emerald PUBLISHING

Information and Learning Scie

Privacy Governance Not Included: Analysis of Third Parties in Learning Management Systems

Journal:	*Information and Learning Sciences*
Manuscript ID	ILS-04-2023-0033.R1
Manuscript Type:	Article
Keywords:	Educational technology, privacy, computing/technology policy, empirical studies in social computing, third-party data controllers, Learning Management Systems

Privacy Governance Not Included: Analysis of Third Parties in Learning Management Systems

Higher education institutions often manage student data through learning management systems (LMS) that support third-party plug-ins and learning tools interoperability (LTI). This paper evaluates the governance of these technologies at universities in the United States and Canada with a focus on the implications for student data privacy. Qualitative interviews, an online questionnaire, and content analysis of online university policy documentation reveal a fragmented and opaque ecosystem of student data collection by LMS plugins and LTIs that is tacitly enabled by limited or ineffective governance across institutions. We argue for greater transparency and oversight of LMS platforms, plug-ins, and LTI supported by the creation of a knowledge commons of institutional governance strategies for addressing privacy challenges posed by third-party data flows, commercialization of student data, and education technology decision-making. We highlight some exemplary governance practices identified in our empirical results and provide recommendations for emerging collaborative efforts that are needed to improve the state of student privacy in higher education.

Additional Key Words and Phrases: Educational technology; privacy; computing/technology policy; empirical studies in social computing; third-party data controllers; learning management systems

1 INTRODUCTION

Privacy concerns have grown in tandem with the digital transformation of educational institutions, particularly when considering the political economy of higher education in North America. From concerns about facial recognition in classrooms and on campuses [2] to ubiquitous platformatization of K–12 education [35], the increase in datafication of educational interactions [17] and profiling of students [4] has drawn scrutiny [2, 19, 33]. This trend was amplified throughout the COVID-19 pandemic, as digital solutionism paved the way for virtual classrooms [7] and digital proctoring [6] via synchronous and asynchronous means of collaboration between students and instructors. In response, student preferences [19], university and instructor practices [7, 18], and specific education technology platforms [28, 35] have received scrutiny in recent privacy research. This research has mainly focused on first-party actors subject to federal and state regulation [7, 39], including the extent to which new educational technologies are more intrusive than their antecedents in ways that are inappropriate or discriminatory [26].

Plugins and learning tools interoperability (LTI) for learning management systems (LMS) exist at a crucial intersection of these student privacy issues. Higher education institutions have access to, and in many cases locally host, substantial amounts of student data on LMS that provide third-party mechanisms to enhance interfaces, add new functionalities, and customize user experiences for specific institutions, departments, or courses. The tight integration of first and third-party tools in this ecosystem raises concerns that student data may be accessed and shared without sufficient transparency or oversight and in violation of established education privacy norms. However, both these technologies and the university governance practices that could check inappropriate data handling remain under-scrutinized.

This paper addresses this gap by investigating the governance practices of higher education institutions with respect to LMS ecosystems. We answer the following research questions:

Author's address:

RQ1 How are LMS and plugins/LTIs governed at higher education institutions?
- Who is responsible for data governance activities around LMS?
- What is the current state of governance over LMS?
- What is the current state of governance over LMS plugins, LTI, etc.?
- What governance issues are unresolved in this domain?

RQ2 How are issues of privacy and governance regarding LMS and plugins/LTIs documented or communicated to the public and/or community members?

We investigate these research questions through a multi-modal study with three components. We first used an online questionnaire to collect reports of LMS governance practices from information technology professionals at 7 universities in the US and Canada.

We then conducted in-depth interviews with 25 data governance professionals and decision-makers at 14 US research universities. These individuals have a diverse range of expertise, authority, and roles at their respective universities, including technical services, educational technology, legal counsel, student affairs, faculty governance, and Provost's offices. 24 of 25 interviewees were in staff or administrative positions, while one was an active faculty member who chaired a faculty senate committee on technology. Through these interviews, we obtained policies, procedures, and frameworks for evaluation of LTIs, plugins, and broader LMS data governance considerations.

We also analyzed publicly-available online documentation from 112 universities, including public (n=41), private (n=40), HBCU (n=7), and community colleges (n=14) across the United States (n=102) and Canada (n=10). These data include details of LMS plugin and LTI usage and management at these universities and cover the most commonly used LMS ecosystems (Canvas, Blackboard, and Moodle).

Our results identify several governance gaps relative to LMS and their associated LTIs and plugins:

- There are few legal requirements protecting students from third-party data flows via LTIs and plugins.
- Most scrutiny and governance of LTIs and plugins comes from non-profits, not from universities themselves.
- The governance processes in effect are highly non-transparent to impacted students and instructors, resulting in disenfranchisement.
- Emerging governance practices around student data localization and evaluation of third-party technologies at a few universities are serving as a model for many in higher education.

We discuss these results relative to successful exemplars of plugin/LTI governance and conclude that transparency and coordination mechanisms are needed to ensure that students interests are protected beyond nominal compliance with state and national laws.

2 BACKGROUND AND RELATED WORK

Substantial prior work has examined issues of privacy in the education context, although little research has directly examined higher education institutions' governance practices of LMS, plugin, and LTI ecosystems. This section outlines the related research in these areas and provides background information on LMS plugins and LTI.

2.1 Education Technology Privacy and Governance

Issues of educational data governance and student privacy [7] are inherently a collective action problem, with universities representing one of the most visible knowledge commons [30]. The tensions between student data as a resource and students' rights to privacy must be resolved iteratively with the engagement of students and their interests [23, 30], thereby making contemporary educational privacy governance challenges well suited to data commons arrangements [20].

In recent years, the continued "datafication" of higher education has fueled the integration of new learning analytics and big data approaches to online education platforms. Learning Management Systems (LMS), Virtual Learning Environments (VLE), and Massive Open Online Course (MOOC) platforms aim to mimic and improve traditional educational practices while applying data-driven approaches to personalize and automate established processes [57]. While the use of leaning analytics is promoted as a way to improve learning and student performance [41], these solutions are often implemented as "black boxes," raising a number of concerns around inaccurate, oversimplified student data representation, perpetuating biases and affecting the power dynamics between institution and the learner [46]. Learning analytics can also result in diminishing autonomy, limits possibilities [47], inducing "chilling effects" on student behavior [37, 41], violating students' privacy expectations [22, 58] and introducing conflicts of interests [41].

The adoption of online education platforms has also accelerated a technological shift from on-site servers to cloud-based solutions for managing student and institutional information [1, 13]. As a result, a substantial number of information flows involving students' academic data are becoming available to third-party service providers [13].

As fiduciaries of student data, educational institutions should adopt student-orientated information governance practices and demand the same from third-party vendors [21]. Furthermore, there is a shift in governance of online educational activities from public scrutiny to contract and commercial law that requires greater transparency in arrangements between higher education institutions and platform companies about what student data is shared with whom and for what purposes [25].

The common lack of appropriate governance for technology procurement in higher education institutions also exacerbates the situation, as institutions are ill-equipped to adequately address new privacy threats [7, 36]. In many universities the policy statements related to student information are outdated and inadequately reflect the privacy issues in modern higher education [5]. This has prompted calls [38] for vetting processes that examine the information handling practices of big data companies and ensure that they align with educational purposes; and for universities' data privacy governance policies and practices to be revised to center around duty of care to students [5].

It is important to recognize that educational contexts, regardless of technological mediation, are sites of collaboration and social engagement [50]; education technology facilitates social computing by default, extending networked and social privacy challenges into this context [52]. Social aspects, and the inherently networked nature of student data flows, require further empirical scrutiny; this gap can be contextualized, and future research informed, by other scholarship on social aspects of privacy.

Connecting to this broader literature on the unequal [15, 31] and contextual nature of privacy [3, 32], recent studies have illustrated the importance of critically engaging with conceptual and theoretical frameworks in order to strengthen empirical studies of privacy [42, 45], spanning qualitative, quantitative, and mixed

research designs [27, 43]. The research community elucidates the social and networked nature of privacy, critically examining the implications of sociotechnical systems on individual collaborators' [52], experts [12] and users' [3], as well as on communities' privacy [24] as experienced. Studies also illustrate the challenges associated with the collection of rich qualitative details to provide insight into the contextual experiences and nuance of examples relative to privacy, documenting mechanisms for rigor with small samples [48], especially in conjunction with multi-method designs [48, 52]. Our work continues this thread by investigating understudied elements of the higher education technology ecosystem.

2.2 LMS Plugins and LTI

The use of extensions in the form of third-party plugins and LTI integrations are commonplace in the LMS ecosystem. They provide mechanisms to enhance or add new interfaces and functionalities to existing LMS platforms and customize user experiences for specific institutions, departments, or courses. LMS plugins typically connect to external web services to implement their functionality. For example, Moodle's Virtual Programming Lab (VPL) [40] integrates programming assignments and assessment and connects to a supported VPL server to compile students' code. Plugins like Turnitin [56] and Crowdmark [53] use the Learning Tools Interoperability (LTI) [54] protocol to communicate with their third-party (non-Moodle) servers. The LTI has become a de facto protocol for LMS plugins on major LMS platforms, including Moodle, Canvas and Blackboard.

2.2.1 Privacy APIs. With the advent of European GDPR regulation, many LMS platforms have deployed a privacy-related API. In Moodle, privacy features are implemented using the Privacy API [55], which is centered around the GDPR notion of protecting personal, identifiable data. Moodle's data model differentiates between information that the user enters and information that is stored. Developers of new third-party plugins need to indicate whether the plugin stores or exports data. When a plugin stores data in a database or interacts with a Moodle subsystem (e.g., Moodle comments, ratings, questions, filesytems) that will result in storing user data, developers explicitly indicate the type of data being stored. When a plugin stores data in its own database, the developer needs to describe each field that includes user data. Moodle API guidelines suggests that "it is a matter of judgement which fields contain user data and which don't. Anything entered by, or directly about, the user probably counts as user data but it may be useful to include additional fields that explain the context of the data." If a plugin exports user data, the developer needs to indicate the target of export and the exported user data fields. In addition, the developer of the plugin needs to implement a function that facilitates the actual export of the data according to the API specifications. A third-party Moodle plugin that adheres to the Privacy API is automatically awarded the "Privacy Friendly" award to inform users that the plugin is following the Privacy API guidelines.

2.2.2 Plugin Certifications. Several universities use 1EdTech's IMS TrustEd Seal program that "certifies that an institution successfully completes training in the IMS TrustEd Apps vetting process and possesses the necessary skills to vet applications for privacy and security using the IMS TrustEd Apps Rubric." [8]

Certified institutions use IMS TrustEd Apps vetting process to conduct independent reviews according to the TrustEd Apps Rubric [8]. The IMS TrustEd Apps Rubric identifies several areas of examinations: data collection, security, third-party data sharing, and advertising. Additional, an optional extension of the

rubric include availability of policy, data handling, social interactions, legal (state and federal regulation), accessibility, mobile and integrations.

For each category, the assessment determines whether the privacy policies and practices "meet expectations" of the rubric. The data collection portion of the rubric comprises five points: 1) The policies list all data collected; 2) The policies indicate how data is collected; 3) The policies state who owns the data; 4) The policies allow users to delete their data entirely; 5) The policies state the retention of data.

The third-party sharing portion of the rubric includes five points: 1) The policies state the use of third parties; 2) The policies state what information is shared with each third party; 3) Users can opt out of third party data sharing; 4) The supplier requires their third parties to adhere to the terms of the vendor/customer agreement; 5) The user is notified of a change in third parties.

A special area of examination is dedicated to advertising. It includes evaluating that policies indicate 1) whether or not advertisements are displayed, 2) whether or not users are targeted for advertisement, 3) whether or not any third parties track or collect information for advertisement, 4) whether or not web beacons or other tracking methods are used for ad purposes, 5) whether or not users can opt out of sharing data with advertisers.

2.2.3 LMS Risk Assessment. Some educational institutions rely on vendors' assessments to evaluate the privacy risks of new education technologies. The EDUCAUSE [10] Higher Education Community Vendor Assessment Toolkit (HECVAT) [11] risk assessment of third-party solutions ranges from questions about whether the entity providing of the technology performs "security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.)" to questions on general governance roles, such as "Do you have a dedicated Information Security staff or office?" and "Do you have a dedicated Software and System Development team(s)?" The form also includes questions about organizational structure, audits, and self assessment histories. From the 13 questions on the *Documentation* section of the HECVAT, two are related to a notion of information privacy: "Does your organization have a data privacy policy?" and "Can you provide overall system and/or application architecture diagrams including a full description of the data flow for all components of the system?" The form also asks seven additional questions about data management, including data isolation, encryption in storage and in transport, backup, and staff access to institutional data.

2.3 Governing Knowledge Commons

The Governing Knowledge Commons (GKC) framework [42, 44] provides an adaptable structure to analyze information governance regarding collective knowledge production and sharing in context. GKC considers the social, economic, and political background in which information is governed, as well as important attributes, such as the relevant actors, their roles and objectives, and their resources. The framework is grounded in a broader tradition of institutional analysis [34] and applies an institutional grammar [9] to examination of strategies, norms, and rules that shape information handling practices, providing a foundation to understand the emergence of new information norms and how communities and stakeholder groups shape specific governance mechanisms.

The GKC framework has been applied to studies in diverse contexts, from biomedical and clinical research [49] to the history of science [29] to activism [44], via diverse methods. Across dozens of case studies,

scholars have demonstrated its utility for understanding governance relative to privacy [43] and the adoption of new technologies [14]. Through questions that can be employed across contexts to understand the nature of knowledge or data as a resource and the mechanisms by which actors negotiate governance of those resources, interview and survey questions can be grounded in the theory and a codebook can be employed for analysis of governance documentation.

3 METHODS

We draw on the GKC framework to inform our multi-method investigation of the governance practices employed by higher education institutions with respect to LMS and third-party plugins or LTIs, as well as to structure analysis of results. Data collection involved three components:

(1) An online questionnaire about LMS, plugin, and LTI governance practices from IT professionals at seven universities in the United States (n=4) and Canada (n=3). The responses from these individuals helped us frame and design the interview schedule.
(2) A review of publicly-available online documentation from 112 universities about LMS plugin and LTI governance. 18 of these universities provide additional documentation, which we analyze in further depth.
(3) A series of extensive interviews with 25 university data governance officers with responsibilities for LMS, plugin, and/or LTI governance, representing 14 different universities.

3.1 Online Questionnaire

We created an online questionnaire to collect descriptions of LMS and plugin/LTI governance practices from IT professionals at four universities in the United States and three universities in Canada. This sample included five public research universities, one private research university, and one private liberal arts college. We recruited these individuals through our professional networks. The use of an online questionnaire was approved by the Institutional Review Boards (IRB) at all authors' universities. All respondents provided their informed consent and were were not monetarily compensated for their participation. The questionnaire contained the following sections:

(1) *Background.* Respondents were given background information on the research project, definitions of LMS, plugins, and LTIs, and instructions for taking the survey. The instructions specified that while LMS details are typically non-sensitive, respondents should not violate their university's procedures for reporting internal protocols.
(2) *LMS Adoption.* Respondents were asked to identify the LMS in use at their university and which individuals and units at their university are involved in the adoption of LMSs, plugins, or LTIs. Respondents then indicated whether their university develops plugins or LTIs internally.
(3) *Third-party Plugin Governance.* Respondents were asked to describe their university's procedures for deciding whether to adopt new LMS plugins/LTIs as well as any formal or informal security audits or privacy considerations performed prior to adopting new LMS plugins/LTIs. They were also asked to indicate the units at their university responsible for managing the adoption of new LMS plugins, performing security audits on new LMS plugins, and considering privacy implications of new LMS plugins.

