THE DATAFIED STUDENT:

Why Students' Data Privacy Matters and the Responsibility to Protect It

APRIL 2022

Kyle M. L. Jones (MLIS, PhD) • Indiana University-Indianapolis (IUPUI)

FUTURE OF PRIVACY FORUM

EXECUTIVE SUMMARY

Some higher education institutions (HEIs) are developing their educational data mining and analytic capacities, while others are purchasing technologies to support their interests in analytics. These efforts involve a broad array of practices that many consider to be a form of learning analytics. Learning analytics are designed to improve student learning outcomes, provide students with just-in-time resources, and make predictions to direct student behaviors toward actions that lead to academic success. Institutions also use learning analytics to discover cost savings and to increase efficiencies. To support learning analytics initiatives, institutions are increasing both their collection of students' data and information and the types of student data they collect.

Learning analytics raises significant privacy issues, such as the potential for bias, racial and other discrimination, and reductive analyses that could compromise or even foreclose students' future education and job opportunities. The increasing collection of student data raises red flags about whether such practices invade privacy, but arguably more notable is the power that institutions gain over their students. Universities can use their ubiquitous data and technology infrastructures to capture student life and behaviors at a granular level, through techniques such as mandated digital learning systems and tracking students' locations via radio-frequency identification chips in their university ID cards. Institutional rules, norms, and expectations—all formally codified or verbally relayed—hold sway over students. The power differential between students and institutional actors, such as administrators, faculty, and staff, is immense. With learning analytics, institutions use data visualization, predictive measures, and targeted messaging to mold student behaviors in ways that potentially and negatively affect their autonomy and direct their choices. Students are mostly unaware of these techniques and cannot remove themselves from a university's network of technology. The result is that students have little agency to contest learning analytics driven by privacy-invading data practices and technologies.

Policymakers and higher education stakeholders could benefit from deeper understanding of student privacy, but there is scant literature explaining its value, and arguments rely too heavily on compliance with federal law. To foster this understanding, this brief explains that student privacy is rooted in contextual values and expectations, is critical to intellectual freedom, and supports students in their various institutional relationships. If learning analytics is to mature in alignment with the privacy protections and ethical practices that students and other stakeholders expect, HEIs must commit to the following actions:

- Higher education actors should review analytic initiatives for fairness, bias, and privacy problems.
- The academic community must reflect on the consequences of privacy-invading technologies, including their ability to prop up administrative interests.
- Stakeholders, including students, need to participate in the co-design of learning analytics to ensure an equitable, agreeable vision and implementation of the technology.

INTRODUCTION

It is no longer abstract or far-fetched to think of higher education institutions (HEIs) as generators of massive amounts of data that can be analyzed. In years past, administrative conversations and edtech literature previously focused on a university's *potential* to create big data (in the technical sense) and to capitalize on Big Data (in the sociopolitical sense).[1] Today, HEIs increasingly have the skill sets and infrastructures to create large, minable data sets,[2] and administrations increasingly want to restructure colleges and universities as data-focused, algorithmically driven institutions to reimagine teaching and learning.[3] HEIs have opportunities to use big data to inform and improve their educational strategies, but these opportunities bring significant, undeniable social, political, ethical, and legal problems that education stakeholders should neither discount nor ignore.[4] Chief among these problems is student data privacy, from which one could argue that most of these other social, political, ethical, and legal issues stem.

This policy brief begins with a description of learning analytics, with a focus on how such practices create student data privacy issues due to sociotechnical conditions (e.g., the conditions under which people and technology interact in organizational processes) (Section One). The brief addresses these conditions through two theoretical lenses: Goffman's "total institutions" (Section Two) and Haggerty and Ericson's "data double" (Section Three). The brief then situates student data privacy within a larger conceptual web of privacy values to highlight its unique, important characteristics (Section Four). Finally, the brief sets up a concluding argument: student data privacy is a collective responsibility, and there are opportunities to redesign learning analytics in accordance with student data privacy as a collective value (Section Five).

