacy beyond consumer standards. EDUCAUSE listed privacy as the third most-pressing issue for higher education information technology in 2019.³ The conversation around data privacy in higher education often centers on regulation, legislation, and policy development. While laws and internal policies are critical, they take time to develop, and in that time new models and practices come forward to bypass proposed and existing regulations. Given the enormous economic incentives to collect personal data, it seems unlikely that law or policy will ever fully catch up with business strategy.

As educators and researchers like Chris Gilliard, Estee Beck, and Audrey Watters have argued, data privacy comes with a special set of concerns and issues for students. First of all, if students want to participate in standard educational activities, they often have little opportunity for real choice or consent around what data is collected. Additionally, once the data is collected, students have little visibility into how that data will be leveraged, monetized, or exposed later on. Given ongoing developments in data science application and analysis, data that seems innocuous or even anonymous today may well put students at risk in the future. And even though it is the job of academia to educate students, in many cases students remain unaware of how valuable their data is, how their data is being collected, and what can be done with their data.

We must work not only toward providing better security around student data but also toward educating students about the need to critically evaluate how their data is used and how to participate in shaping data privacy practices and policies. These policies and practices will affect them for the rest of their lives, as individuals with personal data and also as leaders with power over the personal data of others. Regulation is necessary, but education is the foundation that enables society to recognize when its members’ changing needs require a corresponding evolution in its regulations. And for those of us in academia, unlike those in industry, education is our work.

We don’t want to underestimate the important changes that have occurred in regulations and policies. In the last two years, US higher education institutions have increasingly begun hiring chief privacy officers, a relatively new role.⁴ Google updated its student privacy policies after the Electronic Frontier Foundation filed an FTC complaint about its practices in December 2015.⁵ And there is broad recognition that new laws must be passed to account for the changing landscape, with 41 states passing more than 126 laws related to K-12 and higher education student privacy in the last six years.⁶ Given these signs of progress, some might think we can just hold our breath until law and common sense sort out our data privacy woes in their own due time. These are promising moves toward creating regulation and policy that may better protect student data at a structural level. Nonetheless, we believe that they are insufficient on their own and that education is needed in addition to these efforts.

Fortunately, there have also been a number of critical responses to these issues on the part of educators or workers in higher education. Laura Gibbs, in her impressive blog series, advocates for the ability to entirely opt out of predatory student data-collection practices.⁷ The Ethical EdTech wiki—a collaboration in which we are involved, along with co-founder Nathan Schneider and others—seeks to point out tools that value user freedom, privacy, and control. And we recognize that a number of individuals and communities working within or adjacent to higher education have taken a special interest in advocating around these issues, including SurvDH, FemEdTech, Digital Tattoo, and the Digital Library Federation’s Technology of Surveillance Interest Group.

Data privacy issues may seem secondary to the disciplinary focus of some courses, but ignoring their presence in learning activities teaches students to passively accept
these practices as inevitable and neutral. Our emphasis on education is inspired by pedagogues and civil rights educators such as Septima Clark, Paulo Freire, and bell hooks, all of whom framed education as a liberatory practice. Each of these educators demonstrated the importance of empowering students to critically assess and transform the status quo. Similarly, we believe that the classroom might be leveraged as a powerful site to raise student awareness about the complex struggles occurring with data privacy.

It is not always easy to translate these ideas into teaching. In the spirit of contributing to these important discussions and interventions, we wanted to suggest additional resources to help instructors draw student attention to data privacy issues. One approach that we have explored is placing, in the course syllabus, a statement that invites students to consider their data privacy and discuss concerns with the instructor or other campus experts. We make no claims that such a statement, by itself, will solve problems of data privacy but are hopeful that it might help contribute to a broader conversation and offer concerned educators an accessible way to acknowledge these issues in the classroom. We recently workshopped the idea of such a statement at the Domains 2019 conference in Durham, North Carolina, where participants helped to write the statement and as well as offered a diverse range of questions about its aims and effectiveness. We present a version of that syllabus statement here for reuse and/or remixing.

Your personal data is valuable and important, which is why it is often collected by the digital tools you use in your educational activities. To better understand how and why your data is collected, the potential risks of this collection, and how to better protect your personal data, consider asking yourself the following questions:

- What types of personal data do you think are collected through your use of digital tools for educational activities?
- What value does your personal data have for different contexts and entities? Consider how your data might be valued by your instructor, the institution, yourself, and companies.
- Who owns your personal data, who can sell it, and who can use it?
- Do you have concerns about how your personal data can be used? If so, what are they?
- Are there aspects of your identity or life that you feel would put you in a place of special vulnerability if certain data were known about you or used against you?

If after asking yourself these questions you have concerns, I invite you to reach out to me to discuss them. I may not have easy answers to the questions or concerns that you bring to me (often in these matters no one has these answers), but I will happily explore them further with you or find someone more knowledgeable who can help answer your questions.

We understand that differing power dynamics in various contexts may make including such a statement in the syllabus problematic. Some of the questions that came from our workshop included the following: Would students actually read it? If they did, would overworked instructors have time to address their concerns? Could instructors get in trouble for using it? Is the classroom the right place to address these issues?

We admit that as a resource, the statement may have its limitations, but educators cannot sit on the sidelines when it comes to the issues surrounding students and data privacy. Our larger point is to ask educators to make a statement, be it in the syllabus or otherwise, about the need to educate students on these matters. Other ways to do so might be to create an assignment or even an entire course that addresses these issues, bring these issues to a curriculum committee, inquire about the use of data on campus, and/or request professional development opportunities related to addressing data privacy concerns.

We invite educators to share their adaptations of the syllabus statement, or other ways they are provoking the discussion about data privacy education, on Twitter with the hashtag #StudentPrivacyStatement so that we can learn how others are choosing to address these issues.

Notes
We would like to thank all those who attended our session at the Domains 2019 conference and who assisted in drafting the syllabus statement, including Kristy Lukens, Bill Kronholm, Amanda McAndrew, ipromikegee, Carrie Johnston, Amie Freeman, Joseph M. Murphy, Jonathan Poritz, and Trip K. We would also like to thank Chris Gilliard and Maha Bali, who helped to review early drafts of this article.


Autumn Caines (acaines@umich.edu) is Instructional Designer at the University of Michigan Dearborn. Erin Glass (erglass@ucsd.edu) is the Digital Scholarship Librarian at the University of California San Diego.

© 2019 Autumn Caines and Erin Glass. The text of the syllabus statement is licensed under the Creative Commons No-Rights-Reserved License. The text of the rest of this article is licensed under the Creative Commons Attribution 4.0 International License.