(4) *LMS Challenges.* Finally, respondents described their university's process for addressing any problems or challenges that arise with LMS plugins or LTIs.

We manually reviewed the responses and present the results in Section 4. The data provide a glimpse into LMS/plugin/LTI governance in use at a range of universities.

3.2 Analysis of Publicly-Available Online Documentation

We identified a sample of 112 universities via US News categories: public (n=41), private and liberal arts (n=40), HBCU (n=7), community college (n=14), and Canada (n=10). These institutions reflect a spectrum of geographic, socioeconomic, and student population characteristics, as determined by the US Department of Education National Center for Education Statistics (NCES) and Universities Canada.

In order to understand the scope of LTI and LMS plugin usage and support at these universities, we collected lists of their LTIs and plugins at use via public university knowledge base websites. This information was scraped using Python and identified by keywords "Canvas," "Blackboard," "Moodle," "LTI," "plug-in," and "LMS." In addition to identifying which plugins or LTIs were used by these universities, we sought to determine the number of LTIs or plugins that are developed and supported by the universities locally, as well as the number of LTIs or plugins for which data was hosted locally. In order to identify these statistics and characteristics, we conducted content analysis of the scraped documentation. Throughout this process, we also sought to identify what information is provided to instructors who may want to add or request that their university support other LTIs or plugins. This provides insight into what entities at these universities are responsible for LMS, plugin, and LTI adoption and oversight and how transparent these processes are to instructors, students, and the public.

A majority of the coding was completed by one of the investigators and a student research assistant, identifying five qualitative codes: data localization, internal development, internal hosting, external data flows, and procedural transparency. All five codes merited high agreement and inter-rater reliability scores [51]. Inter-rater reliability was not assessed for counts of LTIs or plugins identified, given that this process was documentation, rather than interpretation.

A subset of 17 of these universities (14 in the USA, 3 in Canada) provided extensive additional information about their LMS and plugin/LTI governance practices on public websites. We focused on these universities for further analysis of practices and stakeholders based on the accessibility of this information.

Section 4.2 presents the findings from the document review portion of this study.

3.3 Interviews with University Data Governance Officers

Interviews were conducted with 25 university data governance officers with responsibilities or decision-making authority regarding LMS, LMS plugins, and/or LTIs at 14 different US universities. Participants volunteered to participate following a professional development workshop regarding data governance, in order to provide empirical support for future data governance in this domain and in recognition of the need to document governance challenges and progress over student data, assessment practices, and educational technology vendors. Respondents at 5 of these 14 universities consented to identify their institutions, while 9 preferred we not disclose their institutions, as they believe it would identify them or could lead to repercussions for their employment.

Table 1. Interview Schedule Indicating Relationships between Research Questions, Theoretical Framework, and Interview Questions

Research Question	GKC Framework Support	Interview Question
Who is responsible for data governance activities around LMSs in higher education?	Background	Can you tell me about your role at [your university]?
	Attributes, Background	How are you involved in LMS data governance?
	Attributes, Background	Are you involved in any other data governance practices or domains?
	Attributes	What other teams, units, or roles are involved in LMS data governance?
	Attributes	How do you engage with [those groups/people]?
What is the current state of governance over LMSs in higher education?	Governance	What are the rules on the books that impact LMS data at the federal level? State level? University level?
	Governance, Patterns and Outcomes	How do you implement those rules?
What is the current state of governance over LMS plugins, LTIs, etc.?	Governance	What rules are in place that impact plugins and LTIs that connect third parties to LMSs at your institution?
	Governance	What procedures are in place to make decisions regarding plugins and LTIs?
	Governance, Patterns and Outcomes	How are those decisions implemented?
What governance issues are unresolved in this domain?	Governance, Patterns and Outcomes	Are there any ongoing debates about LMS data on your campus?
	Governance, Patterns and Outcomes	What issues are unresolved about plugins, LTIs, and/or third parties?

Interviews lasted between 48 and 94 minutes. All interviews were conducted on Zoom, with transcripts auto-generated via closed-captions and lightly edited for clarity around names and acronyms, in particular, based upon investigator notes.

All were prefaced with a brief overview of research motivations, questions, and logistics. The interviews were semi-structured, with theoretically grounded questions developed from the descriptive GKC framework in order to address sub-components of our research questions. The sequence of interview questions was flexible, following the flow of responses and follow-up questions. Table 1 indicates which structured interview questions correspond with which research questions, as well as what aspects of the GKC framework provide conceptual grounding for their framing and subsequent interpretation of results.

3.4 Analysis of Results via the GKC Framework

Results from all three phases of data collection were analyzed through the lens of the GKC framework to surface action arenas around governance challenges that have not yet been resolved, as well as paths to

resolution. We specifically leverage the hierarchy of strategies, norms, and rules in order to understand norm formation and conflicts among governance mechanisms, including their relative enforcement.

4 RESULTS

This section presents our analysis of practices and governance of third-party integrations to university LMS. We document gaps in governance that promote privacy risks relative to third-party data flows and LMS integrations. The results are organized by data collection strategies, reflecting distinct approaches to triangulate insights to our research questions. Internally, results are structured according to the descriptive GKC framework (section 2.3). Contextual attributes and third-party practices are documented in section 4.2, addressing RQ1 in part and complimenting the online questionnaire. We further address the extent of third-party access to student data via LMS plug-ins and LTIs (RQ1) in section 4.2.2. Section 4.3 addresses issues of governance and transparency (RQ2 and RQ3); Section 4.3.4 provides further depth in exploring governance, transparency, and inequality patterns and outcomes.

4.1 Online Questionnaire

This section presents the results from an online questionnaire given to IT professionals at seven universities, as described in Section 3.1.

4.1.1 LMS Use, LMS Management, and Plugin/LTI Development. Seven IT professionals provided responses via our online questionnaire. Of their universities, three use Canvas and Moodle, two use Canvas, one uses Moodle, and one uses Brightspace. Six of the seven universities develop plugins/LTIs internally. All respondents reported that their Information Technology offices had at least partial responsibility for LMS management. Additional responsibility for LMS management was shared by Education Technology units (n=3), Centers for Teaching and Learning (n=2) and the Business Office (n=1).

4.1.2 Deciding Whether to Adopt a New Plugin/LTI. Four respondents reported that requests from faculty, instructors, or other campus community members initiate the process of adding a new plugin/LTI. These requests are considered in light of need, whether existing plugins/LTIs already provide similar functionality, and cost. For example,

> We start users with a request process. After the request is submitted they go through a review to see if we have any duplicative services that already perform the core functionality needed. If we do not have a service that does this we review if that tool can be purchased and at what cost. When cost or features/integration is complex we then consider [in house] development. (P6)

In some (but not all) cases, these requests are then audited according to an existing procedure. For example,

> [If the] plugin or LTI is identified as having a potential for a centrally supported tool, features and functionality are reviewed, [and it] goes through a Privacy and Security audit. Using the external tool instructors can set up their own LTI links – no process followed. (P3)

This distinction between plugins and LTIs was echoed by another respondent (P2), who described auditing for plugins accessible to the entire university while

> Instructors can install LTIs, if supported, within their course, thereby bypassing the request process. (P2)

One respondent noted an explicit preference for vended plugins/LTIs – considering the technical debt that could be incurred from custom development (P7).

One respondent indicated that their university did not have a specific strategy to decide whether to adopt new plugins/LTIs.

4.1.3 Strategies to Update Plugins/LTIs? Five respondents described straegies for updated plugins/LTIs. The most stringent approach involved a multi-year scheduled audit:

> We work with our governance group around when to require the next version of the LTI standard and we also review all LTIs every three years to review safety and security as well as confirming the tool still meets the specified functional needs. (P7)

Other approaches included always attempting to use the most up-to-date version of LTI integrations (P1 & P5), evaluating updates on a case-by-case basis depending on cost and use cases (P6), and evaluating updates in a staging environment to avoid "breaking the LMS" (P2).

Two respondents indicated that their university did not follow any specific protocol for updating plugins/LTIs. This poses clear security risks with privacy implications.

4.1.4 Security Audits Prior to Plugin/LTI Adoption. Three respondents indicated that their university collects extensive information from plugins/LTI vendors for security review before adoption. All three of these universities use the Higher Education Community Vendor Assessment Toolkit (HECVAT) form from EduCause [11] for this purpose.

One respondent reported that they "do a full security review including documenting all endpoint calls, the need for developer keys or not, with a strong preference toward scope dev keys" (P7). One respondent said that their university's IT department performed a security audit, and one respondent reported an audit involving a test of the plugin/LTI, but neither provided additional details.

One respondent indicated that their university did not have any rules regarding security auditing plugins/LTIs prior to adoption (P4).

4.1.5 Privacy Audits Prior to Plugin/LTI Adoption. Three respondents said that their security audits also included privacy considerations (P2, P3, P6). For example, one succinctly explained that "Privacy reviews are part of our third-party assessment security review process" (P6). Two respondents said that their privacy audit included legal considerations involving PIPEDA/FIPPA (P1), FERPA (P7), or the university's legal counsel (P5). One respondent indicated that their university did not have a clear strategy for privacy auditing plugins/LTIs prior to adoption (P4).

4.1.6 Addressing Plugin/LTI Issues. Five of seven respondents described their university's strategies for addressing problems or challenges with LMS plugins or LTIs. The responses suggest that a tiered approach is common, involving attempts to address the issue locally followed by collaboration with the plugin/LTI vendor. Standard troubleshooting approaches, such as checking for updates, temporarily removing misbehaving plugins/LTIs, and finding workarounds to reduce end-user impacts, were also reported. For example,

> If the issue is with a third-party plugin, we verify for updates. If there are no updates, we will try to fix ourselves and notify the plugin maintainer about our fix. If we cannot fix it for any reason, we notify the requester about the impossibility to fix. We try to find a work around for the user. (P2)
>
> Work with vendor or developer to address issues. If not possible, or not timely, remove plugin until addressed. In some instance, address with internal development. (P1)

One respondent reported a phased-deployment system in place to reduce LMS disruptions when new (potentially buggy) plugins/LTIs are added:

> Integrations are usually launched as limited pilot programs only for those users that request access so issues that arise have at most a limited impact and can be dealt with before more widespread University adoption. We also "dogfood" the plugins ourselves trying to anticipate any issues, but if/when issues arise, the IT LMS team takes over troubleshooting with the vendor or in-house team. (P5)

4.2 Analysis of Publicly-Available Online Documentation

This section presents our results from analyzing 112 universities' online documentation about LMS, plugins, and LTI, as described in Section 3.2.

4.2.1 Comparative Indicators of LTI and Plugin Prevalence. Across the 112 universities reviewed, Blackboard (n=47), Canvas (n=61), and Moodle (n=32) are the three most widely used LMS, while Brightspace (n=5), Compass (n=5), and Google Apps for Education (n=3) are much less pervasive. 28 universities currently support more than one LMS, some of which appear to be transitioning between two LMS, while others offer choices or allow individual departments, schools, or colleges to make LMS decisions, rather standardizing across the university.

94 of 112 universities provide online data on plugins and LTIs used, of which 65 publicly document which specific third parties and tools are available for use at their university and 29 provide summary statistics. Of those universities that do not provide these details, 17 of 18 are private and the other is Canadian (Edmonton University). On average, universities have 54 total plugins and LTIs available for instructors to integrate with course sites. 1208 unique plugins and LTIs were identified in total, with 771 developed by universities rather than third-parties. The most pervasively available third-party tools are: Proctorio, TurnItIn, Honorlock, GradeScope, CrowdMark, MindLinks, Digication, Kaltura, LinkedIn Learning, Pushback, Panopto, MatLab Grader, Perusall, YouTube, and ProctorU.

While the total number of plugins and LTIs at any given university is highly correlated with student population size (ρ=0.86), the endowment per student provides significant insight into whether those tools are locally developed and supported or integrate with third-party platforms. **Noah: Do we have specific data to support the endowment correlation?**

4.2.2 Governance of plugins and LTI. Table 2 summarizes which governance strategies are in place for plugins and LTI across 17 universities that provided extensive information about their LMS and plugin/LTI governance practices on public websites. The following paragraphs describe additional findings from the document review.

Table 2. Governance strategies involved in the LMS plug in approval processes across the examined universities

University	Country	LTI related policy	Review Request	Vetting Process	Asks to Inform Students	Includes Data Reuse	Discusses Copyright	Asks for the IMS Certificate	Discusses Internal Development	Mentions FERPA/FIPPA	Data Protection Agreement	Contractual Obligation	Security Assessment	Risk Assessment	Compliance Assessment	New Plugin Request Form
IU, Bloomington	USA	✓	✓	✓		✓	✓			✓						✓
MSU	USA	✓	✓	✓					✓						✓	✓
Northwestern	USA	✓	✓	✓					✓	✓	✓	✓				
Penn. State	USA	✓	✓	✓			✓		✓							✓
Purdue	USA	✓	✓	✓				✓	✓				✓			✓
Rutgers	USA	✓	✓	✓			✓		✓		✓				✓	
UIUC	USA	✓	✓	✓				✓	✓		✓		✓			✓
Iowa	USA	✓	✓	✓		✓	✓				✓					
UMGC	USA	✓	✓	✓		✓				✓		✓	✓			
UM-Dearborn	USA	✓	✓	✓						✓	✓			✓	✓	
UMN-Twin Cities	USA	✓	✓	✓									✓			✓
UWM	USA	✓	✓	✓				✓	✓	✓			✓			✓
UofT	Canada	✓	✓	✓								✓	✓	✓		✓
UCF	USA	✓	✓											✓		✓
Ohio State	USA		✓													
U Regina	Canada			✓									✓		✓	
UWaterloo	Canada			✓	✓	✓				✓						✓

Adoption. Most universities we reviewed require faculty or department/unit to submit a formal request for a new tool or plugin, which initiates a review to determine whether the plugin fulfills university requirements. Notably, with regards to adoption on new education technology (not specifically related to LMS plugins), University of Waterloo asks instructors to inform students about newly introduced data practices and provide opportunities to opt-out.

Security and compliance assessment. The assessment of the plugin includes evaluation of security, risks and compliance. Some universities, for example, Michigan State University and the University of Illinois at Urbana-Champaign, use certifications such as HECVAT [11] and SOC2 [16] questionnaires in their review. Other examples, like Penn State, require that all services are LTI 1.3 Advantaged Certified. As we pointed out in Section 2.2.3, these standardized questionnaires focus on identifying the (mainly security-related) information handling practices and third-party interactions.

A typical assessment involves several stakeholders such as IT departments, security or learning technology teams. Some universities involve vendors or service providers as part of assessment. For example, the University of Michigan-Dearborn asks vendors to complete an internal security-compliance questionnaire.

Similarly the University of Toronto performs an vendor security audit. In another example, Iowa State University also requests the vendor to provide relevant documentation to help with assessment.

Contractual obligation. Out 18 universities we examined in greater detail, 6 universities[1] require some form of contractual obligation, such as data protection agreement and/or Data Protection Addendum to approve a new plugin.

Universities[2] that do not have a contractual obligation requirement refer to existing regulation–such as the Family Educational Rights and Privacy Act (FERPA) in the US institutions and the Freedom of Information and Protection of Privacy Act (FIPPA) in Canada—as benchmark for privacy assessment. Several universities, such as Universities of Indiana, Iowa, and Maryland, include additional assessment criteria regarding copyright infringement of student work and potential reuse of students data by the vendor for their own purposes.