1. Educational Data Mining and Learning Analytics

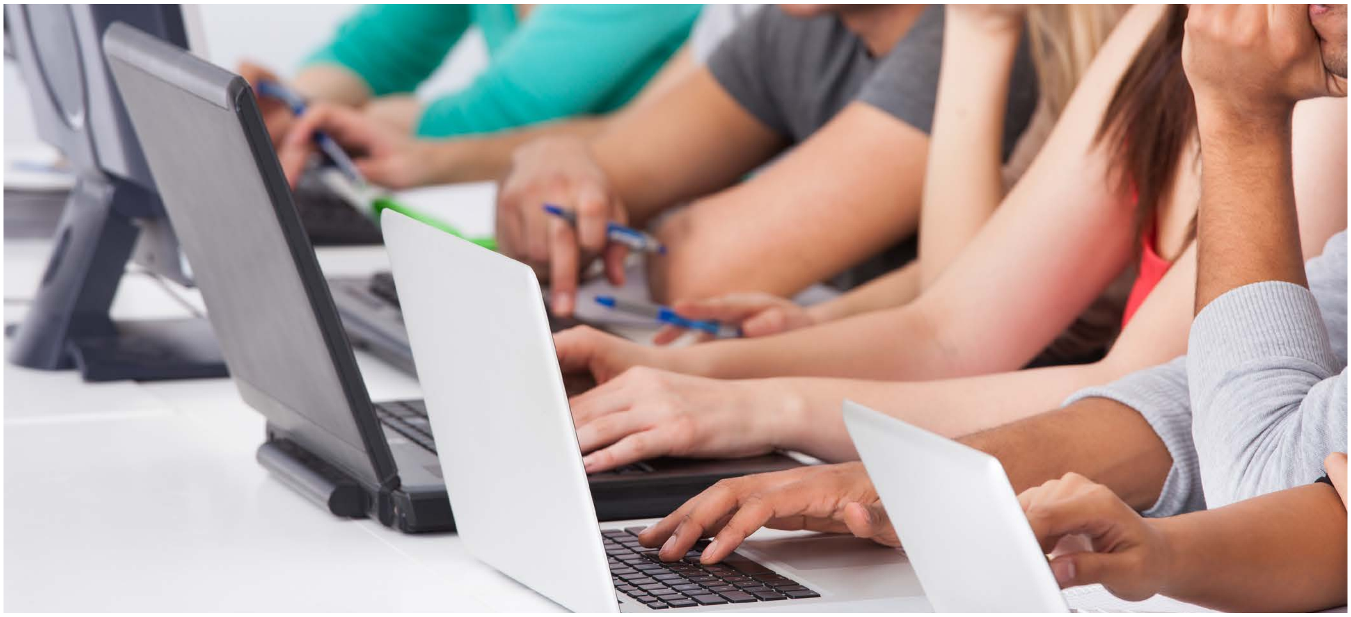
Sometimes referred to as “educational data mining” or “academic analytics,” learning analytics is the larger term—both in terms of political influence and scholarly inclusion—that encompasses data design, aggregation, mining, and analytics (e.g., data visualization, predictive modeling, personalized systems) for myriad purposes, including personalized education, predictive advising, and automated interventions in learning behaviors.[5] It is an interdisciplinary field that has “evolved around the idea of harnessing the power of digital technologies to collect traces that users leave behind, in order to understand activities and behaviors associated with users’ learning.”[6] Since its inception around 2010, learning analytics has met serious critiques.

Institutional advocates of learning analytics, primarily but not exclusively the C-suite and other administrators, along with researchers in the field, have been dogged by the anxiety regarding the collection and use of increasingly granular and extensive data sets. Buckingham Shum and Luckin nicely summarize the unease: Some stakeholders wish to pursue evidence-based practice driven by analytics to improve higher education, a highly bureaucratic institution; others see such practices as the attempt to datafy and quantify human life, a strategy that can never fully succeed.[7] Such quantification of education—an extensively complex process—attempts to simplify learning to inputs and outputs in ways that cannot account for innumerable social and economic factors. The authors argue, in stark terms, that this tension between opposing parties exists in part because of a failure to communicate clearly about learning analytics: “If we do not want to see concerned students, parents and unions protesting against AI in education, we need urgently to communicate in accessible terms what the benefits of these new tools are, and equally, how seriously the community is engaging with their potential to be used to the detriment of society.”[8]

The basic question of benefits versus harms (e.g., educational, financial, social, political, etc.) is central to the sustainability of learning analytics. On the face of it, students are the key beneficiaries, but the focus on efficiencies and political positioning increasingly seems to create benefits for institutions while limiting or even contravening students’ individual and collective interests.[9] In their systematic literature review of learning analytics evidence, Viberg and colleagues[10] examined whether the field’s research verified the following propositions about learning analytics: it improves learning outcomes; it improves learning support and teaching; it is used widely, including at scale;

and it is used in an ethical way. Of 252 papers published between 2012 and 2018, 35 percent suggest that learning analytics improves learning *support* and *teaching*—not necessarily learning; 9 percent present evidence of improved learning outcomes; a mere 6 percent suggest that it is used widely; and only 18 percent address ethics or privacy. These findings are striking given the frequent rhetoric of learning analytics advocates who argue that its "transformative power"[11] is worthy of immense investments by institutions (especially public universities) that often work under tight financial constraints.

