EDM and Privacy: Ethics and Legalities of Data Collection, Usage, and Storage

Mark Klose
North Carolina State University
Raleigh, NC, USA
mwklose@ncsu.edu

Vasvi Desai
North Carolina State University
Raleigh, NC, USA
vcdesai@ncsu.edu

Yang Song
UNC at Wilmington
Wilmington, NC, USA
songy@uncw.edu

Edward Gehringer
North Carolina State University
Raleigh, NC, USA
efg@ncsu.edu

ABSTRACT

Imagine a student using an intelligent tutoring system. A researcher records the correctness and time of each of your attempts at solving a math problem, nothing more. With no names, no birth dates, no connections to the school, you would think it impossible to track the answers back to the class. Yet, class sections have been identified with no more data than this. This paper recounts shocking episodes where educational data was used to re-identify individual students, build profiles on students, and commit fraud. We look at the ethical principles that underlie privacy as it relates to research data, and discuss ethical issues in data mining relating to social networks and big data. We explore four major types of data used in EDM: (i) clickstream data, (ii) student-interaction data, (iii) evaluative data, and (iv) demographic data. Each type of data can be harmful if disclosed in particular contexts, even if all personally identifiable information is removed. We consider laws and legal precedents controlling access to student data in the United States and the European Union. This paper concludes by describing some practical situations in EDM and suggesting privacy policies that satisfy the ethical concerns raised earlier in the paper.

Keywords

Privacy, anonymization, de-identification, ethics, educational data mining

1. OUR DATA ARE MORE THAN VALUABLE

Educational data mining (EDM) analyzes student data from Learning Management Systems (LMSs) and stand-alone educational applications. Educational technology (EdTech) vendors use student data to analyze student performance, improve student models, and discover opportunities to boost learning. Any EdTech data breach or unjustified student tracking infringes student privacy, generates huge controversy, and produces big headlines. The ability to create auxiliary connections with other known information makes data valuable to both hackers and researchers. EDM researchers need to understand privacy risks raised by sensitive data.

1.1 Privacy risks of educational data breaches

One of the biggest leaks of student data was the Edmodo data breach. Edmodo is an EdTech company that provides coaching tools and a collaborative platform for K-12 students and teachers to communicate about course content, quizzes and assignments. The breach involved 11.7 gigabytes of data and over 77 million uniquely identifiable users, exposing at least 50 million usernames and 29 million emails. Edmodo did acknowledge the breach's occurrence, but by that time data was being sold by the hackers on the black market [9]. The breach was important, not because of the inherent value of the data itself, but rather because of how the data could be connected with auxiliary datasets. Having a list of hashed passwords is not useful; knowing that people tend to reuse passwords exposes other systems to greater risk. Leaking names and email addresses also left the students at greater risk of identification or additional tracking.

Since other breaches or publicly available datasets reveal personal information such as addresses or ethnicity, they can be cross-referenced to the leaked data to reveal a more complete identity. Companies shy away from controversy when it places their product or service at risk, and victims tend to not come forward, lest they sacrifice their privacy. It is important to take these breaches seriously, as any data leaked by research projects or products has more value now than before this large data breach.

Let's examine other educational data breaches. At Torrey Pines High School in San Diego, California, the online grading system was hacked to alter students' grades and transcripts [17]. This incident highlights risks like grade changes by unauthorized parties. In Montgomery County, Maryland, a student performed a brute-force attack on Naviance, an online platform for college and career readiness. The attack exposed sensitive data from 5962 accounts, including names,

Mark Klose, Vasvi Desai, Yang Song and Edward Gehringer "EDM and Privacy: Ethics and Legalities of Data Collection, Usage, and Storage" In: *Proceedings of The 13th International Conference on Educational Data Mining (EDM 2020)*, Anna N. Rafferty, Jacob Whitehill, Violetta Cavalli-Sforza, and Cristobal Romero (eds.) 2020, pp. 451 - 459

addresses, phone numbers, GPA, and SAT scores [12], that students trust will remain private and protected.

In the last two years, Chinese media have reported several cases where students' personal information, including their national identity card number, was stolen or leaked. Companies then used students' identities as phantom employees for tax fraud [7, 8]. One of the saddest cases related to an educational data breach occurred in 2016. After the national college entrance exam, a criminal group hacked a local university application system and acquired students' personal information, including phone numbers. The perpetrators posed as financial-aid officers then contacted students, asking them to transfer money into specified accounts before their financial aid could be delivered. One student contacted, Yuyu Xu, died from sudden cardiac arrest after discovering that it was a fraud [6].

1.2 De-identification is not enough

In a 2005 contest to devise better movie-recommendation systems, Netflix released 10 million movie rankings by 500,000 customers after removing all direct customer-related information. Two University of Texas researchers showed that simple anonymization fails to preserve privacy; researchers connected anonymized Netflix dataset entries with distinct users in the Internal Movie Database [43]. Similar risks are present in anonymized datasets used for EDM research.