Internally developed plugins. Internally developed plugins do not go through the same scrutiny. For example, at the University of Wisconsin, strategies vary based on the intended data sharing practices. If the new service solely interacts with local university services, it is approved by the default. However, in cases when the new service shares data with services that are not maintained by the university recognized development groups, it will require further vetting. Examples of additional internal plugin vetting policy, such as used in Rutgers University, include asking developers to explicitly state the scope and permissions before the new plugin is developed.

4.3 Interviews with University Data Governance Officers

This section presents our results from interviewing 25 university data governance officers with responsibilities or decision-making authority regarding LMS, plugins, and/or LTIs at 14 different US universities, as described in Section 3.3. Table 3 summarizes the governance strategies reported by the interviewees. The following sections provide a more detailed analysis of the interview reports.

Table 3. Counts of LMS, plugin, and LTI governance strategies reported by interviewed university data governance officers.

Governance Strategy	Count
Formal policy	12
Decentralized adoption	11
Legal review	10
Faculty governance	8
Formal decision-making protocol	7
Technical evaluation	6
Governance coordination mechanisms	3
Impact assessment	2
Training programs	2

[1]Michigan State University, Northwestern University, University of Illinois at Urbana-Champaign, University of Maryland College Park, University of Wisconsin Madison, University of Toronto
[2]Indiana Bloomington, University of Pennsylvania, University of Iowa, University of Michigan Dearborn, University of Nebraska Lincoln, University of Waterloo

4.3.1 Decision-Making Roles and Disagreement Among Responsible Units. Answers in response to questions about participants' roles and "what other teams, units, or roles are involved in LMS data governance" illustrated the complexity regarding decision-making in this arena. Based on responses from all 25 interviewees, we find that the following units have some say in this process: university IT (n=14), legal departments (n=14), faculty governance via committee or full senate (n=13), individual departments or colleges (n=12), campus center for teaching or educational innovation (n=7), the Provost's office (n=6), a Dean of Students or equivalent office with authority over student affairs (n=5), privacy and/or security offices independent from IT (n=3), procurement (n=2), and individual instructors (n=1). As such, a major challenge recognized by these professionals is that of coordination between units and reconciliation of their differences in opinion.

Respondents from 9 of 14 universities emphasized a general lack of understanding at university level about privacy issues, coordination problems around educational technology decisions, and third-party data flows. While they were concerned about privacy, security, and control issues around student data, many (18 of 25) respondents indicated that their concerns were not shared by other decision-makers. They spoke about how other priorities overtook the general focus in discussion of educational technology broadly, and LMSs specifically, as well as how raising these coordination problems often went unheard. In many of these cases, other values seem to supersede privacy concerns; "there is no interest in streamlining or, on the other hand, students' interests here" one explained. Another participant described, "I can't speak to anywhere else, but here, convenience is king. If an instructor requests something and justifies that with how 'easy' or 'free' or 'simple' it will be, in all likelihood, they're going to get it. And that only got worse with COVID."

4.3.2 Models for Governance Coordination and Emerging Norms. In contrast to all 11 universities that worried about dysfunction, 3 universities stood in contrast, albeit with three different coordination strategies. The only respondent at one university explained that they were the sole person with data governance responsibility at their institution, "which is ridiculous because of course I can't do this all alone and of course other people also do relevant work, but still I'm in an office on my own, trying to be all of the coordination at once." This participant requested that we not identify their institution. In a discussion with two participants at the University of Illinois, one explained "Consolidation and consistency are much more important in campus level discussions right now as we move to one LMS and one central group managing everything, including the LTI issues you asked about."

The University of Michigan also particularly stood out, describing a functional system of coordination without onerous bureaucracy. They had developed clear decision-making tools for individual units that allowed for consistency, without lengthy approval procedures. The guidelines they developed, reflected community norms, state and federal laws, technical standards, and local infrastructural constraints and supports. Upon approval of an individual LTI or plug-in, the completed decision making form would be shared centrally, for verification and transparency, as a reference for the university community and other units that may wish to use something approved elsewhere on campus. Notably, as a participant at Michigan explained "Our current approach to educational data governance and learning analytics did not emerge out of no where. It took years of planning, revision, and really forward-thinking leadership. Without someone in power caring, this never would have happened."

In contrast to many other the institutions that expressed frustration with the dysfunction they experienced, participants at Illinois and Michigan described a positive outlook for data governance with respect to LMSs

at their institutions, and the ways in which they served in leadership roles for broader communities of universities, including peer institutions, HBCUs, and HSIs. As one participant said "I care enough to want to figure out how to do this right, not just to fix things for now. I'm lucky to have support to spend time on these issues and share my expertise with others at conference and via training modules I develop." This facilitates the emergence of specific norms, as well as a broader knowledge commons in which professionals share and govern relevant information, as they learn.

Peer institutions that participated in interviews themselves emphasized hoping to learn from others about how to successfully streamline decisions, more so than normative best outcomes. They wanted to understand logistics and how others had established order, oversight, and coordination.

4.3.3 Ongoing Challenges in LMS and LTI Governance. Ongoing governance challenges described by interviewees included: coordination problems among units, inadequate legal protections at the state and federal levels, confusion about protocols, university politics, and the non-transparent practices of the third-parties developing LTIs and plugins. This section illustrates examples of all of these issues, as well as some of their interrelationships.

Notably, some of the coordination problems stem not only from multiple departments with oversight, but also from policies that address the type of contractual and financial obligations that apply to an LTI or third-party plugin, rather than the category of technology. At one university, a participant explained "Our processes are more of a relic than anything else and we just can't escape it. If an LTI is free, the finance office doesn't care at all; if it's not, it gets a lot of scrutiny. If the license is education specific, legal says that box is checked and doesn't look any further. Then it only gets a tech review. But lots of these cost money, require negotiating a license, and need security, privacy, whatever." Their colleague contextualized further, "in our state, privacy laws, you asked about those, really only apply to K-12, so at our level, we're just looking at federal, basic consumer... That's really why legal is so hands off on this. They're more intense with other liability things, discrimination especially."

A participant from another university echoed this, emphasizing confusion over who had say and when multiple forms of approval were needed. "Everything here has some legal, technical, and faculty oversight, but if certified or with the right license by default, as with many ed-tech specific tools, you know not YouTube, but TurnItIn, whoever is adopting can just sort of self-certify. There's no real order or central place to log this. We have a lot of things adopted with only partial approval. The thing most skipped is the Faculty Senate committee on Technology Adoption, no one wants to deal with the politics, but it's almost worse when it comes out, you know? It might slide under the radar, but it might be that the Business School decided to use Proctorio without taking it to a vote and then you get a student protest and 'Bam.' It's a huge mess and a lot of finger pointing."

Participants from 6 different institutions discussed the governance challenges associated with actually reviewing LTIs and plugins, discussing issues of proprietary algorithms, secrecy, and ambiguity around functions. One respondent summarized the challenge in these terms: "How are we supposed to make a choice without anything more than a sales pitch? I'm supposed to tell the university if something is sound from a privacy and security POV, but all I have are words. No one wants to let me look at the code." Another expanded to tie this to differences in values: "The more of a black box something is, the more I scrutinize, honestly. An endless list of proctoring plugins and every last one is not about assessment or real teaching

needs, they're about covering their ***** during lockdown. It's all we own this, we can't tell you more. That difference is about more that money, it also about secrets as power and criminal justice logic that's spreading in education technology, or really technology everywhere. All surveillance, all the time."

4.3.4 Governance Patterns and Outcomes. While governance processes vary considerably, with few institutions leading in this space, some patterns are beginning to emerge around communication regarding plugins and LTIs, especially at public institutions.

Thus, one key distinctive pattern emerges around the degree of transparency surrounding governance and third-party data flows around LMSs as intersects with the public-private divide. While public universities must provide public-facing documentation, there are no requirements or incentives for private universities to be as forthcoming; typically, private universities provided, at most, guides for their instructors to consider available supported tools and links for further requests on plugins, or else, at least, nothing. In contrast, most public universities provide significant documentation in their knowledge bases, which may not be easily findable by the average student, instructor, or member of the public without some idea of what to search for but are public facing. This may still fall short of data governance transparency values but does provide interpretable records. As one interview participant explained, "I have a rough sense of what people on campus want, and while that's different from student to instructor, we're not providing any of the right information outside of the knowledge base articles. But, those are underused. There's a group of staff and some professors of a certain age, but outside that, people don't know what we provide there." Better publicity around these resources could solve some awareness problems.

A second key pattern that emerges centers around inequality and privacy protections. Not only do economic factors play a role in the imbalance in third-party flows, with less affluent universities depending to a greater extent on "free" integrations, but also the comparative endowment per student corresponds with local support, documentation, and oversight. Thus, community college students, for example, are not only more likely to have third-parties collecting their data via LMS integrations, they are unlikely to find documentation around these practices or know who to turn to in order to ask questions about data governance.

It is notable that some of the more privileged institutions recognize this chasm, with their LMS experts offering workshops and knowledge resources to other institutions, so that all students can benefit from more privacy protecting LMS configurations. As one learning technology specialist at a public university with a relatively high endowment per student stated, "it's not just kids at [my university] that should benefit from this; students should not constantly be documented and monetized by textbook, social media, and "anti-cheating" integrations! LinkedIn and YouTube don't need this data; it's very simple to build around it... I convinced [their boss] to let me offer a workshop to teach how easy and lightweight this is. We had 23 universities attend the first round, with 7 community colleges, 3 HBCUs, 2 HSIs. It was great."

The status quo of LMS governance relative to student data and third parties is one in which "the vendors are leading! They sell people things at conferences, convince faculty they need something, and we're always in a rush to make it happen, at the expense of scrutiny." Yet 12 of 14 interviewed institutions emphasized that they are starting to push back, based on the successes of data localization, on-campus development of features that don't require exogenous data sharing, and DPAs at peer institutions, such as the University of Michigan and the University of Illinois. As one center director of Innovative Education explained, "it's

really hard to do this right, especially as I'm a part of a larger university system in my state that usually wants things done consistently, but I have to the contrarian, because making better choices for students not for-profit developers is the right thing to do."

5 DISCUSSION

The interviews and the content analysis reveal several governance issues that require examination and suggest preliminary recommendations.

5.1 Privacy Threats and Challenges

The rapid transition to online LMS systems introduced unprecedented levels of information complexity to existing educational governance institutions. While universities attempt to meet the challenge with revised review processes of newly introduced tools, they are often outmatched by new digital threats. This problem is especially acute when it comes to supporting a large ecosystem of data-hungry third-party plugins and integrations that can have direct access to LMS data.

Evaluating specific examples of governance and status quo arrangements around LTIs and LMSs, we see that student privacy is being overlooked, ignored, and, in some cases, intentionally sacrificed. Tradeoffs between privacy and efficiency made under emergency pandemic circumstances have amplified the situation, yet other non-privacy related tradeoffs, such as between authority and control with time, lead non-normative strategies and rules. Tradeoffs have also been made that de-prioritize privacy in favor of surveillance over students, justified as critical to academic integrity, yet following carceral logics rather than pedagogical arguments, as discussed by participants regarding value divergence between educational intuitions and vendors. As decisions are made to prioritize convenience, cost or control over the interests of student privacy, significant third-party data sharing with commercial actors ensues.

5.2 Fragmented Governance

To the untrained eye, educational institutions portray competence and systematization. Our analysis, however, indicates a state of fragmented and dysfunctional governance based on outdated regulation and review processes. It is unclear who is in charge. The lack of expertise forces some universities to outsource the risk assessment of new tools to external partners and the use of standardized questionnaires. Furthermore, the increased complexity requires involvement of many institutional stakeholders such as finance, procurement, IT and other units which further complicates and delays reviews. In some cases, the governance processes simply break down. Third-party services can be integrated with little oversight. In cases where a formal review process exists, it is generally designed for evaluating new tools and platforms, with little attention given to third-party integrations.

5.3 Recommendations

Building on the emerging norms and patterns of strategies and practices recognized by interview participants and integrating other suggestions and needs, this section provides recommendations for governance of LMS and integrations moving forward.

An effective means to improve governance and privacy outcomes in this space is to engage with the emerging knowledge commons via collective production efforts for LTI and LMS governance frameworks;

those universities that saw tentative successes in governance aim to do this already, and other interview participants recognized and appreciated their efforts. Professionals in higher education data governance connect with one another via professional development opportunities, conferences, formal networks within academic conferences, and training opportunities. Through these connections, knowledge about successes and failures in governing student data flows and decision-making about third-party services and tools is co-produced with the community, reflecting an emerging knowledge commons, reflecting the co-creation of a community of practitioners and the knowledge needed to appropriately manage and govern technology under their purview. These opportunities and activities are very efficient investments at a time of limited resources and high demands on decision-makers' time, as they provide a knowledge network to draw upon in making decisions.

Beyond the information they might gain about particular decisions or specific LTIs, what multiple respondents viewed as most valuable is learning how other universities have successfully implemented streamlined decision-making processes that reflect community norms, protect student privacy, and can be operationalized without significant challenges. They wanted to be able to benchmark and learn from one another.Examples of such successes include: consistency in decision making criteria via descriptive governance frameworks, clear processes for coordination amongst units, and transparency about what has already been approved and is in place, to avoid replication across colleges and departments.

In contrast with various other established privacy trade offs playing out in this action arena, transparency seems to enhance privacy in many cases. Both transparency over decision-making processes and transparency about what LTIs and plugins are in use seem to support fewer local privacy controversies at many of the universities in the study. Universities that are more open, consistent, and clear about data practices, governance, and data flows can serve as models, not only through formal training modules and governance frameworks, but also in providing transparent, replicable best practices.

Governance mechanisms, including feedback opportunities to support community members' voices, documentation of governance, consistent oversight, and coordination among decision-makers, should institutionalize along the hierarchy, starting with intentional strategies that are crowdsourced, discussed, shared with other universities and tested in multiple contexts in order for norms to emerge and coalesce. Rules must build on these norms with meaningful penalties for violations or other approaches to enforcement. Further, our results suggest that more clarity is needed for students and instructors about privacy and practices of third parties. Further, investing and expanding data governance professional development may enhance the ability of decision-makers to communicate across departments and units, reflecting an interdisciplinary perspective.

6 CONCLUSION

We analyzed the governance institutions and practices of higher education institutions with respect to learning management systems (LMS) and associated plugins and LTIs. Our results indicate a portrait of fragmented and unobtrusive, unnoticed student information flows to third parties. From coordination problems on individual college campuses to disparate distributions of authority across campuses, as well as from significant data collection via individual LTIs to a shared problem of scope across many LTIs, we see that increased and intentional governance is needed to improve the state of student privacy and provide transparency in the complex environment around LMSs. Yet we also see that there are logical

paths forward based on successful governance and leveraging existing collaborative networks among data governance professionals in higher education.

REFERENCES

[1] M. Alier, M.J. Casañ Guerrero, D. Amo, C. Severance, and D. Fonseca. 2021. Privacy and E-Learning: A Pending Task. *Sustainability (Switzerland)* 13, 16 (2021). https://doi.org/10.3390/su13169206

[2] Mark Andrejevic and Neil Selwyn. 2020. Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology* 45, 2 (2020), 115–128.

[3] Karla Badillo-Urquiola, Yaxing Yao, Oshrat Ayalon, Bart Knijnenurg, Xinru Page, Eran Toch, Yang Wang, and Pamela J. Wisniewski. 2018. Privacy in Context: Critically Engaging with Theory to Guide Privacy Research and Design. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Jersey City, NJ, USA) *(CSCW '18)*. Association for Computing Machinery, New York, NY, USA, 425–431. https://doi.org/10.1145/3272973.3273012

[4] Veronica Barassi. 2020. *Child data citizen: How tech companies are profiling us from before birth*. MIT Press.