The weak benefits of learning analytics lead us to question whether investments in data infrastructures and artifacts serving related goals outweigh the real harms, primarily those regarding student data privacy. Even if the learning outcomes of this technology *have been* or do *become* stronger, there are still defensible data privacy justifications that would limit wider adoption of learning analytics strategies. Before discussing what student data privacy is, however, we first need to understand how learning analytics modifies information conditions (i.e., structures supporting or denying acceptable information flow characteristics), thereby leading to data privacy risks. Two major conditional alterations exist, although others are relevant. First, learning analytics advances informational strategies that granularly observe and comprehensively profile students across time, physical places, and digital spaces. Second, learning analytics uses aggregated profile data to develop predictive models and algorithms, which are then used to intervene in students' personal and academic lives. Both of these strategies are cornerstones of the long-term success of learning analytics.



2. Data Infrastructures for Total (Educational) Institutions

Learning analytics and its focus on observing and profiling students is best understood through traditional and digital sociological lenses. First, this section argues that HEIs are softer forms of Goffman's "total institutions" made possible by emerging sociotechnical conditions motivated partly by learning analytics.[12] Goffman's *Asylums* laid out the general social arrangements of life, and described how individuals placed in mental health institutions (in the mid-twentieth century at least) lived stark experiences that contrasted with those arrangements. Unlike the so-called normal person unconstrained by institutional living and fully able to change routines and friendships, as well as pursue personal and professional experiences according to their interests, institutionalized people were forced to live in one place and under one administration's norms, rules, and expectations. Thus, institutionalized people were subjects of and subjected to an authority structure that materially, socially, and economically influenced—if not controlled—their lives. To be clear: HEIs are *not* the same as Goffman's mental institutions, yet there are parallels that demonstrate the degree of control and influence these education programs hold over their subjects—students. And these programs are increasing this control and influence by datafying students' lives.

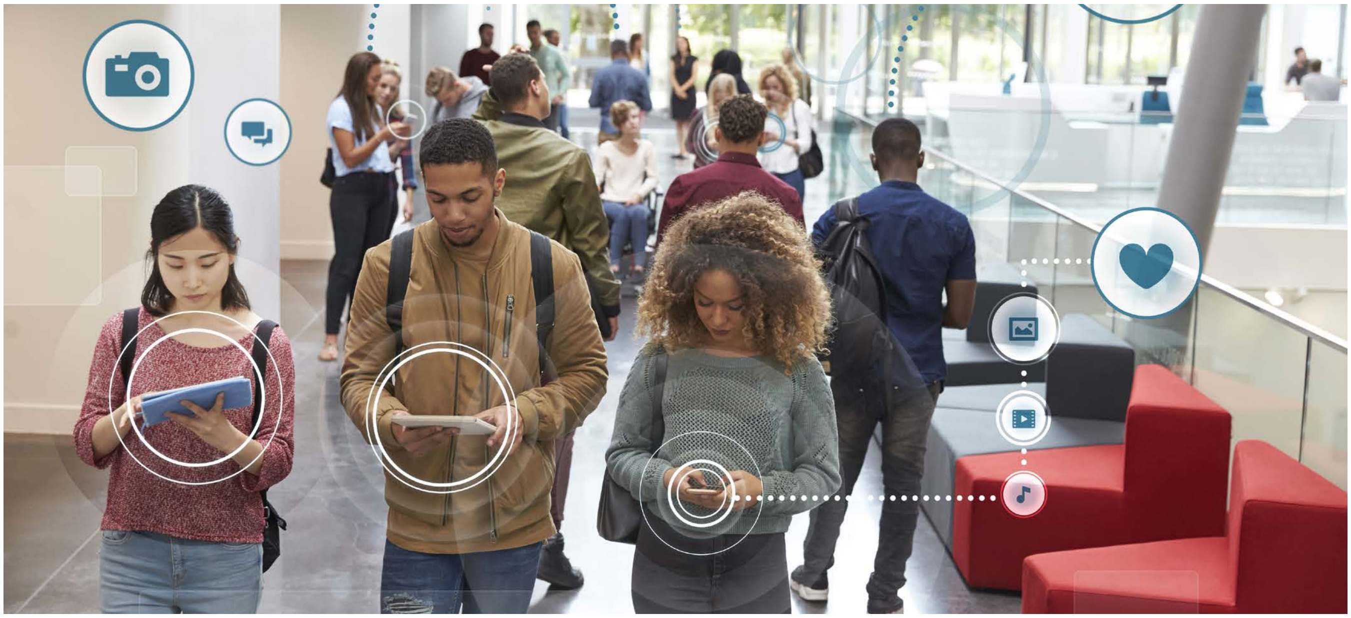
At colleges and universities across the country, incoming first-year students relocate en masse from their family homes to the dormitories of their institutions. Even before they arrive on campus, their universities have begun the institutionalization process. Admissions records are transformed for the registrar and financial aid offices to include highly descriptive profiles of educational, personal, and financial information. University housing offices carefully match students as roommates based on personal interests and community designs. And advisors receive quotas of incoming students, for which they will share responsibility with faculty for each student's academic success.