Another compromise of anonymized data occurred when the "Tastes, Ties, and Time" (T3) project released de-identified Facebook profile data. All personally identifiable data was removed, such as names, email addresses, university name, and names of friends. However, the dataset's associated code book provided a list of students' majors and state or country of origin. Within a couple of days, researchers at University of North Carolina at Chapel Hill and University of Wisconsin-Milwaukee identified the "anonymous northeastern university" as Harvard. This raised significant privacy concerns as research assistants at Harvard University who were "friends" with some students in question, had deeper access to profiles than the general public. Both the Harvard IRB and Facebook had approved the project [69].

In one case, researchers collected clickstream data from multiple classrooms across the country instead of personally identifiable information (PII) or demographic data about an individual student. They created clusters of students from log files, recording time and correctness of students' responses. These clusters were enough to identify classes of gifted students and extract demographic data about student groups [67]. When one cluster missed a day's worth of work, the researchers cross-referenced potential classrooms with announcements of a field trip. This resulted in a single classroom being identified using only anonymized data.

Common de-identification techniques include: *Anonymization*, where all PII is simply removed from the dataset; *hashing*, where multiple fields (e,g., last name and email address) are hashed into a single value, and replace the original fields in the record; *swapping*, where some field, such as a name, is switched to apply to someone else's record; and *noising*, where data values are perturbed (changed) in some way [37]. These common de-identification techniques can have adverse effects on data quality [14]. Protecting students' privacy by removing re-identifiable attributes from data can reduce the data's utility for analysis [67]. Noising data can diminish performances of supervised learning models [44]. Despite not changing aggregations, swapping has similar effects [41]. Thus, it is crucial to balance privacy with utility. Ohm (2009) warns that "the utility and privacy of data are linked, and so long as data is useful, even in the slightest, then it is also potentially re-identifiable" [47].

Building profiles for targeted advertising also endangers student data privacy. Data can be collected by amassing emails or system interactions, like websites visited. Students can be identified and targeted on the basis of their answering patterns, e.g., what questions they answered correctly. Google, which provides the educational content platform GSuite for Education, has been alleged to have built personalized profiles of students based on their GSuite interactions, and to have scanned students' emails to target advertising [23, 28]. Selling the data to third-party vendors without consent would raise severe ethical questions.

In these cases, students' identities and information were used or revealed without explicit permission, undermining the idea of consent. Although releasing someone's homework grade or test score seems trivial, researchers need clear understanding of what constitutes legal and ethical usage of student data so students remain protected while the EDM research efforts continue into noble frontiers.

2. ETHICAL PRINCIPLES RELATING TO EDUCATIONAL RESEARCH DATA

Deciding what constitutes "responsible use" bridges research ethics and other ethics subfields. Each field emphasizes different aspects of the research process. As with any ethical discussion, clarifications of these terms and new realizations of technologies causes these principles to evolve to reflect the state of EDM research. Several analyses have looked at key principles in a more abstract form [48, 51, 59], but these works are too broad to answer specific questions. This paper seeks to highlight key principles from each subfield and applications to specific areas of EDM research.

2.1 Research ethics

Much of the literature on research ethics derives from the Nuremberg Code [34], the Helsinki Declaration [2], and the Belmont Report [15, 35, 65]. But the Belmont report lacks specifics on internet-mediated research [1]. The Menlo Report [4] extends principles from the Belmont Report to computing centric research. It adopts three principles found within the original Belmont Report, and adds a new fourth principle, respect for law and public interest.

2.1.1 Respect for Persons

The Belmont Report establishes the principle of *respect for persons* through two key frames: treating individuals as autonomous agents and entitling individuals to protections [65]. The Menlo Report adds consideration of computer systems and data that directly impact people who are typically not research subjects themselves [4]. This impacts the concept of informed consent. Informed consent comprises three

concepts: notice, comprehension and voluntariness [4]. For EDM research, consent documents must not promise improved service or instruction in return for participation; this could be interpreted as coercion. This is relevant to intelligent tutoring systems (ITSs)—students unwilling to allow an ITS to use their data for research purposes should not thereby be academically disadvantaged.

The Menlo Report reiterates consent from one person does not constitute consent from all members of their group, and consent given for one research purpose should not be considered valid for different purposes. Since data subjects are co-owners of educational data [40], concepts such as downstream consent [13] should be considered for applications like educational data warehouses. To further protect individuals, the Menlo Report suggests de-identification of data. De-identified data can fit into the special regulatory category of "pre-existing public data," which affords more opportunity for exemptions granted by research ethics boards.

2.1.2 *Beneficence*

For identifying of potential benefits and harms, the Menlo Report targets systems assurance (confidentiality, availability, integrity) and individual and organizational privacy [4]. Within EDM, this means identifying likely flaws or biases in ITSs prior to deployment or introducing protections for model inference and model inversion attacks [20, 52, 56, 58].

When collection or storage of high-risk data is necessary, the Menlo Report suggests to destroy data once past the retention period of scientific reproducibility, which is commonly 3 years at minimum [11, 46]. A tension exists between data retention for research replication and ensuring privacy of data subjects, which will be discussed further in section 3.2. Utilizing data aggregations prevents the need to store sensitive information that could tie back to a specific student or class.

