**The Case of Canvas: Longitudinal Datafication through Learning Management Systems**

Citation:  
Marachi, R., & Quill, L. (2020). The Case of Canvas: Longitudinal Datafication through Learning Management Systems. *Teaching in Higher Education*, *25*(4), 418–434.

Link:  
<https://ezproxy.snhu.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1254094&site=eds-live&scope=site>

Interesting Quotes/Points:  
As Hill ([23]) noted, (SaaS) models offered advantages over on-site LMS platforms, namely, the ability to mine and report data, and to use the latter to support outcomes-based (rather than enrollment-based) funding models for public institutions.

CoursEval, a program managed by CampusLabs is an external course evaluation app integrated into San José State University's Canvas Instructure LMS. Course evaluation procedures that previously involved sealed envelopes, campus mailboxes, and confidentiality provisions that wouldn't allow for the removal of faculty dossiers from department offices, have now been transferred to online spaces with data that appear open to analysis by third-party entities and by cloud hosting LMS and AWS data servers. The Canvas Data tool documents a parsing and aggregation of more than 280 million rows of Canvas usage data daily (Instructure [28]).

It is unclear what access is given to whom to engage in the analytics described. If instructors are the only ones with access to their student data, as FERPA would suggest, they would not be the ones to analyze the 280 million rows of Canvas usage data generated daily. If administrators or other data analysts are accessing student/and or faculty data, they would be doing so without knowledge or consent of users, most of whom are given the impression that the LMS is protecting their data from outside use.

What remains unclear is the fate of the student and faculty data as a result of this pending purchase or any other. Data privacy concerns and questions related to the Instructure acquisition have been outlined in a public letter co-signed by dozens of individuals working at colleges and universities that use the Canvas LMS (Young [46]). The letter references legal scholars who have noted the vulnerability of student data to exploitation in private markets. Russell et al. ([43]) have written about the commercial availability of student lists for purchase 'on the basis of ethnicity, affluence, religion, lifestyle, awkwardness, and even a perceived or predicted need for family planning services' (i). With no federal privacy laws governing student data brokers, student data can be collected, sold, and bought without any apparent legal protections from widespread exploitation.

AWS accounts, along with business and government websites and servers, have become vulnerable to 'cryptojacking' schemes in which hackers break into them to mine cryptocurrency, which has become increasingly lucrative in the past year. 'Given the immaturity of cloud security programs today, we anticipate this type of cybercrime to increase in scale and velocity,' RedLock CTO Gaurav Kumar said in a statement to Business Insider. (Matousek [35])

<https://www.softwareadvice.com/lms/blackboard-learn-profile/vs/canvas-instructure/>

<https://www.pcmag.com/reviews/blackboard-learn-lms>

<https://www.pcmag.com/picks/the-best-lms-learning-management-systems>

<https://www.pcmag.com/reviews/instructure-canvas-lms>

<https://help.blackboard.com/Blackboard_App/Feature_Guide>