After arriving on campus, students begin their institutionalization process. They head to the campus union to be documented: their campus record is matched to their state identification card, their picture is taken, and then their new university identification card is printed with a scannable barcode on the back and an embedded radio-frequency identification (RFID) chip, which allows entry into secure locations. During orientation, students learn the institution's norms and values through oral stories; at the same time, students are introduced to the rules and regulations posted on various university websites and in the student handbook. Students create their single sign-on accounts, which give them access to all of their university's digital tools: wifi, email, calendar systems, library databases, the learning management system, and so on. They meet with their advisors, who communicate course schedules, how to navigate the campus, and emphasize that attention to coursework leads to academic success and staves off the financial ruin that could result from failing to earn their degree.

As the semester progresses, students better understand not only the university's expectations but also those of each professor, for every professor seems to have their own norms and guidelines for academic and personal conduct. Students submit themselves to the social, academic, and even temporal ways of being a student in a given class, and attempt to succeed at an intellectual level while not running afoul of their professor's protocols. During their courses, students are required to download certain applications, use particular tools at specific times, and participate in shared digital experiences with their peers. There are rarely opportunities to refuse or choose alternative digital learning experiences because the instructor chose these things, and instructors have the power to dictate learning designs.

One could narrate and illustrate much more about the social and technological construction of student life, but these general themes will do. Students must comply with institutional rules and regulations and must use the tools that the institution has designed and managed or subscribed to, including the ubiquitous information network on which students rely for access to the tools. Students do not have legitimate power over their universities-as-total-institutions, and the institution gains social and political strength by ensuring that the power differential remains lopsided in favor of its administrators, faculty, and other influential staff (e.g., advisors). Students still have some agency, for they can choose to remain at or leave their university. But even then, there are limitations because some students are geographically limited due to other responsibilities (e.g., to a job, to family members). Regardless, students have very little agency to demonstrate disagreement or enact protections against institutional influence.

All of this matters because of technological ubiquity and colleges' and universities' reliance on technology. Information and communication tools are not nice-to-haves; they are must-haves because universities can no longer support their educational mission or manage their large, bureaucratic responsibilities without them. Students are expected to be always on, to stay connected to their university's network, to access, to consume, to share information—and to manage their lives. Universities continue to advance their networking technologies in order to become smart universities equipped with an assemblage of sensors, cameras, and so-called intelligent voice assistants (e.g., Apple's Siri, Google's Alexa) to capture, analyze, and act on an array of data.



3. Profiling Student Lives and Predicting Student Outcomes with Data Doubles

Institutions' power over their students and the network of technologies at their disposal enable the organizations to create stunning, granular student profiles. These profiles are in no way akin to traditional, paper-based education records; rather, they are increasingly a form of a "data double." Citing Haggerty and Ericson,[13] Galič, Timan, and Koops explain how such doubles are created and to what ends:

> The body is first broken down, abstracted from its physical setting, only to then be re-assembled in different settings through a series of data flows. The result is a decorporealised body, more mobile and measurable than its physical counterpart, reassembled [....] The data double constitutes an additional self, a 'functional hybrid' (Hier 2002, 400), serving foremost the purpose of being useful to institutions, which allow or deny access to a multitude of domains (places, information, things) and discriminate between people. The doubles flow through a host of scattered 'centres of calculation' (e.g. forensic laboratories, statistical institutions, police stations, financial institutions and corporate and military headquarters) in which they are re-assembled and scrutinised for developing strategies of administration, commerce and control.[14]