2.1.3 *Justice*

With regard to *justice*, the Menlo Report declares research should not target specific people or groups based on attributes such as technical competency or personal demographics [4]. For EDM researchers creating some model or product, this discourages using convenience samples such as classrooms the researcher worked with previously. Instead, research should target classrooms or groups of students where the potential intervention provides the most benefit. Using prior data providing an accurate cross-section of the larger community being studied is more favorable than potentially excluding future groups from participation.

The Menlo Report compares actively excluding groups out of prejudice and actively including entities willing to cooperate and consent. Including entities demonstrates the principles of Respect for Persons and Beneficence outlined earlier. Specifically targeting subjects through coercion undermines legitimate research and violates the principle of Justice [4].

2.1.4 *Respect for Law and Public Interest*

The Belmont Report implicitly classifies respect for the law and greater public interest as an aspect of Beneficence. The Menlo Report considers it a fourth principle with two applications: compliance and transparency/accountability [4]. These provide some assurance of public good whenever identifying stakeholders is difficult or impossible. Lacking transparency and accountability weakens current research projects at hand and learning analytics research credibility as a whole.

Within EDM research, compliance, transparency, and accountability all require researchers to understand relevant laws in their jurisdictions. Researchers are culpable for being up-to-date on laws and regulations where they perform research. Transparency means releasing source code or clearly communicating what information is collected and what computations are performed. Transparency is in the interest of research subjects, the beneficiaries of research, and research ethics boards as they audit projects where necessary.

2.2 Social networks and ethics

With a growing level of research incorporating data directly from social networks, EDM must consider the various ethical principles guiding online behaviors. The disconnect of individuals from online identities must be considered while using social networking data and its derivations. Seeing incomplete aspects of an individual's personal life through their social network lens affects and alters the perception of them.

Users curate their identities in an online setting [61]. Some students may only use social network services to communicate within specific spheres like family, workplaces, or friends. Students' online actions and behaviors may not truly reflect themselves as learners, but as reflections of the sphere they are in. Social networks have distinct group dynamics, similar to the real world, further complicating the trustworthiness profiles provide as a snapshot of the student. In theory, social network users should be exposed to opinions of diverse worldwide users, but in practice, views and news feed algorithms constrict types of content users see [50]. In online settings, users tend to subjugate their identities to the group identity they participate in (e.g., student, liberal, conservative, Christian, Muslim), in order to conform to the group [50]. With these considerations in mind, this may devalue the student's social network presence to the point where social network data may lack enough integrity to be used.

Some broad concerns with using social network data include availability of users' data to third parties to create marketing profiles, using data mining applications without their knowledge or consent, surveillance by law enforcement, or having third party applications collect and publish user data without notification [66]. Social networking services provide privacy controls for users; however, failure to understand implications of sharing information on a social networking service results in decreased privacy for users in relation to outside actors such as researchers [5].

When releasing de-identified Facebook account data as part of the T3 project, researchers placed limited concern on research ethics and students' privacy. Utilizing data was not the problem; failing to recognize how collection methods affected privacy is the issue. While acquiring profile data, researchers could have broader access than originally intended by the profile owner. This happens if researchers have prior connections through memberships in their organization or having mutual connections to the profiles. If research combines educational and social networking data but disrespects

privacy standards laid out by the student on platforms like Facebook (or if researchers fail to seek further consent from students about using their social network data), then this breaches the student's overall privacy [69].

2.3 Big-data ethics

Data possesses properties distinguishing itself from other advanced forms of technology, not limited to: its regarding as an aspect of societal infrastructure; its interconnectedness; its dynamic nature for discovery beyond original purpose; its real-time analysis and decision-making possibilities; its usability regardless of where, when, and for what purpose it was collected; its reusability for unexpected purposes to reveal unexpected information (the core purpose of data mining); its intrusiveness due to storing data about individuals in multiple databases; its ownership issues, especially in education settings [26, 40]. Each individual datum is useless without context and associated metadata. By this construction, value added to data provides its potential for misuse. In EDM, positive outcomes for students come from discrete products or further insight on learning motivations and processes; this does not exclude potential misuse by researchers.

Although this paper will not discuss algorithmic fairness in detail, the concept applies in big data ethics. Many practices classify or regress individual experiences into common baselines based on socioeconomic status, race, ethnicity, or gender without explanatory data. Division into classification groups and averaging metrics stereotypes students. Unchecked stereotyping could rehash old prejudices that negatively affect research itself. The lack of care to blindly use basic classification groups can be extreme enough to break the principle of "doing good work" [26]. Instead, research should favor groups created by methods like Topological Data Analysis [22] and other Bayesian models that cluster outside of traditional demographic groupings.

2.4 Ethical uses of specific educational data

There are four kinds of data commonly used in EDM that have further ethical concerns for researchers: clickstream, student interaction, evaluative, and demographic data.

