Analysis of Blackboard LMS Privacy Policies

White Paper

February 28, 2022

Dr. Heidi Howkins Lockwood, Joseph Delgado, Gavin Paeth, Alec Leyner, Kyle Landry, Ulish Booker, and Ian Cheung

Contents

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

~ Edward Snowden

Introduction

Privacy is a fundamental human right. It is protected in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Fourth Amendment of the U.S. Constitution, along with the constitution of nearly every country. Minimally, these provisions include the right to privacy in communications and the inviolability of one's personal abode and body. Many recently written constitutions also include specific rights to access and control over one's personal information.

The Connecticut State Colleges and Universities (CSCU) Data Privacy Office is committed to identifying and prioritizing user privacy risks in alignment with the National Institute of Standards and Technology (NIST) Data Privacy Framework. The NIST Privacy Framework calls for institutions to identify, assess, and manage privacy risks involving third parties within the data processing ecosystem.

This paper is an analysis of the potential privacy risks involving Blackboard, a third party Learning Management System (LMS) contracted by the CSCU to provide LMS services for the 17 institutions in the CSCU system. It has been written in response to an invitation to conduct an analysis from the CSCU Associate Vice President of Digital Learning.

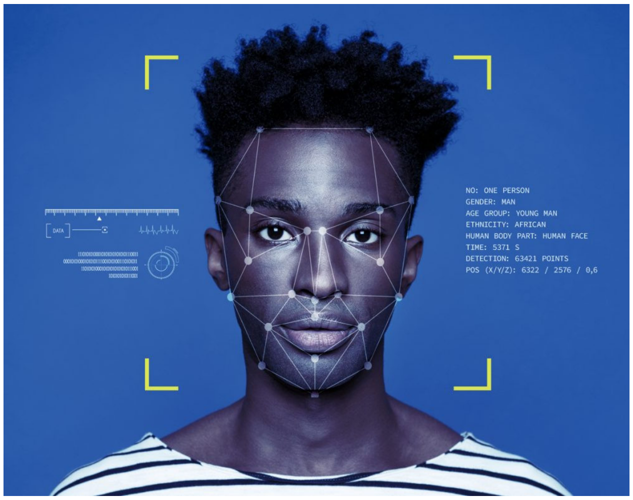
Background

Why Privacy Matters

The American Civil Liberties Union (ACLU) has been sounding the alarm about the sharp increase in police surveillance in U.S. cities for many years now. The number of police-operated cameras in public spaces has increased exponentially over the past decade. And in many cities, including Washington, Dallas, Chicago, New York, and Los Angeles, cameras are equipped with high-resolution lenses, infrared night vision, and facial recognition-enabled scanning technology.

In many cases, the data from public cameras is fed into a national system. The Southern Connecticut State University Police Department, for example, received a grant for a campus-wide system of cameras that feed license plate recognition data into a nationwide network of police-based data called Vigilant Solutions. When the ACLU revealed in 2019 that the SCSU PD was one of eight Connecticut law enforcement agencies feeding license plate data to the Immigration and Customs Enforcement Agency (I.C.E.), the SCSU PD immediately moved to discontinue the data sharing with I.C.E. But the cameras are still in place, and still sharing data with an estimated 3,000 police departments and an unknown number of private investigators.

Some of the police departments in the Vigilant Solutions network, such as the NYPD, have a long history of spying on Muslim Americans far outside their jurisdictions. And both license-plate readers and the information derived from them have already been misused in other jurisdictions.



Concerns about abuse of LPR data have been amplified by the growing number of public cameras collecting data that can be used in conjunction with facial recognition databases.

In March 2019, for example, journalists at *The New York Times* called attention to the problem by using the public online streams from three cameras in Manhattan together with a database of public photos to identify individuals in the field of the cameras.

And in the summer of 2020, an AI startup called Dataminr helped law enforcement digitally monitor the protests that swept the country following the killing of George Floyd, tipping off police to social media posts with the latest whereabouts and actions of demonstrators.

The surveillance in each of these cases was enabled and enhanced by the availability of Personally Identifiable Information (PII).