[5] Michael Brown and Carrie Klein. 2020. Whose Data? Which Rights? Whose Power? A Policy Discourse Analysis of Student Privacy Policy Documents. *The Journal of Higher Education* 91, 7 (2020), 1149–1178. https://doi.org/10.1080/00221546.2020.1770045 arXiv:https://doi.org/10.1080/00221546.2020.1770045

[6] Ben Burgess, Avi Ginsberg, Edward W Felten, and Shaanan Cohney. 2022. Watching the watchers: bias and vulnerability in remote proctoring software. *arXiv preprint arXiv:2205.03009* (2022).

[7] Shaanan Cohney, Ross Teixeira, Anne Kohlbrenner, Arvind Narayanan, Mihir Kshirsagar, Yan Shvartzshnaider, and Madelyn Sanfilippo. 2021. Virtual Classrooms and Real Harms: Remote Learning at {US}. Universities. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 653–674.

[8] MS Global Learning Consortium. 2022. The TrustEd Apps rubric. https://www.imsglobal.org/activity/trustedapps/rubric.

[9] Sue E Crawford and Elinor Ostrom. 1995. A Grammar of Institutions. *American Political Science Review* 89, 3 (1995), 582–600.

[10] EDUCAUSE. 2022. About HEISC. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/about-heisc.

[11] EDUCAUSE. 2022. Higher Education Community Vendor Assessment Toolkit. https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit.

[12] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. 2018. The Influence of Friends and Experts on Privacy Decision Making in IoT Scenarios. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 48.

[13] Tobias Fiebig, Seda Gürses, Carlos H Gañán, Erna Kotkamp, Fernando Kuipers, Martina Lindorfer, Menghua Prisse, and Taritha Sari. 2021. Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds. *arXiv preprint arXiv:2104.09462* (2021).

[14] Brett M Frischmann, Michael J Madison, and Madelyn Rose Sanfilippo. 2023. *Governing smart cities as knowledge commons*. Cambridge University Press.

[15] Christian Fuchs. 2011. Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society* (2011).

[16] Imperva. 2023. SOC 2 Compliance. https://www.imperva.com/learn/data-security/soc-2-compliance/.

[17] Juliane Jarke and Andreas Breiter. 2019. The datafication of education. *Learning, Media and Technology* 44, 1 (2019), 1–6.

[18] Kyle Jones, Amy VanScoy, Kawanna Bright, and Alison Harding. 2021. Do They Even Care? Measuring Instructor Value of Student Privacy in the Context of Learning Analytics. (2021).

[19] Kyle ML Jones, Andrew Asher, Abigail Goben, Michael R Perry, Dorothea Salo, Kristin A Briney, and M Brooke Robertshaw. 2020. "We're being tracked at all times": Student perspectives of their privacy in relation to learning analytics in higher education. *Journal of the Association for Information Science and Technology* 71, 9 (2020), 1044–1059.

[20] Kyle ML Jones and Chase McCoy. 2021. Privacy in Practice. *Governing Privacy in Knowledge Commons* (2021), 98.

[21] Kyle ML Jones, Alan Rubel, and Ellen LeClere. 2020. A matter of trust: Higher education institutions as information fiduciaries in an age of educational data mining and learning analytics. *Journal of the Association for Information Science and Technology* 71, 10 (2020), 1227–1241.

[22] Kyle M. L. Jones, Andrew Asher, Abigail Goben, Michael R. Perry, Dorothea Salo, Kristin A. Briney, and M. Brooke Robertshaw. 2020. "We're Being Tracked at All Times": Student Perspectives of Their Privacy in Relation to Learning Analytics in Higher Education. *Journal of the Association for Information Science and Technology* 71, 9 (2020), 1044–1059. https://doi.org/10.1002/asi.24358

[23] Kyle M. L. Jones and Chase Mccoy. 2018. Reconsidering data in learning analytics: opportunities for critical research using a documentation studies framework. *Learning, Media and Technology* 44, 1 (Dec 2018), 52–63. https://doi.org/10.1080/17439884.2018.1556216

[24] Negar Khojasteh, Cathy Liu, and Susan R. Fussell. 2019. Understanding Undergraduate Students' Experiences of Telepresence Robots on Campus. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing* (Austin, TX, USA) *(CSCW '19)*. Association for Computing Machinery, New York, NY, USA, 241–246. https://doi.org/10.1145/3311957.3359450

[25] Janja Komljenovic. 2022. The future of value in digitalised higher education: why data privacy should not be our biggest concern. *Higher Education* 83, 1 (2022), 119–135.

[26] Priya C Kumar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2019. Privacy and security considerations for digital technology use in elementary schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[27] Yuan Li. 2011. Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems* 28, 1 (2011), 28.

[28] Chen Ling, Utkucan Balcı, Jeremy Blackburn, and Gianluca Stringhini. 2020. A first look at zoombombing. *arXiv preprint arXiv:2009.03822* (2020).

[29] Michael J Madison. 2021. The Republic of Letters and the Origins of Scientific Knowledge Commons. *Governing Privacy in Knowledge Commons* (2021), 151.

[30] Michael J Madison, Brett M Frischmann, and Katherine J Strandburg. 2009. The university as constructed cultural commons. *Wash. UJL & Pol'y* 30 (2009), 365.

[31] Katie Miller. 2020. A matter of perspective: Discrimination, bias, and inequality in ai. In *Legal Regulations, Implications, and Issues Surrounding Digital Data*. IGI Global, 182–202.

[32] Helen Nissenbaum. 2009. *Privacy in context: technology, policy, and the integrity of social life*. Stanford Law Books.

[33] Office of the Privacy Commissioner of Canada. 2022. OPC Privacy Complaint report. https://www.canlii.org/en/on/onipc/doc/2022/2022canlii9040/2022canlii9040.html.

[34] Elinor Ostrom. 1990. *Governing the commons: the evolution of institutions for collective action*. Cambridge University Press.

[35] Hakan Ozalp, Pinar Ozcan, Dize Dinckol, Markos Zachariadis, and Annabelle Gawer. 2022. "Digital Colonization" of Highly Regulated Industries: An Analysis of Big Tech Platforms' Entry into Health Care and Education. *California Management Review* (2022), 00081256221094307.

[36] Britt Paris, Rebecca Reynolds, and Catherine McGowan. 2022. Sins of Omission: Critical Informatics Perspectives on Privacy in E-learning Systems in Higher Education. *Journal of the Association for Information Science and Technology* 73, 5 (May 2022), 708–725. https://doi.org/10.1002/asi.24575

[37] Priscilla M Regan and Jolene Jesse. 2019. Ethical challenges of edtech, big data and personalized learning: Twenty-first century student sorting and tracking. *Ethics and Information Technology* 21, 3 (2019), 167–179.

[38] Joel R Reidenberg and Florian Schaub. 2018. Achieving big data privacy in education. *Theory and Research in Education* 16, 3 (2018), 263–279.

[39] Dalia Ritvo, Christopher Bavitz, Ritu Gupta, and Irina Oberman. 2013. Privacy and Children's Data-An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act. *Berkman Center Research Publication* 23 (2013).

[40] Juan Carlos Rodríguez-del Pino, Enrique Rubio Royo, and Zenón Hernández Figueroa. 2012. A Virtual Programming Lab for Moodle with automatic assessment and anti-plagiarism features. (2012).

[41] Alan Rubel and Kyle ML Jones. 2016. Student privacy in learning analytics: An information ethics perspective. *The information society* 32, 2 (2016), 143–159.

[42] Madelyn R Sanfilippo, Brett M Frischmann, and Katherine J Strandburg. 2018. Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework. *Journal Information Policy* 8 (2018), 116–166. https://doi.org/10.5325/jinfopoli.8.2018.0116

[43] Madelyn Rose Sanfilippo, Brett M Frischmann, and Katherine J Strandburg. 2021. *Governing Privacy in Knowledge Commons*. Cambridge University Press.

[44] Madelyn Rose Sanfilippo and Katherine J. Strandburg. 2019. Privacy Governing Knowledge in Public Facebook Groups for Political Activism. *Information, Communication & Society* (2019). https://doi.org/10.1080/1369118X.2019.1668458

[45] Yan Shvartzshnaider, Madelyn Rose Sanfilippo, and Noah Apthorpe. 2022. GKC-CI: A unifying framework for contextual norms and information governance. *Journal of the Association for Information Science and Technology* (2022).
[46] Sharon Slade and Paul Prinsloo. 2013. Learning Analytics: Ethical Issues and Dilemmas. *American Behavioral Scientist* 57, 10 (Oct. 2013), 1510–1529. https://doi.org/10.1177/0002764213479366
[47] Laura Smithers. 2023. Predictive analytics and the creation of the permanent present. *Learning, Media and Technology* 48, 1 (2023), 109–121.
[48] Enno Steinbrink, Lilian Reichert, Michelle Mende, and Christian Reuter. 2021. Digital Privacy Perceptions of Asylum Seekers in Germany: An Empirical Study about Smartphone Usage during the Flight. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–24.
[49] Katherine J Strandburg, Brett M Frischmann, and Michael J Madison. 2017. *Governing medical knowledge commons*. Cambridge University Press.
[50] Michael Thomas. 2011. *Digital education: Opportunities for social collaboration*. Springer.
[51] Howard EA Tinsley and David J Weiss. 2000. Interrater reliability and agreement. In *Handbook of applied multivariate statistics and mathematical modeling*. Elsevier, 95–124.
[52] Peter Samuelson Wardrip, R. Benjamin Shapiro, Andrea Forte, Spiro Maroulis, Karen Brennan, and Ricarose Roque. 2013. CSCW and Education: Viewing Education as a Site of Work Practice. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work Companion* (San Antonio, Texas, USA) *(CSCW '13)*. Association for Computing Machinery, New York, NY, USA, 333–336. https://doi.org/10.1145/2441955.2442035
[53] Website. 2022. Crowdmark. https://crowdmark.com/help/how-does-crowdmark-work-with-moodle/.
[54] Website. 2022. Learning Tools Interoperability Core Specification. https://www.imsglobal.org/spec/lti/v1p3/.
[55] Website. 2022. Moodle Privacy API. https://docs.moodle.org/dev/Privacy_API.
[56] Website. 2022. Turnitin. https://www.turnitin.com/.
[57] Elana Zeide. 2017. The structural consequences of big data-driven education. *Big Data* 5, 2 (2017), 164–172.
[58] Elana Zeide and Helen Nissenbaum. 2018. Learner Privacy in MOOCs and Virtual Education. *Theory and Research in Education* 16, 3 (2018), 280–307. https://doi.org/10.1177/1477878518815340

Comments From	Comment	Our Response
Guest Editor	After carefully reviewing their notes and recommendations, I have decided to evaluate this submission as fitting the “Minor Revision” category. Please review the words of the reviewers, make appropriate edits, and document your edits in a letter/spreadsheet that replies to the suggested revisions (those which you attend to and those you decide to ignore). Return the letter and the revised paper by August 15th, 2023 in the submission system. Because we are trying to facilitate timely publication of manuscripts submitted to the journal, Information and Learning Sciences, your revised manuscript should be uploaded as soon as possible. If it is not possible for you to submit your revision in a reasonable amount of time, we may have to consider your paper as a new submission.	We thank you and the reviewers' for their feedback and are happy to make minor revisions based on comments and questions. We appreciate the suggestions and believe that they have helped us to clarify and improve our manuscript.
	Reviewer #1 was positive and constructive in their review. I highly recommend carefully reading their “Comments to the Author” notes. I emphasize for your consideration their remarks about:	We are happy to address their constructive comments
	More focused attention on the ”…political economy of higher education in North America…,” but only if you find that these focus is 1) doable given the revision timeframe and 2) does not overly limit the potential impact of your work to a non-North American audience.	We appreciate this suggestion to contextualize. We have added some background on the modern political economy of educational technology and the emerging market around "learning loss," with emphasis on North America and some comparison to other markets.
	Many excellent references are provided by Reviewer #1, which could add depth to your findings and discussion when strategically used. Take these into consideration.	We greatly appreciate these suggestions. We have incorporated the references from ...

	Consider the comment: “I wonder if the reader might benefit from a focus on one or two of the emerging themes that would allow you to dig deeper into some of the nuance and complexity of the findings within and between institutions.” Deeper detailed analysis is always welcome instead of shallow and wide coverage—in my opinion. See what you can do here.	We have revised our discussion of emerging themes, in response to this comment. We appreciate the recommendation to provide more depth; rather than limiting our discussion to one or two, we provide examples and implications for each, leveraging the list as structure.
	Reviewer #2, like Reviewer #1, was equally positive about your work, noting: “The paper has a great story to tell and one that needs to be told.”	Thank you.
	Like with Reviewer #1, Reviewer #2 noted that “Reliance on the concept and lit of "knowledge commons" may need better scaffolding, especially given the idea's prominence in the paper's orientation. Providing such scaffolding will help more readers understand the value of the paper and the investigation it reports.” You are deep experts in GKC, but remember that your readers are not. To convince them of the value and relevance of GKC elements, the onus is on you to make the parts of GKC intelligible. As hard as this may be, simplify GKC language to make it more approachable where you can.	It is very helpful to know where we were unclear or too brief; we have edited to provide more illustrative examples and clarity.
	Reviewer #2 provides notes in the “Quality of Communication” section, which I urge you to take into consideration.	Thank you. We have edited end to end for clarity and accessibility.
Referee 1	This is an intriguing, timely, and wide-ranging article with a strong empirical basis. I believe the manuscript could be advanced towards publication by a consideration of the following:	We appreciate your comments and hope the revisions address.
	• Given the specific focus on post-secondary education and the nature of the framework, I had expected more of a focus on the political economy of higher education in North America- both as part of the review of the literature and within the findings and discussion. Right now, there’s an emphasis on technological problems and explanations, but part of what you observer are organizational problems and arrangements. For example, the ‘wealthier’ orgs have a trickle down effect sounds like stratification and mimetic isomorphism. There’s a substantial literature that illustrates mechanisms for how mimetic isomorphism drives organizational change in higher education.	We greatly appreciate these suggestions. The revised manuscript does provide significantly more background on the political economy of educational technology, especially emphasizing the emerging "learning loss" market that has shaped so many third party data flows.

• In terms of the literature, I think you could consider some of the following pieces which frame and add complexity to the argument you are making. I believe they also give sensitizing concepts that could advance your analysis. Much of your findings are reflected in this earlier work, so by building off this work you can maybe narrow the wide ranging discussion and add more explicit nuance to your discussion (which, while well supported is quite broad in the assertions you make).	Thank you for the suggested references. After reading through these papers, we found many of them to be applicable and have referenced them as follows:
• I think the Komljemnovic and the Brown articles are particularly worth engaging with as the former encourages us to think beyond just privacy and the Brown article did the student facing version of your analysis (and found strikingly similar results which adds weight to your argument).	We agree; thank you for the suggestion.
Brown, M., & Klein, C. (2020). Whose data? Which rights? Whose power? A policy discourse analysis of student privacy policy documents. The Journal of Higher Education, 91(7), 1149–1178. https://doi.org/10.1080/00221546.2020.1770045	This work is very relevant and we have included it in the background.
Komljenovic, J. (2020). The future of value in digitalized higher education: Why data privacy should not be our biggest concern. Higher Education, 83(1), 119–135. https://doi.org/10. 1007/s10734-020-00639-7 Lattuca, L., & Brown, M. (2023	This paper is also now cited, helping us to contextualize the significant of this project and the need for future directions.
Smithers, L. (2023). Predictive analytics and the creation of the permanent present. Learning, Media and Technology, 48(1), 109–121. https://doi.org/10.1080/17439884.2022.2036757 (This one might not of been published when you were drafting the article, admittedly!)	We have also cited this paper to help provide mor background on learning analytics.
Taylor, L. D., Jr. (2020). Neoliberal consequence: Data-driven decision making and the subversion of student success efforts. The Review of Higher Education, 43(4), 1069–1097. https:// doi.org/10. 1353/rhe.2020.0031	This paper is very interesting, but does not clearly align with our paper, especially as revised.
Whitman, M. (2020). “We called that a behavior”: The making of institutional data. Big Data & Society, 7 (1), 205395172093220. https://doi.org/10.1177/2053951720932200	Again, an interesting paper, but somewhat misaligned with our approach to institutional theory, as opposed to universities as institutions.