2.4.1 Clickstream data

At minimum, clickstream data provides information that some generic user initiated an interaction at a given time. Although relatively safe on its own, a classroom worth of students generating clicks can reveal the location of the classroom, especially if the classroom functions on a daily or weekly routine. Studies have already shown tracking IP addresses to reveal geolocation [38], which shows the potential for this to be done for clickstream data as well. Utilizing this aspect of clickstream data allowed Yacobson et al. to identify a gifted student classroom from a completely anonymized dataset of over 500 students after clustering time of clicks and correctness of answers. Once a class deviated from the schedule due to a field trip, researchers then identified the school and classroom in question [67].

2.4.2 Student interaction data

Student interaction data includes peer assessments, online discussion forums, and team-member evaluations—data with a clear writer-respondent relationship. These interactions directly reflect the respondent's viewpoints, which may violate privacy if shared outside of the student-teacher relationship when they cast aspersions on the student. If negative comments are given about the writer, and that information somehow leaves the model or is revealed to an outside source, this could affect student's relationships and future prospects. Similarly, sharing class forums regarding sensitive subjects like sexuality to wider audiences is not proper since this could potentially identify and harm a student.

2.4.3 Evaluative data

Evaluative data references include grades and other inputs to predictive analytics models. In educational settings, clear benefits to predictive models include quality assurance and improvement of instruction, tracking and predicting retention rates, and enabling the development of adaptive learning [3, 57]. These same models could influence later interactions between students and instructors, thus affecting the relationship and trust—a proven factor in the academic success of students [19, 21, 39, 53]. For example, if a predictive model flags a student for high potential of failure and dropout from a course, the instructor may focus interventions on that student. This could overcome other reasons for a student's poorer performance, thus remedying symptoms rather than determining underlying causes for the struggles.

2.4.4 Demographic data

Many studies looked at how simple demographics can identify a non-negligible number of individuals [24, 60]. Student demographic data can be combined with other data to infer identities of students. In the T3 project, student Facebook data identified many individuals as being the only Harvard freshman student from a certain state or country. Identifying an exact student is possible when combining news announcements or other university materials [49]. With the growing number of data breaches like the Edmodo case and the noted intrusiveness of big data due to an individual's membership in many databases, this leads to a risk that often goes unnoticed for smaller research applications. For EDM researchers, having researchers redact some demographic information, when not integral to research, may assist students in controlling their information and privacy.

In summary, it is vital to see how ethics does not adhere to data itself; the researchers themselves and how the data are used carries significant ethical implications. Understanding the scope of data collection, storage, and usage ultimately impacts the ethics of research and benefits for learners.

3. LAWS AND LEGAL PRECEDENTS

Legal regimes vary substantially throughout the world; an exhaustive comparison is beyond the scope of this paper. Legal frameworks for educational data exist in other countries, but their impacts are less clear [18, 62, 63, 64]. We focus on the two largest EDM research communities: the United States and the European Union.

3.1 United States

In the United States, the most relevant legislation is the Family Educational Rights and Privacy Act (FERPA). Enacted in 1974 after widespread concern about intrusive psychological testing of students, FERPA defined the circum-

stances which allow schools to release a student's "education records" to outsiders (including EDM researchers). Personally identifiable information (PII) about a student must not be disclosed unless the student, or the parents if the student is under 18 years old, give their prior consent. The law applies to all schools that receive funds under a program administered by the US Department of Education. In practice, this includes virtually all colleges and universities, as well as public (but not private) elementary and secondary schools.

Under the law, PII includes students' names, names of parents and family members, Social Security or student ID numbers, biometric records, and other indirect identifiers including date or place of birth and mother's maiden name. It also includes "[o]ther information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty."

This raises two main issues: What is an education record, and what does the "other information" mentioned above include? For example, does clickstream data collected by an ITS count as an "education record"? The most relevant court case is Owasso v. Falvo (534 US 426 (2002)). This case arose in Oklahoma, when a teacher had students peer-grade each other's papers. Papers were collected from students and passed out to other students. The teacher called out the correct answers, and each student would mark answers on the paper in front of them as correct or incorrect. The school district was sued by the a student's mother who said that her son, who had not scored very well, had been embarrassed when a fellow student called out his score.

The case eventually reached the US Supreme Court, which ruled unanimously that peer grades did not constitute "educational records." FERPA established a two-part test to determine what was an educational record: (i) The material must "directly relate to the student" and (ii) must be maintained by the institution or an individual acting on the institution's behalf. The decision turned on the test's second part. The court ruled grades were not "maintained by .. an individual acting on behalf of the institution," at least until entered in the teacher's gradebook. The court did not rule whether teachers' gradebooks are an educational record.

The Owasso decision seems to imply that FERPA does not prevent the disclosure of student classwork and homework to outside researchers, except possibly if outsiders can use it to discover students' grades for the assignment. In general, data from web-based participatory learning tools is not covered under FERPA [27]. Note that this is a legal judgment, not an ethical one, since disclosure of student information from some such tools may allow re-identification by others.

However, one clause in FERPA implies this situation may not last. The clause on linkable information implies that what constitutes PII changes as technology changes [68]. As datasets become higher dimensional, the possibility of using an auxiliary dataset to re-identify people grows [42]. Thus, every researcher releasing a de-identified dataset should be familiar with the growing risks.