Privacy and the Pandemic

The concerns associated with privacy risks in the collection of PII have also been exacerbated by the COVID-19 pandemic, which has provided just about every governmental entity — and many non-governmental entities — a "justifiable" reason to significantly extend already broad surveillance capabilities.

Israel granted its spy services emergency powers to hack citizens' phones without a warrant. South Korea sent text alerts to warn people when they may have been in contact with a coronavirus patient, including personal details like age and gender. Singapore used a smartphone app to monitor the spread of the coronavirus by tracking people who may have been exposed. In Poland, citizens under quarantine were required to download a government app that mandates they respond to periodic requests for selfies. Taiwan introduced an "electronic fence" system that alerted the police if quarantined patients move outside their homes.

Even individual U.S. states launched COVID tracking apps. The U.S. federal government did not publicly use the pandemic as an excuse to extend surveillance powers. But that might be because the government has already managed to secure what the editors of *The New York Times* called, in a February 2020 op-ed, "near-perfect surveillance data on Americans."

Aggregation of Data

The practice of selling or renting data with PII markers has extended surveillance capabilities beyond governments to the private sector. The global facial recognition market size was estimated at USD 4.45 billion in 2021, and is expected to triple over the next 5-7 years. Geolocation data was valued at around USD 12 billion in 2021 and is growing at a similar pace. When combined with PII such as name and contact information, data such as facial recognition, geolocation, educational records, and speech patterns provide powerful information for anyone interested in identifying and tracking a targeted group or individual.

A 2018 Supreme Court ruling prevented the U.S. government from obtaining location data from cell phone towers without a warrant because, as Chief Justice Roberts put it, "When the government tracks the location of a cellphone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." The U.S. government, however, has simply purchased information available on the private market to anyone, and used it to track the location of persons of interest — without a search warrant. A November 2020 investigative piece by Motherboard (a division of VICE News) revealed that the U.S. military currently purchases location data from a wide range of apps, including Craiglist, a Muslim prayer app, BlackMingle, and an app for following storms.

Analysis

Data Collection

According to the Blackboard Privacy Statement, information that is directly harvested from an end user at an institution includes profile information (first/last name, email, similar contact data); responses to quizzes, assignments and other course work; files that are submitted or uploaded; comments in discussion forums and chats or messages to other users; grading; and feedback and assessments.

Information that is indirectly collected in the form of usage of Blackboard products and services includes data about location and time of access, including information that is sent by the browser or mobile app (which may include IP address or other unique device identifiers, cookie data, and language preferences); enrollment data; classes attended, including time and date of attendance; and responses to notifications. Cookie data may include preferences, security, analytics, social sharing, and targeted advertisement and engagement data.

Blackboard does not respond to Do Not Track or other opt-out mechanisms from browsers or portable devices. According to the Blackboard Privacy Statement Disclosures, users can opt out of receiving marketing information from Blackboard, but collection data is done for all users over the age of 13, with no opt-out procedure.

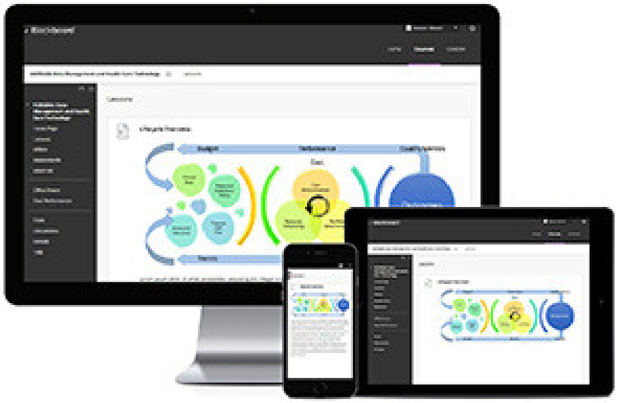
Data Security

At least one of the CSCU institutions (SCSU) provides access to Blackboard via multifactor authentication (MFA) through Microsoft. Other institutions in the system are working on shifting to this model.

