

Putting MOOCs in Context: Student Privacy in Digital Learning Spaces

Helen Nissenbaum & Elana Zeide

The student privacy discussion has reached a fever pitch. President Obama spoke of the need to better protect student information at the Federal Trade Commission and his State of the Union address in January 2015. Much of the current student privacy debate stems from concerns raised by cloud computing and big data technologies which make school records more permeable, portable, and repurposable. Third parties are quickly becoming integral to data flow in education, both as service providers to traditional educational institutions and in delivering instruction directly to learners via independent platforms. Stakeholders worry about unauthorized access or “commercial” misuse of sensitive student information as schools increasingly rely on private entities to supply data-driven education services ranging from instructional modules to cafeteria management.

Policymakers, industry representatives, and advocates have responded with a flurry of proposed reforms, including amendments to the primary federal statute governing school records, the Family Educational Rights Act (FERPA). Most of the existing, new, and proposed reforms regulate how primary and secondary schools share student information to limit vendor's ability to sell student information or use it to drive targeted advertising.

The student privacy conversation focuses on protecting children and information generated in traditional educational institutions. In doing so, it neglects the increasing prominence of private learning platforms like Massive Open Online Courses (MOOCs) that increasingly perform traditional school functions in the education system.

The New York Times declared 2012 the “Year of the MOOC.” Reformers heralded these free, on-demand, digitally delivered courses as a panacea to the high costs and questioned value of higher education in America. These platforms not only provide access to inexpensive educational resources, but also collect information about students at every moment of the learning process that can be used to evaluate outcomes and drive decisions through big data analytics. As Coursera founder Daphne Koller has noted, “Every variable in a course is tracked . . . Every [student] action, no matter how inconsequential it may seem, becomes grist for the statistical mill.”

The original MOOCs have since evolved into a variety of “MOOC-ish” digital, interactive learning platforms that are no longer massive, free, strictly online, or complete courses. Many of these new education providers are for profit companies that offer instruction for free while charging for assessment, certification, or connection to potential employers. The business model for these entities is still emerging, as some consider raising revenue through targeted marketing or mining student information to sell to employers or advertisers.

While the pedagogical and institutional effects of these platforms remain controversial, their easy accessibility, efficiencies of scale, and ability to provide more “personalized” learning paths fill important gaps in the education system. Students access these tools to supplement classroom activity, prepare for standardized tests, or take advantage of mobile learning apps,

often at the direction of their teachers and professors. As independent actors become more central to students' learning experiences and credentialing, their information practices will be crucial to students' educational success and the broader political, economic, and social goals of the education context.

This presentation, based on a forthcoming article, situates MOOCs, and similar virtual education providers, within the information ecosystem and regulatory regimes governing the education and commercial contexts. Although for-profit online learning platforms perform the functions of traditional educational institutions, and present themselves as similarly serving the public good, they operate under the commercial notice-and-consent regime that permits information practices at odds with existing norms about student data. Because FERPA does not explicitly prohibit certain practices but imposes requirements as a condition to receive federal funding, it does not apply to these new, virtual education providers that receive information directly from learners.

These entities instead operate under the minimal constraints of the commercial notice and consent regime. They have almost unlimited leeway to share and monetize this data in ways at odds with user expectations, companies' self-presentation, and the broader purposes served by education as a public good. Many platforms, for example, share student information with unspecified third party "partners" or "affiliates" in ways that would require parent, student, or school approval under FERPA.

Student-consumers are frequently unaware that these new educational entities may not prioritize educational goals and approach privacy accordingly. While these platforms are free to use learners' information in ways that run counter to the norms of traditional learning environments, they present themselves as public service-oriented educational providers, not commercial entities. Their status as for-profit entities is hardly acknowledged, and in some cases obscured, on company websites.

Existing regulation and the proliferation of new student privacy reforms highlight an important, almost too-obvious point: that, we, as a society, seek a higher level of protection for information created in learning environments. Unlike commercial relationships, we presume a certain level of trust between educators and students of all ages.

FERPA, for all its flaws, acknowledges that information generated in schools should be treated differently from common commercial data. Student privacy regimes codify our skepticism about outsiders in the education system that may prioritize their own interests over students'. As has been abundantly illustrated by the actions of for-profit colleges, the potential conflict of interests between providers' economic and students' educational interest creates an environment that will exert tremendous pressure on companies to extract additional economic value from student data.

Even absent profit motive, student information in the existing regulatory regime may be treated as an ordinary corporate commodity in ways that run counter to stakeholder expectations. It can be sold to an acquiring company or as part of a bankruptcy proceeding to entities that have no intent to use learners' personal data to provide education services. Further, privacy self-management does not account for the broader consequences of these entities'

information practices to the education context itself. Ubiquitous surveillance may, for example, chill intellectual exploration and rigorous predictive analytics have the potential to retrench existing inequalities.

Applying education context norms to virtual learning providers is more consistent with their self-presentation, user expectations, and furthering the goals, purposes, and values of the broader educational enterprise in America. Student privacy regimes reflect the measure of trust that learners, parents, and society must have to be able to entrust education providers to train individual minds and promote import broader political and economic ends. While these norms are continuing to emerge and shift as society and schools adapt to new technological capabilities, students, who happen to also be consumers, should be protected accordingly.