A distinction should also be made between datasets used for analytics and datasets used for intervention [30]. A researcher simply analyzing effects of some practice or tool on student learning has little need to track individual identities. If the dataset is used for intervention—to improve experiences of particular students—obviously the students' identities must be preserved. In this case, FERPA may still apply, since neither the law nor Owasso v. Falvo clearly delineates what kind of research data constitutes an "educational record." Fortunately, interventions are often in house; data of this nature would rarely be important to outside researchers. However, if interventions are with students in other institutions, it would be worth seeking legal guidance.

3.2 European Union

The European Union adopted the General Data Protection Regulation (GDPR) in April 2016, which took effect in May 2018. GDPR applies to processing "personal data" tied to an identifiable person. For practical purposes, this seemingly is the same as FERPA [45] (except GDPR also applies outside educational contexts). According to GDPR [33],

> [A]n identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This is subject to the same uncertainties as FERPA. One place where the two laws differ is in the EU, the subject must consent to use of their personal data: the researcher must secure "a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her ... Silence, pre-ticked boxes or inactivity should not ... constitute consent [recital 32]" [29].

Another consideration is the GDPR's signature provision: the "right to be forgotten." If the subject of the data withdraws consent, the data must be erased. The data must also be erased when no longer needed for the purpose (e.g., research) that it was collected for [29].

4. IMPLICATIONS OF EDM RESEARCH

Having discussed privacy risks, ethical considerations, and legal risks for EDM researchers, we now examine current privacy concerns and work needed in the near future. Through correspondence with EDM 2019 researchers and reflection on our own research, we identify the following areas as requiring attention to the principles and risks established earlier.

4.1 Crawling learners' data outside a platform

Though most EDM researchers use data generated *within* educational platforms/systems such as MOOCs/ITSs, sometimes it can be tempting to acquire data on learners *beyond* a specific tool and beyond the course duration. When researchers use the learners' information to access their data on social web platforms after they have finished a MOOC,

for example, more research questions can be answered, such as "does displaying MOOC certificates have an impact on learners' career paths?" Chen et al. traced the learners' profile data overtime on Gravatar, StackExchange, GitHub, Twitter, and LinkedIn after the MOOCs to investigate the impact of MOOCs in the long-term [10]. Chen et al. used data from 18 MOOCs and reported they could reliably identify the highest of 42% of the learners in a MOOC on social web platforms. The MOOC data (from edX) they started with had the usernames, full names, email addresses. Therefore, it is not a surprise that a high percentage of learners can be identified. However, crawling data of learners on five social-media platforms several years after they have finished a MOOC does bring up privacy concerns.

Arguably, learners' profile and posts are the data available to the public, but EDM researchers are able to join learners' data from an educational platform with learners' data on social web platforms, which may give researchers too much power in mining learners' data after they have finished their learning. Considering the learners' additional data can potentially be crawled, the sharing and reusing learners' data should be backed with appropriate legal agreements. For example, Yacobson et al. suggested to "ban linking application data with external data sources" [67].

4.2 Community consensus on learners' privacy

Researchers need data with high utility, but the effort to anonymize data hurts this. In other words, keeping datasets of high utility and high privacy level concurrently is hard. De-identification protects learners' privacy, but too strict de-identification can negatively affect analysis [37].

Besides, there is always a risk that de-identified data can be re-identified, especially if de-identification is done in a shallow approach (e.g., by removing learners' full names, emails). The reason is that learners' personal "footprints" also reside in their artifacts and interaction patterns with the educational platform. Yacobson et al. presented an example where they re-identified the school that the learners were in based on de-identified clickstream logs [67]. Similarly, being teaching software engineering long enough, the paper's fourth author would argue it is possible to tell learners' demographic characteristics by reading their code.

The tension between usefulness and anonymity of the data is not likely to be solved by legislation. Hoel et al. analyzed three different privacy frameworks in selected countries [32] and presented clear differences on value focuses – e.g., the European framework focuses on individuals and the Asian privacy framework focuses on the organizations. Though we have observed that the legislation in one region can have an influence on future legislations in other countries [25], the time for those data protection legislations to "converge" (if possible) may take a long tune.

As a result, the best short-term result we can have could be a community consensus in the EDM and LA (Learning Analytics) research communities. In addition, when an anonymized dataset is posted/shared, we advocate that researchers limit the *additional information* provided about the student population to reduce the risk of re-identification. For example, a dataset generated by "graduate Algorithms II students in an R2 university on the east coast of the U.S." is more likely to be re-identified than a dataset generated by "students in a graduate Algorithms course".

4.3 A protocol for configuring privacy policies

A common definition for privacy is the POQ framework: "some person or persons P, some domain of information O, and some other person or persons Q, such that P has privacy regarding O with respect to Q" [54]. For example, Alice (P) took an online course with sponsorship from her employer (Q). Her course completion status (O) is accessible by her employer; in other words, P does not have privacy regarding to O with respect to Q. This privacy policy may not be configurable by the learner based on the privacy policy of some online learning platform, for example, edX [16].