• With the GKC, I think you could extend your organizational analysis by emphasizing what institutional attributes you either focused on or observed in your study. The current approach, including your questions, seems to emphasize the individual. That's fine, but it doesn't align with your research questions. Explaining more clearly for the reader how our knowledge of the individual illuminates the organizational would help the reader follow the logic of your inquiry (the table was very helpful in this regard).	We have aimed in our revisions to better explain both the GKC framework and how we have leveraged it to identify the strategies, norms, and rules that guide governance of LTI and plugin adoption.
• Similarly, I'd like to see you engage a little bit more with the policy environment beyond the LTI specific solutions you've identified. What role does FERPA play in this context for the US institutions?	This suggestion really resonated. We have engaged deeply with this question in another article and are happy to address via cross referencing to that paper; we identify that as an "author citation" in revisions and can unblind for publication.
• The current manuscript provides lots of high level summary, in part because you cover so much territory with your research questions and data. I wonder if the reader might benefit from a focus on one or two of the emerging themes that would allow you to dig deeper into some of the nuance and complexity of the findings within and between institutions.	We appreciate this suggestion and hope that some of the additional examples help to clarify and deepen understanding of key themes. We do believe comparisions between institutions would provide a very different paper and may serve to identfy some of our respondents who participated on the premise that their university would not be named.

• The magnitude reporting “e.g. “Respondents from many universities (n=9) emphasized a general lack of understanding at university level about privacy issues, coordination problems around educational technology decisions, and third-party data flows” is less convincing than the description of the nuanced organizational arrangements that resulted. For example, how did Michigan get to its effective process?	In our revisions, we sought to balance more explanation with the aggregation via magnitude reporting, given that some respondents did not agree to identification of their university.
• Some terms are used without clarification. What’s the emerging knowledge commons?	We have defined emerging knowledge commons and hope all concepts are more clearly defined upon revision.
Additional Questions:	
Originality: Does the paper contain new and significant information adequate to justify publication?: The paper has some distinctive and original findings, but would benefit from a narrower focus with greater depth and an engagement with the existing literature on privacy in HGED.	Our revisions have clarified our scope and aimed to provide more depth via examples. Our expanded background section does now connect to the suggested literature
Originality: Does the paper contain new and significant information adequate to justify publication?: The paper has some distinctive and original findings, but would benefit from a narrower focus with greater depth and an engagement with the existing literature on privacy in HGED.	
Methodology: Is the paper's argument built on an appropriate base of theory, concepts, or other ideas? Has the research or equivalent intellectual work on which the paper is based been well designed? Are the methods employed appropriate?: See comments to the author. No major concerns.	We are glad the original methodology was appropriate and clear.
Results: Are results presented clearly and analysed appropriately? Do the conclusions adequately tie together the other elements of the paper?: See comments to the author. The results would benefit from a deeper focus on one or two themes rather than the wide ranging approach the authors use. In its current form, there is a greater deal of data, but a lack of depth and specificity.	We have revised our discussion of emerging themes, in response to this comment. We appreciate the recommendation to provide more depth; rather than limiting our discussion to one or two, we provide examples and implications for each, leveraging the list as structure.

	Implications for research, practice and/or society: Does the paper identify clearly any implications for research, practice and/or society? Does the paper bridge the gap between theory and practice? How can the research be used in practice (economic and commercial impact), in teaching, to influence public policy, in research (contributing to the body of knowledge)? What is the impact upon society (influencing public attitudes, affecting quality of life)? Are these implications consistent with the findings and conclusions of the paper?: Similar to above, the implications would benefit from a focus on fewer, well motivated, well supported recommendations. See comments to the authors.	As noted, relative to reviewer 2's comments, our revisions aim to clarify recommendations and provide depth in examples.
	Quality of Communication: Does the paper clearly express its case, measured against the technical language of the field and the expected knowledge of the journal's readership? Has attention been paid to the clarity of expression and readability, such as sentence structure, jargon use, acronyms, etc.: The paper is well written and clearly communicated. Occasionally, some jargon could use a definition. See comments to the author.	Thank you; through edits we hope that conceptual clarity has improved.
Referee 2	This is a first-rate paper that some minor revisions, particularly with greater clarity about research methods and a bit more care with the use of language, would make an excellent contribution to the research literature.	Thank you! We hope our revisions to methodology and conceptual clarity address your concerns.
	Additional Questions:	
	Originality: Does the paper contain new and significant information adequate to justify publication?: Yes, in particular but not limited to the fact that it reports an empirical investigation. This fact allows the author(s) to move from general statements to specific analysis and holistic interpretation of their useful data with clear implications for academic info systems practice. The paper has a great story to tell and one that needs to be told.	Thank you.
	Relationship to Literature: Does the paper demonstrate an adequate understanding of the relevant literature in the fields of scholarship represented by the journal, and cite an appropriate range of literature sources in information and learning sciences? Is any significant work ignored?: Its review of related literature is largely much more than adequate; it is sophisticated and thoughtful and marshals the ideas therein to good effect.	Thank you.
	The paper's focus on third parties' use of data about students in specific and clear ways is a major contribution.	Thank you.
	Reliance on the concept and lit of "knowledge commons" may need better scaffolding, especially given the idea's prominence in the paper's orientation. Providing such scaffolding will help more readers understand the value of the paper and the investigation it reports.	In our revisions, we sought to greatly clarify this concept and its use as an analytical and conceptual lens.

Methodology: ***Is the paper's argument built on an appropriate base of theory, concepts, or other ideas? Has the research or equivalent intellectual work on which the paper is based been well designed? Are the methods employed appropriate?:*** Generally, the research methods are clear and defensible, with some important exceptions. The reader needs more clarity about how data analysis was done, especially a bit earlier in the paper, and the question of data quality is not even asked much less answered.	We acknowledge that our effort to meet the word limit impacted the level of detail in our methodology in our original manuscript. Through revisions, we have provided additional detail about analysis and data quality.
I'm certain the author(s) can address these concerns explicitly and easily, and they should.	We appreciate the comments and hope our revisions address your concerns.
Results: Are results presented clearly and analysed appropriately? Do the conclusions adequately tie together the other elements of the paper?: Yes, to both questions. While the conclusion seems more than a bit rushed (perhaps reflecting concerns about length), a summary table for the interview and other results would be of great value to many readers. But the conclusions and recommendations are clear, well-argued, and plainly based on a lucid interpreation of the data.	We have incorporated a summary table and revised our discussion of emerging themes, in a way that we hope provides more depth and clarity.
Implications for research, practice and/or society: Does the paper identify clearly any implications for research, practice and/or society? Does the paper bridge the gap between theory and practice? How can the research be used in practice (economic and commercial impact), in teaching, to influence public policy, in research (contributing to the body of knowledge)? What is the impact upon society (influencing public attitudes, affecting quality of life)? Are these implications consistent with the findings and conclusions of the paper?: One of the great strengths of the paper, besides its clarity and strong conceptualization, is, as noted above, its clear bridging of concerns about third parties' access to and use of data about students to empirical data of various kinds and from various actors and sources. And the paper helps readers see what might be done to better protect students and information about them in specific and explicit ways . . . despite reliance on the tired and questionable concept of "best practices."	The critique of the best practices framing was taken to heart in our revisions. We describe our recommendations as such, noting when specific recommendations might be "transferrable," "generalizable," or candidates for "standards." This is also helpful in tying back to the GKC framework and strengthening our case for why this approach to governance anaylsis is useful to the educational technology context.

	Quality of Communication: Does the paper clearly express its case, measured against the technical language of the field and the expected knowledge of the journal's readership? Has attention been paid to the clarity of expression and readability, such as sentence structure, jargon use, acronyms, etc.: With rare exceptions, noted below, the paper is quite clear in its identification of the rationale and conceptualization of the research study it reports, quite clear in its organization, and quite clear in its language.	Thank you. We prioritize clarity in communication and hope that our edits to those exeptions, as described in C42, better suit the audience.
	One niggling but important point is the verbal and conceptual lack of care in overusing the terms "process" and its cognates (some 36 times) and transparency (at least 18 times). Usually "process" is redundant, while "transparency," if used at all, should make plain transparency of what? To whom? To what effect? And, more generally, "transparency" is a misnomer for the use of "visibility," which also needs to answer the questions about what, whom, and to what effect.	We appreciate that the reviewer brought this to our attention. 1. We have clarified the conceptual importance of "process" as opposed to "practice" or other institutional constraint, limiting its use to those instances when it is conceptually relevant, and tying it back to the GKC framework. 2. We differentiate between visability and transparency in our edits, as well as clarify the answers to those questions asked.
	Less important, but still notable, is the distracting use of "this," usually at the beginning of a sentence without specifying what the reference for "this" is. It may be apparent to the author(s), but that is not always for the case for even the most engaged reader.	We have taken care in our edits to be as clear as possible, replacing "this" whenever possible with the entity/practice/actor in question.

Privacy Governance Not Included: Analysis of Third Parties in Learning Management Systems

ANONYMOUS AUTHOR(S)*

Higher education institutions often manage student data through learning management systems (LMS) that support third-party plug-ins and learning tools interoperability (LTI). This paper evaluates the governance of these technologies at universities in the United States and Canada with a focus on the implications for student data privacy. Qualitative interviews, an online questionnaire, and content analysis of publicly-available university policy documentation reveal a fragmented and opaque ecosystem of student data collection by LMS plugins and LTIs that is tacitly enabled by limited or ineffective governance across institutions. We argue for greater transparency and oversight of LMS platforms, plug-ins, and LTI supported by the creation of a knowledge commons of institutional governance strategies for addressing privacy challenges posed by third-party data flows, commercialization of student data, and education technology decision-making. We highlight some exemplary governance practices identified in our empirical results and provide recommendations for emerging collaborative efforts that are needed to improve the state of student privacy in higher education.

Additional Key Words and Phrases: Educational technology; privacy; computing/technology policy; empirical studies in social computing; third-party data controllers

1 INTRODUCTION

Privacy concerns have grown in tandem with the digital transformation of educational institutions. From concerns about facial recognition in classrooms and on campuses [2] to ubiquitous platformatization of K–12 education [29], the increase in datafication of educational interactions [14] and profiling of students [4] has drawn scrutiny [2, 16, 28]. This trend was amplified throughout the COVID-19 pandemic, as digital solutionism paved the way for virtual classrooms [6] and digital proctoring [5] via synchronous and asynchronous means of collaboration between students and instructors. In response, student preferences [16], university and instructor practices [6, 15], and specific education technology platforms [24, 29] have received scrutiny in recent privacy research. This research has mainly focused on first-party actors subject to federal and state regulation [6, 33], including the extent to which new educational technologies are more intrusive than their antecedents in ways that are inappropriate or discriminatory [22].

Plugins and learning tools interoperability (LTI) for learning management systems (LMS) exist at a crucial intersection of these student privacy issues. Higher education institutions have access to, and in many cases locally host, substantial amounts of student data on LMS that provide third-party mechanisms to enhance interfaces, add new functionalities, and customize user experiences for specific institutions, departments, or courses. The tight integration of first and third-party tools in this ecosystem raises concerns that student data may be accessed and shared without sufficient transparency or oversight and in violation of established education privacy norms. However, these technologies and the university governance practices that could check inappropriate data handling remain under-scrutinized.

This paper addresses this gap by investigating the governance practices of higher education institutions with respect to LMS ecosystems. We answer the following research questions:

RQ1 How are LMS and plugins/LTIs governed at higher education institutions?
- Who is responsible for data governance activities around LMS?
- What is the current state of governance over LMS?
- What is the current state of governance over LMS plugins, LTI, etc.?
- What governance issues are unresolved in this domain?

RQ2 How are issues of privacy and governance regarding LMS and plugins/LTIs documented or communicated to the public and/or community members?

We investigate these research questions through a multi-modal study with three components. We first used an online questionnaire to collect reports of LMS governance practices from information technology professionals at 7 universities in the US and Canada.

We then conducted in-depth interviews with 25 data governance professionals and decision-makers at 14 US research universities. These individuals have a diverse range of expertise, authority, and units, including technical services, educational technology, legal counsel, student affairs, faculty governance, and Provost's offices. 24 of 25 interviewees were in staff or administrative roles, while one was an active faculty member who chaired a faculty senate committee on technology. Through these interviews, we obtained policies, procedures, and frameworks for evaluation of LTIs, plugins, and broader LMS data governance considerations.

We also analyzed public data from 112 universities, including public (n=41), private (n=40), HBCU (n=7), and community colleges (n=14) across the United States (n=102) and Canada (n=10). These data include details of LMS plugin and LTI usage and management at these universities and covers the most commonly used LMS ecosystems (Canvas, Blackboard, and Moodle).

Our results identify several governance gaps relative to LMS and their associated LTIs and plug-ins:

- There are few legal requirements protecting students from third-party data flows via LTIs and plugins.
- Most scrutiny and governance of LTIs and plugins comes from non-profits, not from universities themselves.
- The governance processes in effect are highly non-transparent to impacted students and instructors, resulting in disenfranchisement.
- Emerging governance practices around student data localization and evaluation of third-party technologies at a few universities are serving as a model for many in higher education.

We discuss these results relative to successful exemplars of plugin/LTI governance and conclude that transparency and coordination mechanisms are needed to ensure that students interests are protected beyond nominal compliance with state and national laws.

2 BACKGROUND AND RELATED WORK

Substantial prior work has examined issues of privacy in the education context, although little research has directly examined higher education institutions' governance practices of LMS, plugin, and LTI ecosystems. This section outlines the related research in these areas and provides background information on LMS plugins and LTI.

2.1 Education Technology Privacy and Governance

Issues of educational data governance and student privacy [6] are inherently a collective action problem, with universities representing one of the most visible knowledge commons [25]. The tensions between student data as a resource and students' rights to privacy must be resolved iteratively with the engagement of students and their interests [20, 25], thereby making contemporary educational privacy governance challenges well suited to data commons arrangements [17].

In recent years, the continued "datafication" of higher education has fueled the integration of new learning analytics and big data approaches to online education platforms. Learning Management Systems (LMS), Virtual Learning Environments (VLE), and Massive Open Online Course (MOOC) platforms aim to mimic and improve traditional

educational practices while applying data-driven approaches to personalize and automate established processes [49]. While the use of leaning analytics is promoted as a way to improve learning and student performance [35], these solutions are often implemented as "black boxes," raising a number of concerns around inaccurate, oversimplified student data representation, perpetuating biases and affecting the power dynamics between institution and the learner [40]. Learning analytics can also result in diminishing autonomy, inducing "chilling effects" on student behavior [31, 35], violating students' privacy expectations [19, 50] and introducing conflicts of interests [35].