While a useful explanation of a data double, the quotation's focus on corporeality is limited. Homing in on the surveillance of a physical form does not explicitly address a core problem: the doubling of one's self into digital form enables greater opportunities by those making and controlling the double to influence or even control one's emotions, thoughts, and eventual speech acts. Moreover, Galič and colleagues focus on other actors (e.g., police, finance, military) who see and use the double to effect some outcome. What also needs to be considered is the consequence of seeing one's *own double*. We take our mirror images for granted; we know they are visual representations of ourselves, assuming we are not looking at a funhouse mirror with obvious distortions. But what of our virtual replicant, our data double? Do we take that for granted? Because so many interests affect its construction, including its accuracies, inaccuracies, and potentially misleading additions (e.g., predictive measures), we should criticize our data doubles when we encounter them. But that assumes we have the capabilities to recognize them when we see them and to ask useful questions about them.

The granular student profiles that HEIs create can become staggeringly robust data doubles, and these doubles enable learning analytics to maximize analytical insights. Individual profiles enable a deep historical view of a student's learning activities, social engagements, demographics, and more. When analyzing specific segments of joined profiles, institutions can more carefully analyze subdivisions of their student body based on demographics (e.g., first-year students, minority students), behaviors (e.g., students who interact with the library, students who socialize in the union), and outcomes (e.g., students who successfully passed Statistics 101 and 201). Without access to these profiles, the analytical opportunities diminish significantly.

The data that drives learning analytics enables vast descriptions of students and their behaviors, but this descriptive work is typically not what has motivated its development. When using predictive measures and targeted interventions to influence student behaviors, adjust educational variables (e.g., instructional designs), and personalize learning to achieve the greatest effect, advocates care less about what *has* happened and more about influencing what *can* happen.[15] Universities focus on and invest in their student retention activities, as lower-than-expected retention can lead to financial hardship and political fallout. Researchers have examined the effect of predicting that students will not be retained.[16] Research has naturally focused on improving student success with predictive analytics, and numerous studies have attempted to identify variables that indicate at-risk academic behaviors[17] or that advise students to enroll in courses in which they are predicted to succeed.[18] Identifying weak academic behavior is one thing, but it matters not if no action follows. Therefore, much of the predictive learning analytics inquiry focuses on intervention practices that aim to influence the at-risk student's decision-making processes and to provide more personalized education according to the student's needs.[19]

Identifying and intervening in students' lives raises significant questions regarding statistical error and social consequences. Machine learning strategies and artificial intelligence technologies often drive the analytic measurements, raising the specter of statistical bias, issues of fair treatment, and concerns about discrimination. Numerous studies have exposed bias in educational data mining and analytics algorithms, especially when the models do not accurately represent the population studied (e.g., due to under-sampling).[20] While still in its infancy, an emerging conversation in the learning analytics literature regards how to *define* fair practices and what such practices *look like*.[21] Some see fairness as a matter of student treatment when institutions apply analytics, while others argue that fairness means balancing student interests with—or even prioritizing them over—institutional interests. Selwyn sees this as a good "first step" but worries it will lead to simple "ethics-washing,"[22] where institutions proffer statements regarding their ethical principles but do not also validate that ethical practices take place. The problem of discrimination concerns whether students who have been profiled, analyzed, and categorized will receive differential and disadvantageous treatment based on the analytical categories in which an algorithm has grouped them. Scholes explains, "the disadvantage could include being required or encouraged to engage in unnecessary extra work that could also be an added expense (for example, being directed to take a bridging course)."[23] Rubel and Jones provide another example of potential discrimination, describing how a prediction that 25 percent of students will fail a course results in differential treatment: the students ultimately receive less attention and support from their instructor and teaching assistants, since the instruction team determines that, according to the algorithm, those efforts would be for naught.[24]

Data infrastructures and the learning analytics initiatives they enable HEIs to pursue raise myriad ethics and policy-related questions, but they all seem to boil down to privacy. The core issue is that HEIs collect more data and information, disclose that information internally and externally to third-party actors (e.g., edtech), and craft analytic findings onto student profiles in order to influence students' educational experiences and personal behaviors. While scholars have extensively cataloged the privacy problems,[25] it is less clear why data privacy matters for students and how various actors within HEIs treat it.