Though the POQ framework can serve as a basis for privacy policies, it leaves out some essential components [55]. The privacy protocol helps learners manage privacy in any learning environment. Hoel and Chen suggest the policy should achieve privacy by negotiating "with each student" [31]. Certain components should be added to the POQ framework to extend it for educational service providers.

First, the lifespan of privacy policies should be added. To follow the example above, when Alice leaves the current company, should the former employer still have access to Alice's records on edX? Besides, the purpose of the planned usage of the data (e.g., to gain generalized knowledge of the student population, to predict individual student's success in a course, etc.) should be part of the protocol. Educational data can be "justifiably collected and analyzed for one educational context, but not another" [55]. Moreover, privacy protocols should stipulate that learners can access data analysis results based on their data. It is common for researchers to use students' data to predict student success (or failure) [36]. When there is a prediction, not all the students are willing to see this information, and some educators may not be ready to share this information with students.

5. CONCLUSION

Overall, it does not seem likely that legislation related to educational-data privacy in different countries will be harmonized in the near future. Many datasets from education settings have re-identification risk, even after personal information is removed. Therefore, the research community has to move forward and establish a certain level of consensus to discourage research projects that are of high ethical risk and relatively low research value. Seeking excessive personal data on learners from the social web could be one of them. EDM researchers and third-party tool providers should take responsibility to foster a trusting relationship between learner and teacher, and learner and institution.

Like any survey paper, this work is not specific enough to guide each and every research action, and it will not cover all legislation relevant to an EDM researcher. Within a couple of years, most of this information will be supplanted by new legislation, research paradigms, innovative technologies, and research by the exciting generation of upcoming EDM researchers. Being aware of and vigilant against all possible risks will protect the interests of the EDM research's most important stakeholders: learners, students and teachers.

6. REFERENCES

[1] I. F. Anabo, I. Elexpuru-Albizuri, and L. Villardón-Gallego. Revisiting the Belmont Report's ethical principles in internet-mediated research: perspectives from disciplinary associations in the social sciences. *Ethics and Information Technology*, 21(2):137–149, 2019.

[2] W. M. Association et al. World Medical Association Declaration of Helsinki. Ethical principles for medical research involving human subjects. *Bulletin of the World Health Organization*, 79(4):373, 2001.

[3] J. T. Avella, M. Kebritchi, S. G. Nunn, and T. Kanai. Learning analytics methods, benefits, and challenges in higher education: A systematic literature review. *Online Learning*, 20(2):13–29, 2016.

[4] M. Bailey, D. Dittrich, E. Kenneally, and D. Maughan. The Menlo Report. *IEEE Security Privacy*, 10(2):71–75, Mar 2012.

[5] N. Baym. Social Networks 2.0. *The handbook of Internet studies*, 2:384, 2011.

[6] 李栋． 黑客入侵报名网站盗取徐玉玉信息 (Hacker attacked registration website and stole Xu Yuyu's information) , Sep 2016. http://tc.people.com.cn/n1/2016/0910/c183008-28705847.html.

[7] 陈晶晶． 学生信息不容泄露 (Students' information must not be leaked) , Sep 2018. http://m.people.cn/n4/2018/0917/c3521-11620211.html.

[8] 陈禹潜． 泄露学生个人信息没有理由放过 (There is no reason to allow someone who leaks students' personal information to get away without punishment) , Feb 2020. http://edu.people.com.cn/gb/n1/2020/0207/c1053-31575345.html.

[9] A. Casares. Deep dive into the Edmodo data breach, Oct 2017. https://medium.com/4iqdelvedeep/deep-dive-into-the-edmodo-data-breach-f1207c415ffb.

[10] G. Chen, D. Davis, J. Lin, C. Hauff, and G.-J. Houben. Beyond the MOOC platform: gaining insights about learners from the social web. In *Proceedings of the 8th ACM Conference on Web Science*, pages 15–24, 2016.

[11] Columbia University. Data Retention: Research, 2020. https://research.columbia.edu/content/data-retention.

[12] A. Constantino. Data breach exposed personal info of nearly 6,000 Montgomery County student accounts | WTOP, 2019. https://wtop.com/montgomery-county/2019/12/data-breach-exposed-personal-info-of-nearly-6000-montgomery-county-student-accounts/.

[13] A. Cormack. Downstream consent: A better legal framework for Big Data. *Journal of Information Rights, Policy and Practice*, 1(1), 2016.

[14] J. P. Daries, J. Reich, J. Waldo, E. M. Young, J. Whittinghill, A. D. Ho, D. T. Seaton, and I. Chuang. Privacy, anonymity, and big data in the social sciences. *Communications of the ACM*, 57(9):56–63, 2014.

[15] H. Drachsler and W. Greller. Privacy and Learning Analytics—it's a DELICATE issue. *Proceedings of LAK: International Conference on Learning Analytics & Knowledge*, 16, 2016.