Adoption of online education platforms has also accelerated a technological shift from on-site servers to cloud-based solutions for managing student and institutional information [1, 11]. As a result, a substantial number of information flows involving students' academic data are becoming available to third party service providers [11]. As fiduciaries of student data, educational institutions should adopt student-orientated information governance practices and demand the same from the third party vendor [18].

The common lack of appropriate governance for technology procurement in higher education institutions also exacerbates the situation, as institutions are ill-equipped to adequately address new privacy threats [6, 30]. This has prompted calls [32] for vetting processes that examine the information handling practices of big data companies and ensure that they align with educational purposes.

It is important to recognize that educational contexts, regardless of technological mediation, are sites of collaboration and social engagement [42]; education technology facilitates social computing by default, extending networked and social privacy challenges into this context [44]. Social aspects, and the inherently networked nature of student data flows, require further empirical scrutiny; this gap can be contextualized, and future research informed, by other scholarship on social aspects of privacy.

Connecting to this broader literature on the unequal [12, 26] and contextual nature of privacy [3, 27], recent studies have illustrated the importance of critically engaging with conceptual and theoretical frameworks in order to strengthen empirical studies of privacy [36, 39], spanning qualitative, quantitative, and mixed research designs [23, 37]. The research community elucidates the social and networked nature of privacy, critically examining the implications of sociotechnical systems on individual collaborators' [44], experts [10] and users' [3], as well as on communities' privacy [21] as experienced. Studies also illustrate the challenges associated with the collection of rich qualitative details to provide insight into the contextual experiences and nuance of examples relative to privacy, documenting mechanisms for rigor with small samples [41], especially in conjunction with multi-method designs [41, 44]. Our work continues this thread by investigating understudied elements of the higher education technology ecosystem.

2.2 Governing Knowledge Commons

The Governing Knowledge Commons (GKC) framework [36, 38] provides a guide for analyzing information governance, especially in contexts where knowledge is collectively produced and shared by a community. GKC considers the social, economic, and political factors in which information is governed, as well as important attributes, such as the relevant actors, their roles and objectives, and their resources. GKC structures the examination of strategies, norms, and rules that shape information handling practices, providing a foundation to understand the emergence of new information norms and how communities and stakeholder groups shape governing institutions and specific governance mechanisms. We use to GKC inform our investigation of the governance practices employed by higher education institutions with respect to LMS and third-party plugins/LTIs.

2.3 LMS Plugins and LTI

The use of extensions in the form of third-party plugins and LTI integrations are commonplace in the LMS ecosystem. They provide mechanisms to enhance or add new interfaces, functionalities to existing LMS platforms and customize user experiences for specific institutions, departments, or courses. LMS plugins typically connect to external web services to implement their functionality. For example, Moodle's Virtual Programming Lab (VPL) [34] integrates programming assignments and assessment and connects to a supported VPL server to compile students' code. Plugins like Turnitin [48] and Crowdmark [45] use the Learning Tools Interoperability (LTI) [46] protocol to communicate with their third-party (non-Moodle) servers. The LTI has become a de facto protocol for LMS plugins on major LMS platforms, including Moodle, Canvas and Blackboard.

2.3.1 Privacy APIs. With the advent of European GDPR regulation, many LMS platforms have deployed a privacy-related API. In Moodle, privacy features are implemented using the Privacy API [47], which is centered around the GDPR notion of protecting personal, identifiable data. Moodle's data model differentiates between information that the user enters and information that is stored. Developers of new third-party plugins need to indicate whether the plugin stores or exports data. When a plugin stores data in a database or interacts with a Moodle subsystem (e.g., Moodle comments, ratings, questions, filesytems) that will result in storing user data, developers explicitly indicate the type of data being stored. When a plugin stores data in its own database, the developer needs to describe each field that includes user data. Moodle API guidelines suggests that "it is a matter of judgement which fields contain user data and which don't. Anything entered by, or directly about, the user probably counts as user data but it may be useful to include additional fields that explain the context of the data." If a plugin exports user data, the developer needs to indicate the target of export and the exported user data fields. In addition, the developer of the plugin needs to implement a function that facilitates the actual export of the data according to the API specifications. A third-party Moodle plugin that adheres to the Privacy API is automatically awarded the "Privacy Friendly" award to inform users that the plugin is following the Privacy API guidelines.

2.3.2 Plugin Certifications. Several universities use 1EdTech's IMS TrustEd Seal program that "certifies that an institution successfully completes training in the IMS TrustEd Apps vetting process and possesses the necessary skills to vet applications for privacy and security using the IMS TrustEd Apps Rubric." [7]

Certified institutions use IMS TrustEd Apps vetting process to conduct independent reviews according to the TrustEd Apps Rubric [7]. The IMS TrustEd Apps Rubric identifies several areas of examinations: data collection, security, third-party data sharing, and advertising. Additional, an optional extension of the rubric include availability of policy, data handling, social interactions, legal (state and federal regulation), accessibility, mobile and integrations.

For each category, the assessment determines whether the privacy policies and practices "meet expectations" of the rubric. The data collection portion of the rubric comprises five points: 1) The policies list all data collected; 2) The policies indicate how data is collected; 3) The policies state who owns the data; 4) The policies allow users to delete their data entirely; 5) The policies state the retention of data.

The third-party sharing portion of the rubric inlcudes five points: 1) The policies state the use of third parties; 2) The policies state what information is shared with each third party; 3) Users can opt out of third party data sharing; 4) The supplier requires their third parties to adhere to the terms of the vendor/customer agreement; 5) The user is notified of a change in third parties.

A special area of examination is dedicated to advertising. It includes evaluating that policies indicate 1) whether or not advertisements are displayed, 2) whether or not users are targeted for advertisement, 3) whether or not any third parties track or collect information for advertisement, 4) whether or not web beacons or other tracking methods are used for ad purposes, 5) whether or not users can opt out of sharing data with advertisers.

2.3.3 LMS Risk Assessment. Some educational institutions rely on vendors' assessments to evaluate the privacy risks of new education technologies. The EDUCAUSE [8] Higher Education Community Vendor Assessment Toolkit (HECVAT) [9] risk assessment of third-party solutions ranges from questions about whether the entity providing of the technology performs "security assessments of third party companies with which you share data? (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.)." to questions on general governance roles, such as "Do you have a dedicated Information Security staff or office?," "Do you have a dedicated Information Security staff or office?," and "Do you have a dedicated Software and System Development team(s)?" The form also includes questions about organizational structure, audits, and self assessment histories. From the 13 questions on *Documentation* section of the HECVAT, two are related to a notion of information privacy: "Does your organization have a data privacy policy?" and "Can you provide overall system and/or application architecture diagrams including a full description of the data flow for all components of the system?" The form also asks seven additional questions about data management, including data isolation, encryption in storage and in transport, backup, and staff access to institutional data.

3 METHODS

This study involved three components:

(1) An online questionnaire about LMS, plugin, and LTI governance practices from IT professionals at seven universities in the United States (n=4) and Canada (n=3). The responses from these individuals helped us frame and design the interview schedule.
(2) A review of public data from 112 universities about LMS plugin and LTI governance. 18 of these universities provide additional documentation, which we analyze in further depth.
(3) A series of extensive interviews with 25 university data governance officers with responsibilities for LMS, plugin, and/or LTI governance, representing 14 different universities.

3.1 Online Questionnaire

We created an online questionnaire to collect descriptions of LMS and plugin/LTI governance practices from IT professionals at four universities in the United States and three universities in Canada. This sample included five public research universities, one private research university, and one private liberal arts college. We recruited these individuals through our professional networks. The use of an online questionnaire was approved by the Institutional Review Boards (IRB) at all authors' universities. All respondents provided their informed consent and were were not monetarily compensated for their participation. The questionnaire contained the following sections:

(1) *Background.* Respondents were given background information on the research project, definitions of LMS, plugins, and LTIs, and instructions for taking the survey. The instructions specified that while LMS details are typically non-sensitive, respondents should not violate their university's procedures for reporting internal protocols.

(2) *LMS Adoption.* Respondents were asked to identify the LMS in use at their university and which individuals and units at their university are involved in the adoption of LMSs, plugins, or LTIs. Respondents then indicated whether their university develops plugins or LTIs internally.
(3) *Third-party Plugin Governance.* Respondents were asked to describe their university's procedures for deciding whether to adopt new LMS plugins/LTIs as well as any formal or informal security audits or privacy considerations performed prior to adopting new LMS plugins/LTIs. They were also asked to indicate the units at their university responsible for managing the adoption of new LMS plugins, performing security audits on new LMS plugins, and considering privacy implications of new LMS plugins.
(4) *LMS Challenges.* Finally, respondents described their university's process for addressing any problems or challenges that arise with LMS plugins or LTIs.

We manually reviewed the responses and present the results in Section 4. The data provide a glimpse into LMS/plugin/LTI governance in use at a range of universities.

3.2 Data Collection and Analysis of Publicly Available Documents

We identified a sample of 112 universities via US News categories: public (n=41), private and liberal arts (n=40), HBCU (n=7), community college (n=14), and Canada (n=10). These institutions reflect a spectrum of geographic, socioeconomic, and student population characteristics, as determined by the US Department of Education National Center for Education Statistics (NCES) and Universities Canada.

In order to understand the scope of LTI and LMS plugin usage and support at these universities, we collected lists of their LTIs and plugins at use via public university knowledge base websites. This information was scraped using Python and identified by keywords "Canvas," "Blackboard," "Moodle," "LTI," "plug-in," and "LMS." In addition to identifying which plugins or LTIs were used by these universities, we sought to determine the number of LTIs or plugins that are developed and supported by the universities locally, as well as the number of LTIs or plugins for which data was hosted locally. In order to identify these statistics and characteristics, we conducted content analysis of the scraped documentation. Throughout this process, we also sought to identify what information is provided to instructors who may want to add or request that their university support other LTIs or plugins. This provides insight into what entities at these universities are responsible for LMS, plugin, and LTI adoption and oversight and how transparent these processes are to instructors, students, and the public.

A majority of the coding was completed by one of the investigators and a student research assistant, identifying five qualitative codes: data localization, internal development, internal hosting, external data flows, and procedural transparency. All five codes merited high agreement and inter-rater reliability scores [43]. Inter-rater reliability was not assessed for counts of LTIs or plugins identified, given that this process was documentation, rather than interpretation.

A subset of 18 of these universities (15 in the USA, 3 in Canada) provided extensive additional information about their LMS and plugin/LTI goverenance practices on public websites. We focused on these universities for further analysis of practices and stakeholders based on the accessibility of this information. Table 2 summarizes the main governance institutions related to new LMS plugin approvals.

3.3 Interviews with University Data Governance Officers

Interviews were conducted with 25 university data governance officers with responsibilities or decision-making authority regarding LMSs, LMS plugins, and/or LTIs at 14 different US universities. Participants volunteered to participate following a professional development workshop regarding data governance, in order to provide empirical support for future data

Table 1. Interview Schedule Indicating Relationships between Research Questions, Theoretical Framework, and Interview Questions

Research Question	GKC Framework Support	Interview Question
Who is responsible for data governance activities around LMSs in higher education?	Background	Can you tell me about your role at [the university]?
	Attributes, Background	How are you involved in LMS data governance?
	Attributes, Background	Are you involved in any other data governance practices or domains?
	Attributes	What other teams, units, or roles are involved in LMS data governance?
	Attributes	How do you engage with [those groups/people]?
What is the current state of governance over LMSs in higher education?	Governance	What are the rules on the books that impact LMS data at the federal level? State level? University level?
	Governance, Patterns and Outcomes	How do you implement those rules?
What is the current state of governance over LMS plugins, LTIs, etc.?	Governance	What rules are in place that impact plugins and LTIs that connect third parties to LMSs at your institution?
	Governance	What procedures are in place to make decisions regarding plugins and LTIs?
	Governance, Patterns and Outcomes	How are those decisions implemented?
What governance issues are unresolved in this domain?	Governance, Patterns and Outcomes	Are there any ongoing debates about LMS data on your campus?
	Governance, Patterns and Outcomes	What issues are unresolved about plugins, LTIs, and/or third parties?

governance in this domain and in recognition of the need to document governance challenges and progress over student data, assessment practices, and educational technology vendors. Respondents at 5 of these 14 universities consented to identify their institutions, while 9 preferred we not disclose their institutions, as they believe it would identify them or could lead to repercussions for their employment.

Interviews lasted between 48 and 94 minutes. All interviews were conducted on Zoom, with transcripts auto-generated via closed-captions and lightly edited for clarity around names and acronyms, in particular, based upon investigator notes.

All were prefaced with a brief overview of research motivations, questions, and logistics. The interviews were semi-structured, with theoretically grounded questions developed from the descriptive GKC framework in order to address sub-components of our research questions. The sequence of interview questions was flexible, following the flow of responses and follow-up questions. In Table 1, we indicate which structured interview questions correspond with which research questions, as well as what aspects of the GKC framework provide conceptual grounding for their framing and subsequent interpretation of results.

4 RESULTS

This section presents our analysis of practices and governance of third-party integrations to university LMSs. We document gaps in governance that promote privacy risks relative to third-party data flows and LMS integrations. The results are organized by data collection strategies, reflecting distinct approaches to triangulate insights to our research questions. Internally, results are structured according to the descriptive GKC framework (section 2.2). Contextual attributes and third-party practices are documented in section 4.2, addressing RQ1 in part and complimenting the online questionnaire. We further address the extent of third-party access to student data via LMS plug-ins and LTIs (RQ1) in section 4.2.2. Section 4.3 addresses issues of governance and transparency (RQ2 and RQ3); Section 4.3.4 provides further depth in exploring governance, transparency, and inequality patterns and outcomes.

4.1 Online Questionnaire

4.1.1 LMS Use, LMS Management, and Plugin/LTI Development. Seven IT professionals provided responses via our online questionnaire. Of their universities, three use Canvas and Moodle, two use Canvas, one uses Moodle, and one uses Brightspace. Six of the seven universities develop plugins/LTIs internally. All respondents reported that their Information Technology offices had at least partial responsibility for LMS management. Additional responsibility for LMS management was shared by Education Technology units (n=3), Centers for Teaching and Learning (n=2) and the Business Office (n=1).

4.1.2 Deciding Whether to Adopt a New Plugin/LTI. Four respondents reported that requests from faculty, instructors, or other campus community members initiate the process of adding a new plugin/LTI. These requests are considered in light of need, whether existing plugins/LTIs already provide similar functionality, and cost. For example,

> We start users with a request process. After the request is submitted they go through a review to see if we have any duplicative services that already perform the core functionality needed. If we do not have a service that does this we review if that tool can be purchased and at what cost. When cost or features/integration is complex we then consider [in house] development. (P6)

In some (but not all) cases, these requests are then audited according to an existing procedure. For example,

> [If the] plugin or LTI is identified as having a potential for a centrally supported tool, features and functionality are reviewed, [and it] goes through a Privacy and Security audit. Using the external tool instructors can set up their own LTI links – no process followed. (P3)

This distinction between plugins and LTIs was echoed by another respondent (P2), who described an auditing process for plugins accessible to the entire university while

> Instructors can install LTIs, if supported, within their course, thereby bypassing the request process. (P2)

One respondent noted an explicit preference for vended plugins/LTIs – considering the technical debt that could be incurred from custom development (P7).

One respondent indicated that their university did not follow any specific process for deciding whether to adopt new plugins/LTIs.