4. Why Student Data Privacy Matters: A Hybrid Approach

The literature has documented the depth and breadth of theories explaining privacy's intrinsic and instrumental value. Notably, work by Daniel Solove, Herman Tavani, and Helen Nissenbaum, among others, has helped practitioners and researchers make sense of the moral arguments explaining privacy's value.[26] With regard to students, especially *university* students, there exists no theory of privacy that serves as a useful tool of advocacy when students' data privacy is questioned or at stake. More often than not, the Family Educational Rights and Privacy Act of 1974 (FERPA) has served as an explanatory stand-in for student privacy, given how much institutional actors rely on it to justify or limit their information practices. But FERPA is not a theory and does not in any way *explain* why student data and information should be protected; in fact, FERPA is so ill suited to a big data world that whatever student privacy guidance and protections it used to provide have been significantly weakened.[27] The freedom that FERPA allows HEIs, along with a commonly held view that students do not care about their privacy, has enabled some analytics advocates to create privacy-invading technologies and pursue analytic strategies that pose significant privacy risks. But research shows that students *do* care about their privacy,[28] and just because laws or other policies allow invasive practices does not mean that HEIs should pursue such practices. Better understanding of why student privacy matters in the first place may help to establish stronger guardrails in policy, guide practitioners' decision-making, and make technological design more ethical.

This brief proposes a hybrid approach to student data privacy that draws from three theoretical views. The hybrid explains why student data privacy has value and serves students' educational needs beyond what a single approach could achieve. The first theory informing the hybrid is Helen Nissenbaum's framework of contextual integrity,[29] the second theory is Neil Richards's theory of intellectual privacy,[30] and the third includes relevant relational aspects of privacy proposed by James Rachels.[31]

Whether student data privacy is relevant to the context of higher education is not in question. Privacy is an embedded contextual value built into the overall mission of higher education, and it has normatively moderated the flow and ends of student data and information use for some time. In other words, informational norms mapped to student privacy have served to "regulate the flow of information of certain types about [students] from one actor (acting in a particular capacity or role) to another or others (acting in a particular capacity or role) according to particular transmission principles."[32] Actors, such as registrars and chief information officers, are attentive to student privacy as a primary component of their jobs; but so, too, are advisors, faculty, and librarians, among others—all of whom in various ways interact with students' information, whose improper disclosure could be harmful. The problem with learning analytics is that it has raised numerous challenges to contextual integrity because traditional types and sources of student data and information have changed both in form and in function, and new actors have gained access (e.g., other HEIs working in tandem as a data consortium, edtech). Empirical research on students' expectations and preferences vis-à-vis learning analytics has shown significant disconnects between what students *want* done with their data and privacy compared to what *is* being done, demonstrating that the integrity of the context is at risk.[33]

Since privacy is an undeniable contextual value, what intrinsic and instrumental qualities make it so important to higher education that it warrants protection? Intellectual freedom is a key component. Pluralistic, diverse societies respect an individual's right to create ideas, contemplate myriad points of view and facts, and speak freely. It does not matter to what ends such speech acts are directed (except in obvious cases, such as hate speech). Higher education enables students to develop the capabilities and capacities to do those things, but it requires unique conditions. Its commitment to intellectual freedom requires that its faculty and students participate in an educational experience free of influence, especially influence motivated by nonacademic goals (e.g., revenue enhancement, political favors). Privacy is an instrumental element of higher education's commitment to intellectual freedom. According to Richards, privacy provides the "protection from surveillance or unwanted interference by others when we are engaged in the processes of generating ideas and forming beliefs."[34] Students in higher education need intellectual privacy protections to uphold their intellectual freedom now more than ever due to the fine granularity of institutional surveillance and intellectual interventions of learning analytics.

The final aspect of this hybrid approach to student privacy incorporates relational facets. Scholars note how privacy enables various relationships to emerge and be sustained (or how failure to protect the privacy of information ends relationships). Rachels argues that "there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people."[35] This aspect of student privacy is lacking in the literature, which is surprising given the types and degrees of relationships students develop with institutional actors. Students often develop close connections with their instructors. Those instructors can act as mentors or even confidants. Similarly, students work closely with their academic advisors to address academic and professional goals and the variables that may affect their ability to achieve those goals. These conversations incorporate more than just grades; they touch on aspects of family life, financial concerns, and social struggles, among other topics. Resident assistants (RAs), who are often students themselves, are responsible for students' safety and for community building within dormitories. It is part of an RA's ethos to develop relationships with their residential community members, which can enmesh them in the residents' personal lives, to provide timely resources and support.