[16] edX. Notice: On may 15, 2018, edx adopted an amended privacy policy, providing as follows. https://www.edx.org/edx-privacy-policy.

[17] S. Foo. School district officials investigating possible breach of online grading system, Feb 2020. https://www.kusi.com/school-district-officials-investigating-possible-breach-of-online-grading-system/.

[18] L. Forde, J. D'Andrea, and N. Stornebrink. Legal matters: Schools and data privacy, May 2015. https://www.teachermagazine.com.au/articles/legal-matters-schools-and-data-privacy.

[19] P. B. Forsyth, L. L. Barnes, and C. M. Adams. Trust-effectiveness patterns in schools. *Journal of Educational Administration*, 2006.

[20] M. Fredrikson, S. Jha, and T. Ristenpart. Model inversion attacks that exploit confidence information and basic countermeasures. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS 15*, Oct 2015.

[21] R. D. Goddard, M. Tschannen-Moran, and W. K. Hoy. A Multilevel examination of the distribution and effects of teacher trust in students and parents in urban elementary schools. *The Elementary School Journal*, 102(1):3–17, 2001. http://www.jstor.org/stable/1002166.

[22] A. Godwin, A. R. H. Thielmeyer, J. A. Rohde, D. Verdin, B. S. Benedict, R. A. Baker, and J. Doyle. Using topological data analysis in social science research: unpacking decisions and opportunities for a new method. In *2019 ASEE Annual Conference & Exposition*, Tampa, Florida, June 2019. ASEE Conferences. https://peer.asee.org/33522.

[23] D. Golightly. Google, New Mexico AG Spar Over Chromebook Student Data Collection, 2020. https://www.androidheadlines.com/2020/02/google-new-mexico-attorney-general-lawsuit-student-data-collection-chromebook.html.

[24] P. Golle. Revisiting the uniqueness of simple demographics in the US population. In *Proceedings of the 5th ACM workshop on Privacy in electronic society*, pages 77–80, 2006.

[25] G. Greenleaf. GDPR-Lite and Requiring Strengthening—Submission on the Draft Personal Data Protection Bill to the Ministry of Electronics and Information Technology (India). *UNSW Law Research Paper*, pages 18–83, 2018.

[26] D. J. Hand. Aspects of data ethics in a changing world: where are we now? *Big Data*, 6(3):176–190, 2018.

[27] H. Heevner. *FERPA in a Modern World*. PhD thesis, Pennsylvania State University, 2017. https://sites.psu.edu/heevner/files/2017/04/Heevner_FERPA_Final-1fpmgjy.pdf.

[28] B. Herold. Google Under Fire for Data-Mining Student Email Messages, 2014. https://www.edweek.org/ew/articles/2014/03/13/26google.h33.html.

[29] T. Hoel and W. Chen. Implications of the European data protection regulations for learning analytics design. In *Workshop paper presented at the international workshop on learning analytics and*

educational data mining (LAEDM 2016) in conjunction with the international conference on collaboration technologies (CollabTech 2016), Kanazawa, Japan-September, pages 14–16, 2016.

[30] T. Hoel and W. Chen. Towards Developing an Educational Maxim for Privacy and Data Protection in Learning Analytics. In *EC-TEL Workshop on Ethics and Privacy for Learning Analytics, Tallinn, Estonia, September*, volume 12, 2017.

[31] T. Hoel and W. Chen. Privacy and data protection in learning analytics should be motivated by an educational maxim—towards a proposal. *Research and Practice in Technology Enhanced Learning*, 13(1):20, 2018.

[32] T. Hoel, W. Chen, and D. Griffiths. Is international consensus about privacy policies for learning analytics possible? In *Draft workshop paper presented at LAK17 workshop on LA policies*, 2017.

[33] L. Irwin. The GDPR: What exactly is personal data?, Jan 2020. https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data.

[34] A. C. Ivy and L. Alexander. The Nuremberg Code. *Trials of war criminals before the Nuremberg military tribunals under control council law*, 10:181–182, 1949.

[35] D. Kay, N. Korn, and C. Oppenheim. Legal, risk and ethical aspects of analytics in higher education. *Analytics series*, 2012.

[36] G. Kennedy, C. Coffrin, P. De Barba, and L. Corrin. Predicting success: how learners' prior knowledge, skills and activities predict MOOC performance. In *Proceedings of the fifth international conference on learning analytics and knowledge*, pages 136–140, 2015.

[37] M. Khalil and M. Ebner. De-identification in learning analytics. *Journal of Learning Analytics*, 3(1):129–138, 2016.

[38] R. Koch, M. Golling, and G. D. Rodosek. Geolocation and verification of IP-addresses with specific focus on IPv6. In *Cyberspace safety and security*, pages 151–170. Springer, 2013.

[39] S.-J. Lee. The relations between the student–teacher trust relationship and school success in the case of Korean middle schools. *Educational studies*, 33(2):209–216, 2007.

[40] C. F. Lynch. Who prophets from big data in education? New insights and new challenges. *Theory and Research in Education*, 15(3):249–271, 2017.