4.1.3 Process for Updating Plugins/LTIs? Five respondents described a process followed for updated plugins/LTIs. The most stringent approach involved a multi-year scheduled audit:

> We work with our governance group around when to require the next version of the LTI standard and we also review all LTIs every three years to review safety and security as well as confirming the tool still meets the specified functional needs. (P7)

Other approaches included always attempting to use the most up-to-date version of LTI integrations (P1 & P5), evaluating updates on a case-by-case basis depending on cost and use cases (P6), and evaluating updates in a staging environment to avoid "breaking the LMS" (P2).

Two respondents indicated that their university did not follow any specific protocol for updating plugins/LTIs. This poses clear security risks with privacy implications.

4.1.4 Process for Security Audits Prior to Plugin/LTI Adoption. Three respondents indicated that their university collects extensive information from plugins/LTI vendors for security review before adoption. All three of these universities use the Higher Education Community Vendor Assessment Toolkit (HECVAT) form from EduCause [9] for this purpose.

One respondent reported that they "do a full security review including documenting all endpoint calls, the need for developer keys or not, with a strong preference toward scope dev keys" (P7). One respondent said that their university's IT department performed a security audit, and one respondent reported an audit involving a test of the plugin/LTI, but neither provided additional details.

One respondent indicated that their university did not follow any specific process for security auditing plugins/LTIs prior to adoption (P4).

4.1.5 Process for Privacy Audits Prior to Plugin/LTI Adoption. Three respondents said that their security audits also included privacy considerations (P2, P3, P6). For example

> Privacy reviews are part of our third-party assessment security review process. (P6)

Two respondents said that their privacy audit included legal considerations involving PIPEDA/FIPPA (P1), FERPA (P7), or the university's legal counsel (P5).

One respondent indicated that their university did not follow any specific process for privacy auditing plugins/LTIs prior to adoption (P4).

4.1.6 Addressing Plugin/LTI Issues. Five of seven respondents described their university's process for addressing problems or challenges with LMS plugins or LTIs. The responses suggest that a tiered approach is common, involving attempts to address the issue locally followed by collaboration with the plugin/LTI vendor. Standard troubleshooting approaches, such as checking for updates, temporarily removing misbehaving plugins/LTIs, and finding workarounds to reduce end-user impacts, were also reported. For example,

> If the issue is with a third-party plugin, we verify for updates. If there are no updates, we will try to fix ourselves and notify the plugin maintainer about our fix. If we cannot fix it for any reason, we notify the requester about the impossibility to fix. We try to find a work around for the user. (P2)

> Work with vendor or developer to address issues. If not possible, or not timely, remove plugin until addressed. In some instance, address with internal development. (P1)

One respondent reported a phased-deployment system in place to reduce LMS disruptions when new (potentially buggy) plugins/LTIs are added:

> Integrations are usually launched as limited pilot programs only for those users that request access so issues that arise have at most a limited impact and can be dealt with before more widespread University

adoption. We also "dogfood" the plugins ourselves trying to anticipate any issues, but if/when issues arise, the IT LMS team takes over troubleshooting with the vendor or in-house team. (P5)

4.2 Analysis of Public Records and Documentation

4.2.1 Comparative Indicators of LTI and Plugin Prevalence. Across the 112 universities reviewed, Blackboard (n=47), Canvas (n=61), and Moodle (n=32) are the three most widely used LMSs, while Brightspace (n=5), Compas (n=5), and Google Apps for Education (n=3) are much less pervasive. Note that 28 universities currently support more than one LMS. Some of these universities appear to be transitioning from one to another, while others offer choices or allow individual departments, schools, or colleges to make LMS decisions, rather standardizing across the university.

94 of 112 universities provide data on plugins and LTIs used, of which 65 publicly document which specific third parties and tools are available for use at their university and 29 provide summary statistics. Of those universities that do not provide these details, 17 of 18 are private and the other is Canadian (Edmonton University). On average, universities have 54 total plugins and LTIs available for instructors to integrate with course sites. 1208 unique plugins and LTIs were identified in total, with 771 developed by universities rather than third-parties. The most pervasively available third-party tools are: Proctorio, TurnItIn, Honorlock, GradeScope, CrowdMark, MindLinks, Digication, Kaltura, LinkedIn Learning, Pushback, Panopto, MatLab Grader, Perusall, YouTube, and ProctorU.

While the number of total plugins and LTIs at any given university is highly correlated with student population size (ρ=0.86), the endowment per student provides significant insight into whether those tools are locally developed and supported or integrate with third-party platforms.

4.2.2 Analysis of Institutions Publicly Available Policy Documents. Most universities we reviewed require faculty or department/unit to submit a formal request for a new tool or plugin, which initiates a review process to determine whether the plugin fulfills university requirements. Notably, with regards to adoption on new education technology (not specifically related to LMS plugins), University of Waterloo asks instructors to inform students about newly introduced data practices and provide opportunities to opt-out.

The assessment of the plugin includes evaluation of security, risks and compliance. Some universities, for example, Michigan and Illinois universities, use certifications such as HECVAT [9] and SOC2 [13] questionnaires in their review. Other examples, like Penn State, require that all services are LTI 1.3 Advantaged Certified. As we pointed out in Section 2.3.3, these standardized questionnaires focus on identifying the (mainly security-related) information handling practices and third-party interactions.

A typical assessment involves several stakeholders such as IT departments, security or learning technology teams. Some universities involve vendors or service providers as part of the assessment process. For example, the University of Michigan-Dearborn asks vendors to complete an internal security-compliance questionnaire. Similarly the University of Toronto performs an vendor security audit. In another example, Iowa State University also requests the vendor to provide relevant documentation to help with assessment.

Contractual obligation. Out 18 universities we examined in greater detail, 6 universities require some form of contractual obligation, such as data protection agreement and/or Data Protection Addendum[1] to approve a new plugin.

[1]Michigan State University, Northwestern University, University of Illinois at Urbana-Champaign, University of Maryland College Park, University of Wisconsin Madison, University of Toronto

Table 2. Governance institutions involved in the LMS plug in approval processes across the examined universities

University	Country	LTI related policy	Review Request	Vetting Process	Asks to Inform Students	Includes Data Reuse	Discusses Copyright	Asks for the IMS Certificate	Discusses Internal Development	Mentions FERPA/FIPPA	Data Protection Agreement	Contractual Obligation	Security Assessment	Risk Assessment	Compliance Assessment	New Plugin Request Form
IU, Bloomington	USA	✓	✓	✓		✓	✓		✓							✓
MSU	USA	✓	✓	✓						✓				✓		✓
Northwestern	USA	✓	✓	✓					✓	✓	✓	✓				
Penn. State	USA	✓	✓	✓				✓		✓						✓
Purdue	USA	✓	✓	✓				✓	✓	✓				✓		✓
Rutgers	USA	✓	✓	✓				✓		✓		✓			✓	
UIUC	USA	✓	✓	✓				✓	✓	✓		✓		✓		✓
Iowa	USA	✓	✓	✓			✓	✓			✓					
UMGC	USA	✓	✓	✓		✓				✓		✓	✓			
UM-Dearborn	USA	✓	✓	✓						✓	✓			✓	✓	
UMN-Twin Cities	USA	✓	✓	✓								✓				✓
UWM	USA	✓	✓	✓				✓	✓	✓		✓				✓
UofT	Canada	✓	✓	✓							✓	✓	✓			✓
UCF	USA	✓	✓										✓			✓
Ohio State	USA		✓													
U Regina	Canada			✓								✓		✓		
UWaterloo	Canada			✓	✓	✓			✓							✓

Universities[2] that do not have a contractual obligation requirement refer to existing regulation–such as the Family Educational Rights and Privacy Act (FERPA) in the US institutions and the Freedom of Information and Protection of Privacy Act (FIPPA) in Canada—as benchmark for privacy assessment. Several universities, such as Universities of Indiana, Iowa and Maryland, include additional assessment criteria regarding copyright infringement of student work and potential reuse of students data by the vendor for their own purposes.

Internally developed plugins. Internally developed plugins do not go through the same scrutiny. For example, at the University of Wisconsin, the process varies based on the intended data sharing practices. If the new service solely interacts with local university services, it is approved by the default. However, in cases when the new service shares data with services that are not maintained by the university recognized development groups, it will require further vetting. Examples of additional internal plugin vetting policy, such as used in Rutgers University, include asking developers to explicitly state the scope and permissions before the new plugin is developed.

[2]Indiana Bloomington, University of Pennsylvania, University of Iowa, University of Michigan Dearborn, University of Nebraska Lincoln, University of Waterloo

4.3 Interview Analysis

4.3.1 Decision-Making Roles and Disagreement Among Responsible Units. Answers in response to questions about participants' roles and "what other teams, units, or roles are involved in LMS data governance" illustrated the complexity regarding decision-making in this arena. Based on responses from all 25 interviewees at 14 universities, we find that the following units have some say in this process: university IT (n=14), legal departments (n=14), faculty governance via committee or full senate (n=13), individual departments or colleges (n=12), campus center for teaching or educational innovation (n=7), the Provost's office (n=6), a Dean of Students or equivalent office with authority over student affairs (n=5), privacy and/or security offices independent from IT (n=3), procurement (n=2), and individual instructors (n=1). As such, a major challenge recognized by these professionals is that of coordination between units and reconciliation of their differences in opinion.

Respondents from many universities (n=9) emphasized a general lack of understanding at university level about privacy issues, coordination problems around educational technology decisions, and third-party data flows. They spoke about how other priorities overtook the general focus in discussion of educational technology broadly, and LMSs specifically, as well as how raising these coordination problems often went unheard. In many of these cases, other values seem to supersede privacy concerns; "there is no interest in streamlining or, on the other hand, students' interests here" one explained. Another participant described, "I can't speak to anywhere else, but here, convenience is king. If an instructor requests something and justifies that with how 'easy' or 'free' or 'simple' it will be, in all likelihood, they're going to get it. And that only got worse with COVID."

4.3.2 Models for Governance Coordination and Best Practices. In contrast to all 11 universities that worried about dysfunction, 3 universities stood in contrast, albeit with three different coordination strategies. The only respondent at one university explained that they were the sole person with data governance responsibility at their institution, "which is ridiculous because of course I can't do this all alone and of course other people also do relevant work, but still I'm in an office on my own, trying to be all of the coordination at once." This participant preferred not to identify their institution. In a discussion with two participants at the University of Illinois, one explained "Consolidation and consistency are much more important in campus level discussions right now as we move to one LMS and one central group managing everything, including the LTI issues you asked about."

The University of Michigan also particularly stood out, describing a functional system of coordination without onerous bureaucracy. They had developed clear decision-making tools for individual units that allowed for consistency, without lengthy approval processes. The guidelines they developed, reflected community norms, state and federal laws, technical standards, and local infrastructural constraints and supports. Upon approval of an individual LTI or plug-in, the completed decision making form would be shared centrally, for verification and transparency, as a reference for the university community and other units that may wish to use something approved elsewhere on campus.

In contrast to many other the institutions that expressed frustration with the dysfunction they experienced, participants from these latter two universities described a positive outlook for data governance with respect to LMSs at their institutions, and the ways in which they served in leadership roles for broader communities of universities, including peer institutions, HBCUs, and HSIs.

Peer institutions that participated in interviews themselves emphasized hoping to learn from others about how to successfully streamline decisions, more so than normative best outcomes. They wanted to understand process and how others had established order, oversight, and coordination.

4.3.3 Ongoing Challenges in LMS and LTI Governance. Ongoing governance challenges described by interviewees included: coordination problems among units, inadequate legal protections at the state and federal levels, confusion about protocols, university politics, and the non-transparent practices of the third-parties developing LTIs and plugins. This section illustrates examples of all of these issues, as well as some of their interrelationships.

Notably, some of the coordination problems stem not only from multiple departments with oversight, but also from policies that address the type of contractual and financial obligations that apply to an LTI or third-party plug-in, rather than the category of technology. At one university, a participant explained "Our processes are more of a relic than anything else and we just can't escape it. If an LTI is free, the finance office doesn't care at all; if it's not, it gets a lot of scrutiny. If the license is education specific, legal says that box is checked and doesn't look any further. Then it only gets a tech review. But lots of these cost money, require negotiating a license, and need security, privacy, whatever." Their colleague contextualized further, "in our state, privacy laws, you asked about those, really only apply to K-12, so at our level, we're just looking at federal, basic consumer... That's really why legal is so hands off on this. They're more intense with other liability things, discrimination especially."

A participant from another university echoed this, emphasizing confusion over who had say and when multiple forms of approval were needed. "Everything here has some legal, technical, and faculty oversight, but if certified or with the right license by default, as with many ed-tech specific tools, you know not YouTube, but TurnItIn, whoever is adopting can just sort of self-certify. There's no real order or central place to log this. We have a lot of things adopted with only partial approval. The thing most skipped is the Faculty Senate committee on Technology Adoption, no one wants to deal with the politics, but it's almost worse when it comes out, you know? It might slide under the radar, but it might be that the Business School decided to use Proctorio without taking it to a vote and then you get a student protest and 'Bam.' It's a huge mess and a lot of finger pointing."

Participants from 6 different institutions discussed the governance challenges associated with actually reviewing LTIs and plugins, discussing issues of proprietary algorithms, secrecy, and ambiguity around functions. One respondent summarized the challenge in these terms: "How are we supposed to make a choice without anything more than a sales pitch? I'm supposed to tell the university if something is sound from a privacy and security POV, but all I have are words. No one wants to let me look at the code." Another expanded to tie this to differences in values: "The more of a black box something is, the more I scrutinize, honestly. An endless list of proctoring plugins and every last one is not about assessment or real teaching needs, they're about covering their ***** during lockdown. It's all we own this, we can't tell you more. That difference is about more that money, it also about secrets as power and criminal justice logic that's spreading in education technology, or really technology everywhere. All surveillance, all the time."

4.3.4 Governance Patterns and Outcomes. While governance processes vary considerably, with few institutions leading in this space, some patterns are beginning to emerge around communication regarding plugins and LTIs, especially at public institutions.

Thus, one key distinctive pattern emerges around the degree of transparency surrounding governance and third-party data flows around LMSs as intersects with the public-private divide. While public universities must provide public-facing documentation, there are no requirements or incentives for private universities to be as forthcoming; typically, private universities provided, at most, guides for their instructors to consider available supported tools and links for further requests on plugins, or else, at least, nothing. In contrast, most public universities provide significant documentation in their knowledge bases, which may not be easily findable by the average student, instructor, or member of the public without some idea of what to search for but are public facing. This may still fall short of data governance

transparency values but does provide interpretable records. As one interview participant explained, "I have a rough sense of what people on campus want, and while that's different from student to instructor, we're not providing any of the right information outside of the knowledge base articles. But, those are underused. There's a group of staff and some professors of a certain age, but outside that, people don't know what we provide there." Better publicity around these resources could solve some awareness problems.

A second key pattern that emerges centers around inequality and privacy protections. Not only do economic factors play a role in the imbalance in third-party flows, with less affluent universities depending to a greater extent on "free" integrations, but also the comparative endowment per student corresponds with local support, documentation, and oversight. Thus, community college students, for example, are not only more likely to have third-parties collecting their data via LMS integrations, they are unlikely to find documentation around these practices or know who to turn to in order to ask questions about data governance.