The literature reveals many examples of these types of institutional actors gaining access to sensitive data and information,[36] but students are mostly unaware of data dashboards and other informational tools. Because of this information asymmetry, students cannot develop relationships by selectively disclosing information and with appropriate awareness of how others use, analyze, and store their information. As Rachels writes, "we have good reason to object to anything that interferes with these relationships and makes it difficult or impossible for us to maintain them in the way that we want to."[37] There are valid reasons to restrain the development and use of analytic tools if they negatively affect a student's ability to build important relationships with key institutional actors, especially when analytics allow those actors to develop preconceived and/or incomplete notions about students before getting to know them as individuals and students.

5. A Shared Value, a Community Responsibility

The desire to increase efficiencies, to decrease costs, and to prove value to various stakeholders has led modern HEIs to redirect and invest their limited resources into learning analytics and other data initiatives. The result, as described above, has decreased student privacy and increased the possibility of harm to students, notably to their autonomy and intellectual freedom. Some may point fingers to determine the root cause: politicians, provosts, chief information officers, legal counsel, federal and state law, progenitors of learning analytics, data science advocates, and so forth. But such finger pointing does not help to resolve the possibilities of harm. Since student data is critical to much of the work that faculty, staff, and administrators do, there is no room to suggest that student privacy is the responsibility of just one person or one office. The choice to use and the duty to protect students' information is the responsibility of all in the academic community, but how does that responsibility play out? How do education stakeholders protect privacy?

First, learning analytics and other data science-driven actions are reductive activities. They expose student life for analysis and then drill down to various aspects and variables that best fit a model (e.g., a prediction, a pathway to a desired outcome). These practices reduce the richness of students' lives; they are a form of statistical erasure. The academic community needs to assess whether the exposure of students' lives is acceptable and the subsequent reduction is justifiable. These decisions should *not* be left to technology vendors or powerful administrators. Each application of an analytic must be evaluated for its consequences regarding the fair treatment of students and discriminatory results that can ensue. Reflecting on reductionism in learning analytics, Rosé writes,

> Are analytics necessarily reductive, decontextualized, and opaque/uninterpretable/inscrutable? These qualities can certainly be true of analytics. But are they necessarily true? We have a choice about the extent to which we take up a reductive position on the spectrum in our analytics work.[38]

Rosé is right: There are choices. The academic community should require that an analytic be, to the extent possible, auditable and triangulated with secondary research (e.g., related statistical inquiry, qualitative methods) before the community accepts it. Review committees should establish standards for auditing and heuristics for determining whether an analytic is acceptable. These committees should include various stakeholders who hold diverse intellectual expertise (e.g., philosophers alongside data scientists) and should reflect a campus's diverse community and all the experiences and perspectives that diversity represents.

Second, learning analytics is usually an expression of administrative power and a tool to achieve administrative interests. Administrators, such as chief information officers and directors of educational technology offices, determine the technologies its faculty will teach with and, subsequently, the environments in which students must participate. Legal counsel enact policy and contractual agreements that govern the flow of student data and information. Selwyn argues that these actions are often *not* in alignment with core educational needs:

> [A] key question to ask of any instance of data collection and analysis (such as Learning Analytics) is 'what [is] the underlying intent here?'. I would argue that for all its talk of 'influencing learner decision-making', 'supporting learner choices', or 'informing teacher actions', Learning Analytics is fundamentally concerned with control and the exercise of power. What one person might see as offering 'support', is what another person might experience as being 'screwed'.[39]

The academic community should ask key questions about learning analytics initiatives and identify who is pushing their integration into the teaching and learning environment. These questions must challenge those in power who make claims about learning analytics but have little evidence that the technology's efficacy outweighs the investments and potential harms. Furthermore, the academic community must carefully consider how learning analytics and other data projects attempt to calculate and reform academic labor and student support systems by 1) making student life granularly accessible and analyzable and 2) forcing faculty and staff to perform according to narrowly defined metrics.

Finally, the most important point: the academic community must rethink the development and evolution of learning analytics in order to protect students and their privacy—and must actively participate in the design of learning analytics tools and the goals at which they are directed. No successful implementation of learning analytics infrastructures and artifacts is possible unless faculty, staff, administration—and, yes, students—frame their construction according to the core educational mission and with a shared, collective vision. That vision may accept some forms of learning analytics and reject others, but at least the vision will reflect joint development instead of administrative force.

REFERENCES

Avella, J. T., Kebritchi, M., Nunn, S. G., and Kanai, T. *Learning Analytics Methods, Benefits, and Challenges in Higher Education: A Systematic Literature Review*. Online Learning (2016) 20 (2): 13–29. https://eric.ed.gov/?id=EJ1105911.