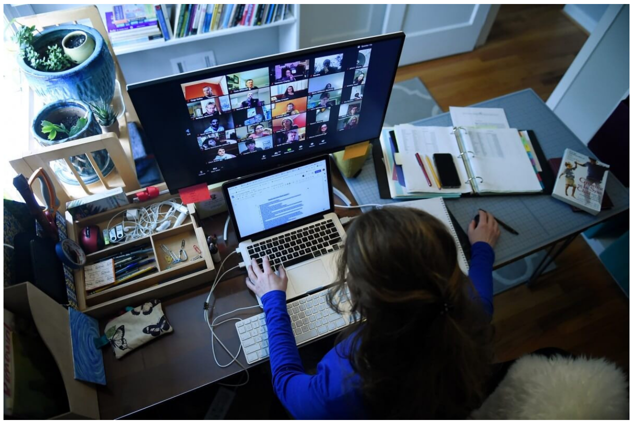
However, Blackboard uses Amazon S3 and Amazon CloudFront to store, cache, and accelerate the retrieval of content. There is currently no password protection on recordings. It is also unlikely that end users are notified in the event of a data breach, given that the services are managed by Amazon.

It is unclear whether end users would have legal recourse in the event of a breach that resulted in tangible harm. Blackboard users are required to waive the right to a jury trial, and the right to class action lawsuits. Users are required to use arbitration to settle disputes on an individual basis.

The Blackboard Terms of Use also specify that the company “shall have no liability for your interactions with other users, nor for any user’s acts or omissions.”



Data Sharing



According to the Blackboard Privacy Statement, Blackboard “may share a common account identifier related to your use of our websites (such as an email address or user ID) with our third-party advertising partners to help identify and contact you across devices. We and our third-party partners use this information to make the advertisements you see online more relevant to your interests, as well as to provide advertising-related services such as reporting, attribution, analytics and market research.”

The Blackboard California Privacy Notice required under the California Consumer Privacy Act of 2018 (CCPA) further specifies that the information that “may be disclosed for business purposes” includes: (1) “protected classification characteristics, such as age or disability (if provided for accommodation purposes)”, (2) “commercial information related to the produced that you… intend to purchase”, (3) “internet/network information, such as device information, IP address, logs and analytics data”, (4) “geolocation data, such as precise location information from your device” and (5) “other personal information that may be contained in online chat, document uploads, and user-generated content.”

Content that is posted by users on Blackboard may also be shared. Section 3 of the Blackboard Terms of Use specifies that “By submitting, posting or displaying content… you grant [Blackboard Inc., a Delaware Corporation] a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, host, store, copy, reproduce, process, adapt, modify, publish, transmit, create derivative works from, communicate, display, and/or distribute such content in any and all media or distribution methods (now known or later developed).”

While the sharing of such content must be in accordance with laws such as the Family Educational Rights and Privacy Act (FERPA), and therefore cannot include the sharing of, say, grades that are associated with PII, it can include the sharing of anonymized or disaggregated data. Grade distribution reports by class and by professor have been intermittently available for institutions in the CSCU system over the past 5-10 years on sites such as the now-defunct MyEdu.com (formerly Pick-a-Prof), or on smaller cluster sites such as GradeToday.com.

Users are not notified when their data is shared, and are not notified when there are policy updates or changes. And, although the Blackboard Privacy Statement and Terms of Use are publicly available documents, the data sharing model is not the "freely given consent" model under the General Data Protection Regulation (GDPR) of the EU.

Conclusion

In October 2021, Federal Trade Commission (FTC) Commissioner Rebecca Kelly Slaughter delivered two addresses in which she warned about the dangers of a market based on the harvesting of data, and signaled the intent to apply "bright-line purpose and use restrictions that minimize the data that can be collected and how it can be deployed."

We write this paper in a week in which the world is bracing for a global cyberwar as Russia invades Ukraine — and in an era in which unconstrained data collection, retention, and sharing has increased the severity of data breaches and fueled misinformation campaigns.

We echo growing public concerns that unchecked data collection could be used by companies and hostile nations to harm targeted groups, and even if harm is not intended, could exacerbate economic or racial inequalities, marginalize workers, or deepen other disparities.

We are concerned that information collected and shared through Blackboard can be combined with data from brokers to categorize and target CSCU students, alumni, and faculty based on their race, ethnicity, sexual orientation, economic status, political or religious affiliation.

We urge the CSCU administration to negotiate increased privacy protections with Blackboard, and to conduct a thorough risk assessment of other platforms and apps used to deliver education across the system.