It is notable that some of the more privileged institutions recognize this chasm, with their LMS experts offering workshops and knowledge resources to other institutions, so that all students can benefit from more privacy protecting LMS configurations. As one learning technology specialist at a public university with a relatively high endowment per student stated, "it's not just kids at [my university] that should benefit from this; students should not constantly be documented and monetized by textbook, social media, and "anti-cheating" integrations! LinkedIn and YouTube don't need this data; it's very simple to build around it… I convinced [their boss] to let me offer a workshop to teach how easy and lightweight this is. We had 23 universities attend the first round, with 7 community colleges, 3 HBCUs, 2 HSIs. It was great."

The status quo of LMS governance relative to student data and third parties is one in which "the vendors are leading! They sell people things at conferences, convince faculty they need something, and we're always in a rush to make it happen, at the expense of scrutiny." Yet 12 of 14 interviewed institutions emphasized that they are starting to push back, based on the successes of data localization, on-campus development of features that don't require exogenous data sharing, and DPAs at peer institutions, such as the University of Michigan and the University of Illinois. As one center director of Innovative Education explained, "it's really hard to do this right, especially as I'm a part of a larger university system in my state that usually wants things done consistently, but I have to the contrarian, because making better choices for students not for-profit developers is the right thing to do."

5 DISCUSSION

The interviews and the content analysis highlight several governance issues that require examination, as well as suggest some preliminary best practices.

5.1 Privacy Threats and Challenges

The rapid transition to online LMS systems introduced unprecedented levels of information complexity to existing educational governance institutions. While universities attempt to meet the challenge with revised review processes of newly introduced tools, they are often outmatched by new digital threats. This problem is especially acute when it comes to supporting a large ecosystem of data-hungry third-party plugins and integrations that can have direct access to LMS data.

Evaluating specific examples of governance and status quo arrangements around LTIs and LMSs, we see that student privacy is being overlooked, ignored, and, in some cases, intentionally sacrificed. Tradeoffs between privacy and efficiency made under emergency pandemic circumstances have amplified the situation, yet other non-privacy related

trade offs, such as between authority and control with time, lead non-normative strategies and rules. Trade offs have also been made that de-prioritize privacy in favor of surveillance over students, justified as critical to academic integrity, yet following carceral logics rather than pedagogical arguments, as discussed by participants regarding value divergence between educational intuitions and vendors. As decisions are made to prioritize convenience, cost or control over the interests of student privacy, significant third-party data sharing with commercial actors ensues.

5.2 Fragmented Governance

To the untrained eye, educational institutions put up a brave front. Our analysis, however, indicate a state of fragmented and dysfunctional governance based on outdated regulation and review processes. It is unclear who is in charge. The lack of expertise forces some universities to outsource the risk assessment of new tools to external partners and the use of standardized questionnaires. Furthermore, the increased complexity requires involvement of many institutional stakeholder such as finance, procurement, IT and other units which further complicates and delays the review process. In some cases, the governance processes simply breakdown. Third-party services can be integrated with little oversight. In cases where a formal review process exist, it is generally designed for evaluating new tools and platforms, with little attention is given to the third-party integration.

5.3 Recommendations

Building on the emerging best practices recognized by interview participants and integrating other suggestions and needs, this section provides recommendations for governance of LMS and integrations moving forward.

An effective means to improve governance and privacy outcomes in this space is to engage with the emerging knowledge commons via collective production efforts for LTI and LMS governance frameworks; those institutions that saw tentative successes in governance aim to do this already, and other interview participants recognized and appreciated their efforts. Professionals in higher education data governance connect with one another via professional development opportunities, conferences, formal networks within academic conferences, and training opportunities. Through these connections, knowledge about successes and failures in governing student data flows and decision-making about third-party services and tools is co-produced with the community, reflecting a knowledge commons. These opportunities and activities are very efficient investments at a time of limited resources and high demands on decision-makers' time, as they provide a knowledge network to draw upon in making decisions.

Beyond the information they might gain about particular decisions or specific LTIs, what multiple respondents viewed as most valuable is learning how other universities have successfully implemented streamlined decision-making processes that reflect community norms, protect student privacy, and can be operationalized without significant challenges. They wanted to be able to benchmark and learn from one another.Examples of such successes include: consistency in decision making criteria via descriptive governance frameworks, clear processes for coordination amongst units, and transparency about what has already been approved and is in place, to avoid replication across colleges and departments.

In contrast with various other established privacy trade offs playing out in this action arena, transparency seems to enhance privacy in many cases. Both transparency over decision-making processes and transparency about what LTIs and plugins are in use seem to support fewer local privacy controversies at many of the universities in the study. Universities that are more open, consistent, and clear about data practices, governance, and data flows can serve as models, not only through formal training modules and governance frameworks, but also in providing transparent, replicable best practices.

Best practices for governance mechanisms, including feedback opportunities to support community members' voices, documentation of governance, consistent oversight, and coordination among decision-makers, that are crowdsourced, discussed, shared with other universities and tested in multiple contexts emerge and coalesce. Further, our results suggest that more clarity is needed in terms of where students and instructors look for information about privacy and practices of third parties. Further, investing and expanding data governance professional development may enhance the ability of decision-makers to communicate across departments and units, reflecting an interdisciplinary perspective.

6 CONCLUSION

We analyzed the governance institutions and practices of higher education institutions with respect to learning management systems (LMS) and associated plugins and LTIs. Our results indicate a portrait of fragmented and unobtrusive, unnoticed student information flows to third parties. From coordination problems on individual college campuses to disparate distributions of authority across campuses, as well as from significant data collection via individual LTIs to a shared problem of scope across many LTIs, we see that increased and intentional governance is needed to improve the state of student privacy and provide transparency in the complex environment around LMSs. Yet we also see that there are logical paths forward based on successful governance and leveraging existing collaborative networks among data governance professionals in higher education.

REFERENCES

[1] M. Alier, M.J. Casañ Guerrero, D. Amo, C. Severance, and D. Fonseca. 2021. Privacy and E-Learning: A Pending Task. *Sustainability (Switzerland)* 13, 16 (2021). https://doi.org/10.3390/su13169206

[2] Mark Andrejevic and Neil Selwyn. 2020. Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology* 45, 2 (2020), 115–128.

[3] Karla Badillo-Urquiola, Yaxing Yao, Oshrat Ayalon, Bart Knijnenurg, Xinru Page, Eran Toch, Yang Wang, and Pamela J. Wisniewski. 2018. Privacy in Context: Critically Engaging with Theory to Guide Privacy Research and Design. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Jersey City, NJ, USA) *(CSCW '18)*. Association for Computing Machinery, New York, NY, USA, 425–431. https://doi.org/10.1145/3272973.3273012

[4] Veronica Barassi. 2020. *Child data citizen: How tech companies are profiling us from before birth.* MIT Press.

[5] Ben Burgess, Avi Ginsberg, Edward W Felten, and Shaanan Cohney. 2022. Watching the watchers: bias and vulnerability in remote proctoring software. *arXiv preprint arXiv:2205.03009* (2022).

[6] Shaanan Cohney, Ross Teixeira, Anne Kohlbrenner, Arvind Narayanan, Mihir Kshirsagar, Yan Shvartzshnaider, and Madelyn Sanfilippo. 2021. Virtual Classrooms and Real Harms: Remote Learning at {US}. Universities. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 653–674.

[7] MS Global Learning Consortium. 2022. The TrustEd Apps rubric. https://www.imsglobal.org/activity/trustedapps/rubric.

[8] EDUCAUSE. 2022. About HEISC. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/about-heisc.

[9] EDUCAUSE. 2022. Higher Education Community Vendor Assessment Toolkit. https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit.

[10] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. 2018. The Influence of Friends and Experts on Privacy Decision Making in IoT Scenarios. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 48.

[11] Tobias Fiebig, Seda Gürses, Carlos H Gañán, Erna Kotkamp, Fernando Kuipers, Martina Lindorfer, Menghua Prisse, and Taritha Sari. 2021. Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds. *arXiv preprint arXiv:2104.09462* (2021).

[12] Christian Fuchs. 2011. Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society* (2011).

[13] Imperva. 2023. SOC 2 Compliance. https://www.imperva.com/learn/data-security/soc-2-compliance/.

[14] Juliane Jarke and Andreas Breiter. 2019. The datafication of education. *Learning, Media and Technology* 44, 1 (2019), 1–6.

[15] Kyle Jones, Amy VanScoy, Kawanna Bright, and Alison Harding. 2021. Do They Even Care? Measuring Instructor Value of Student Privacy in the Context of Learning Analytics. (2021).

[16] Kyle ML Jones, Andrew Asher, Abigail Goben, Michael R Perry, Dorothea Salo, Kristin A Briney, and M Brooke Robertshaw. 2020. "We're being tracked at all times": Student perspectives of their privacy in relation to learning analytics in higher education. *Journal of the Association for Information Science and Technology* 71, 9 (2020), 1044–1059.

[17] Kyle ML Jones and Chase McCoy. 2021. Privacy in Practice. *Governing Privacy in Knowledge Commons* (2021), 98.

[18] Kyle ML Jones, Alan Rubel, and Ellen LeClere. 2020. A matter of trust: Higher education institutions as information fiduciaries in an age of educational data mining and learning analytics. *Journal of the Association for Information Science and Technology* 71, 10 (2020), 1227–1241.

[19] Kyle M. L. Jones, Andrew Asher, Abigail Goben, Michael R. Perry, Dorothea Salo, Kristin A. Briney, and M. Brooke Robertshaw. 2020. "We're Being Tracked at All Times": Student Perspectives of Their Privacy in Relation to Learning Analytics in Higher Education. *Journal of the Association for Information Science and Technology* 71, 9 (2020), 1044–1059. https://doi.org/10.1002/asi.24358

[20] Kyle M. L. Jones and Chase Mccoy. 2018. Reconsidering data in learning analytics: opportunities for critical research using a documentation studies framework. *Learning, Media and Technology* 44, 1 (Dec 2018), 52–63. https://doi.org/10.1080/17439884.2018.1556216

[21] Negar Khojasteh, Cathy Liu, and Susan R. Fussell. 2019. Understanding Undergraduate Students' Experiences of Telepresence Robots on Campus. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing* (Austin, TX, USA) *(CSCW '19)*. Association for Computing Machinery, New York, NY, USA, 241–246. https://doi.org/10.1145/3311957.3359450

[22] Priya C Kumar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2019. Privacy and security considerations for digital technology use in elementary schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[23] Yuan Li. 2011. Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems* 28, 1 (2011), 28.

[24] Chen Ling, Utkucan Balcı, Jeremy Blackburn, and Gianluca Stringhini. 2020. A first look at zoombombing. *arXiv preprint arXiv:2009.03822* (2020).

[25] Michael J Madison, Brett M Frischmann, and Katherine J Strandburg. 2009. The university as constructed cultural commons. *Wash. UJL & Pol'y* 30 (2009), 365.

[26] Katie Miller. 2020. A matter of perspective: Discrimination, bias, and inequality in ai. In *Legal Regulations, Implications, and Issues Surrounding Digital Data*. IGI Global, 182–202.

[27] Helen Nissenbaum. 2009. *Privacy in context: technology, policy, and the integrity of social life*. Stanford Law Books.

[28] Office of the Privacy Commissioner of Canada. 2022. OPC Privacy Complaint report. https://www.canlii.org/en/on/onipc/doc/2022/2022canlii9040/2022canlii9040.html.

[29] Hakan Ozalp, Pinar Ozcan, Dize Dinckol, Markos Zachariadis, and Annabelle Gawer. 2022. "Digital Colonization" of Highly Regulated Industries: An Analysis of Big Tech Platforms' Entry into Health Care and Education. *California Management Review* (2022), 00081256221094307.

[30] Britt Paris, Rebecca Reynolds, and Catherine McGowan. 2022. Sins of Omission: Critical Informatics Perspectives on Privacy in E-learning Systems in Higher Education. *Journal of the Association for Information Science and Technology* 73, 5 (May 2022), 708–725. https://doi.org/10.1002/asi.24575

[31] Priscilla M Regan and Jolene Jesse. 2019. Ethical challenges of edtech, big data and personalized learning: Twenty-first century student sorting and tracking. *Ethics and Information Technology* 21, 3 (2019), 167–179.

[32] Joel R Reidenberg and Florian Schaub. 2018. Achieving big data privacy in education. *Theory and Research in Education* 16, 3 (2018), 263–279.

[33] Dalia Ritvo, Christopher Bavitz, Ritu Gupta, and Irina Oberman. 2013. Privacy and Children's Data-An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act. *Berkman Center Research Publication* 23 (2013).

[34] Juan Carlos Rodríguez-del Pino, Enrique Rubio Royo, and Zenón Hernández Figueroa. 2012. A Virtual Programming Lab for Moodle with automatic assessment and anti-plagiarism features. (2012).

[35] Alan Rubel and Kyle ML Jones. 2016. Student privacy in learning analytics: An information ethics perspective. *The information society* 32, 2 (2016), 143–159.

[36] Madelyn R Sanfilippo, Brett M Frischmann, and Katherine J Strandburg. 2018. Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework. *Journal Information Policy* 8 (2018), 116–166. https://doi.org/10.5325/jinfopoli.8.2018.0116

[37] Madelyn Rose Sanfilippo, Brett M Frischmann, and Katherine J Strandburg. 2021. *Governing Privacy in Knowledge Commons*. Cambridge University Press.

[38] Madelyn Rose Sanfilippo and Katherine J. Strandburg. 2019. Privacy Governing Knowledge in Public Facebook Groups for Political Activism. *Information, Communication & Society* (2019). https://doi.org/10.1080/1369118X.2019.1668458

[39] Yan Shvartzshnaider, Madelyn Rose Sanfilippo, and Noah Apthorpe. 2022. GKC-CI: A unifying framework for contextual norms and information governance. *Journal of the Association for Information Science and Technology* (2022).

[40] Sharon Slade and Paul Prinsloo. 2013. Learning Analytics: Ethical Issues and Dilemmas. *American Behavioral Scientist* 57, 10 (Oct. 2013), 1510–1529. https://doi.org/10.1177/0002764213479366

[41] Enno Steinbrink, Lilian Reichert, Michelle Mende, and Christian Reuter. 2021. Digital Privacy Perceptions of Asylum Seekers in Germany: An Empirical Study about Smartphone Usage during the Flight. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–24.

[42] Michael Thomas. 2011. *Digital education: Opportunities for social collaboration*. Springer.

[43] Howard EA Tinsley and David J Weiss. 2000. Interrater reliability and agreement. In *Handbook of applied multivariate statistics and mathematical modeling*. Elsevier, 95–124.

[44] Peter Samuelson Wardrip, R. Benjamin Shapiro, Andrea Forte, Spiro Maroulis, Karen Brennan, and Ricarose Roque. 2013. CSCW and Education: Viewing Education as a Site of Work Practice. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work Companion* (San Antonio, Texas, USA) *(CSCW '13)*. Association for Computing Machinery, New York, NY, USA, 333–336. https://doi.org/10.1145/2441955.2442035

[45] Website. 2022. Crowdmark. https://crowdmark.com/help/how-does-crowdmark-work-with-moodle/.

[46] Website. 2022. Learning Tools Interoperability Core Specification. https://www.imsglobal.org/spec/lti/v1p3/.

[47] Website. 2022. Moodle Privacy API. https://docs.moodle.org/dev/Privacy_API.
[48] Website. 2022. Turnitin. https://www.turnitin.com/.
[49] Elana Zeide. 2017. The structural consequences of big data-driven education. *Big Data* 5, 2 (2017), 164–172.
[50] Elana Zeide and Helen Nissenbaum. 2018. Learner Privacy in MOOCs and Virtual Education. *Theory and Research in Education* 16, 3 (2018), 280–307. https://doi.org/10.1177/1477878518815340