[41] K. Mivule. Data Swapping for Private Information Sharing of Web Search Logs. *Procedia Computer Science*, 114:149–158, Sep 2017.

[42] A. Narayanan and E. W. Felten. No silver bullet: De-identification still doesn't work. *White Paper*, pages 1–8, 2014. https://www.cs.princeton.edu/ arvindn/publications/no-silver-bullet-de-identification.pdf.

[43] A. Narayanan and V. Shmatikov. Robust De-anonymization of Large Sparse Datasets. *2008 IEEE Symposium on Security and Privacy (sp 2008)*, 2008.

[44] D. F. Nettleton, A. Orriols-Puig, and A. Fornells. A study of the effect of different types of noise on the precision of supervised learning techniques. *Artificial Intelligence Review*, 33(4):275–306, 2010.

[45] A. A. of Collegiate Registrars and A. Officers. Comparing FERPA and GDPR, Mar 2018. https://www.aacrao.org/resources/newsletters-blogs/aacrao-connect/article/comparing-ferpa—gdpr.

[46] Office of Research Integrity. Data Management, 2020. https://ori.hhs.gov/education/products/rcradmin/topics/data/tutorial_11.shtml.

[47] P. Ohm. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57:1751, Aug 2009.

[48] A. Pardo and G. Siemens. Ethical and privacy principles for learning analytics. *British Journal of Educational Technology*, 45(3):438–450, 2014.

[49] M. Parry. Harvard researchers accused of breaching studentsĂŹ privacy. *The chronicle of higher education*, 10, 2011.

[50] M. Parsell. Pernicious virtual communities: Identity, polarisation and the Web 2.0. *Ethics and Information Technology*, 10(1):41–56, 2008.

[51] P. Prinsloo and S. Slade. Ethics and learning analytics: Charting the (un)charted. In *Handbook of Learning Analytics*. SOLAR, 2017.

[52] M. A. Rahman, T. Rahman, R. Laganiere, N. Mohammed, and Y. Wang. Membership inference attack against differentially private deep learning model. *Transactions on Data Privacy*, 11:61‘Ă‘Ş79, Feb 2018. http://www.tdp.cat/issues16/tdp.a289a17.pdf.

[53] L. S. Romero. Trust, behavior, and high school outcomes. *Journal of Educational Administration*, 2015.

[54] A. Rubel and R. Biava. A framework for analyzing and comparing privacy states. *Journal of the Association for Information Science and Technology*, 65(12):2422–2431, 2014.

[55] A. Rubel and K. M. Jones. Student privacy in learning analytics: An information ethics perspective. *The information society*, 32(2):143–159, 2016.

[56] A. Salem, Y. Zhang, M. Humbert, P. Berrang, M. Fritz, and M. Backes. ML-Leaks: Model and data independent membership inference attacks and defenses on machine learning models. *Proceedings 2019 Network and Distributed System Security Symposium*, 2019.

[57] N. Sclater, A. Peasgood, and J. Mullan. Learning analytics in higher education. *London: Jisc. Accessed February*, 8(2017):176, 2016.

[58] R. Shokri, M. Stronati, C. Song, and V. Shmatikov. Membership inference attacks against machine learning models. *2017 IEEE Symposium on Security and Privacy (SP)*, 2017. https://www.cs.cornell.edu/ shmat/shmat$_o ak$17.*pdf*.

[59] S. Slade and A. Tait. Global guidelines: Ethics in learning analytics. *International Council for Open and Distance Education*, Mar 2019.

[60] L. Sweeney. Simple demographics often identify people uniquely. *Health (San Francisco)*, 671:1–34, 2000.

[61] S. Turkle. *Life on the Screen*. Simon and Schuster, 2011.

[62] United Kingdom Parliament. Children Act 1989, c. 41, 1989.

http://www.legislation.gov.uk/ukpga/1989/41/contents.
[63] United Kingdom Parliament. Education Act 1996, c. 56, 1996. http://www.legislation.gov.uk/ukpga/1996/56/part/IX/chapter/IV.
[64] United Kingdom Parliament. Education Act 2005, c. 18, 2005. http://www.legislation.gov.uk/ukpga/2005/18/part/4/crossheading/information.
[65] US Department of Health Human Services et al. The Belmont Report, 1979. https://videocast.nih.gov/pdf/ohrp_appendix_belmont_report_vol_2.pdf.
[66] S. Vallor. Social Networking and Ethics. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Winter 2016 edition, 2016. https://plato.stanford.edu/archives/win2016/entries/ethics-social-networking/.
[67] E. Yacobson, G. Alexandron, and S. Hershkovitz. De-identification is not enough to guarantee student privacy: De-anonymizing personal information from basic logs. In *Companion Proceedings 10th International Conference on Learning Analytics & Knowledge (LAK20)*, Dec 2019.
[68] E. Young. Educational privacy in the online classroom: FERPA, MOOCs, and the big data conundrum. *Harv. JL & Tech.*, 28:549, 2014.
[69] M. Zimmer. "But the data is already public": on the ethics of research in Facebook. *Ethics and information technology*, 12(4):313–325, 2010.