Baer, L. L., and Norris, D. M. “Unleashing the Transformative Power of Learning Analytics.” In C. Lang, G. Siemens, A. Wise, and D. Gasevic (Eds.), *Handbook of Learning Analytics* (2017), pp. 309–318. Society for Learning Analytics Research (SoLAR). https://doi.org/10.18608/hla17.026.

Bienkowski, M., Feng, M., and Means, B. *Enhancing Teaching and Learning Through Educational Data Mining and Learning Analytics*. (2012). US Department of Education. http://www.ed.gov/edblogs/technology/files/2012/03/edm-la-brief.pdf.

boyd, d, and Crawford, K. *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*. Information, Communication & Society (2012) 15 (5), 662–679. https://doi.org/10.1080/1369118X.2012.678878.

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

Buckingham Shum, S. J., and Luckin, R. *Learning Analytics and AI: Politics, Pedagogy and Practices*. British Journal of Educational Technology (2019) 50 (6): 2785–2793. https://doi.org/10.1111/bjet.12880.

Campus Labs. *Case Study: Northern Arizona University–Using Data to Improve Student Retention*. (2014). https://web.archive.org/web/20150919204541/http://www.campuslabs.com/pdf/caseStudy-NAU.

Campus Labs. *Using Engage for Residence Life*. Engage Help Center. (2020). https://engagesupport.campuslabs.com/hc/en-us/articles/360000454103-Using-Engage-for-Residence-Life.

Daniel, B. K. “Big Data in Higher Education: The Big Picture.” In B. Kei Daniel (Ed.), *Big Data and Learning Analytics in Higher Education: Current Theory and Practice* (2017), pp. 19–28. Springer International Publishing. https://doi.org/10.1007/978-3-319-06520-5_3.

Dawson, S., Gašević, D., Siemens, G., and Joksimovic, S. *Current State and Future Trends: A Citation Network Analysis of the Learning Analytics Field*. Proceedings of the Fourth International Conference on Learning Analytics And Knowledge. (2014). https://doi.org/10.1145/2567574.2567585.

Dawson, S., Jovanovic, J., Gašević, D., and Pardo, A. *From Prediction to Impact: Evaluation of a Learning Analytics Retention Program*. Proceedings of the Seventh International Learning Analytics and Knowledge Conference. (2017). https://doi.org/10.1145/3027385.3027405.

Galič, M., Timan, T., and Koops, B. J. *Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation*. Philosophy & Technology (2017) 30 (1): 9–37. https://doi.org/10.1007/s13347-016-0219-1.

Goffman, E. *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates*. (1961). New York: Anchor Books/Doubleday.

Greller, W., and Drachsler, H. *Translating Learning into Numbers: A Generic Framework for Learning Analytics*. Journal of Educational Technology & Society (2012) 15 (3): 42–57. https://www.jstor.org/stable/jeductechsoci.15.3.42.

Haggerty, K. D., and Ericson, R. V. *The Surveillant Assemblage*. The British Journal of Sociology (2000) 51 (4): 605–622. https://doi.org/10.1080/00071310020015280.

Haythornthwaite, C. *An Information Policy Perspective on Learning Analytics*. Proceedings of the Seventh International Learning Analytics and Knowledge Conference. (2017). https://doi.org/10.1145/3027385.3027389.

Holstein, K., and Doroudi, S. *Fairness and Equity in Learning Analytics Systems (FairLAK).* Companion Proceedings of the Ninth International Conference on Learning Analytics and Knowledge. (2019). https://www.solaresearch.org/wp-content/uploads/2019/08/LAK19_Companion_Proceedings.pdf.

Howell, J. A., Roberts, L. D., Seaman, K., and Gibson, D. C. *Are We On Our Way to Becoming a “Helicopter University”? Academics’ Views on Learning Analytics*. Technology, Knowledge and Learning (2018) 23 (1): 1–20. https://doi.org/10.1007/s10758-017-9329-9.

Jarke, J., and Breiter, A. *Editorial: The Datafication of Education*. Learning, Media and Technology (2019) 44 (1): 1–6. https://doi.org/10.1080/17439884.2019.1573833.

Jones, K. M. L. *Advising the Whole Student: Eadvising Analytics and the Contextual Suppression of Advisor Values*. Education and Information Technologies (2019) 24 (1): 437–458. https://doi.org/10.1007/s10639-018-9781-8.

Jones, K. M. L., Asher, A., Goben, A., Perry, M. R., Salo, D., Briney, K. A., and Robertshaw, M. B. *“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 (2020) 71 (9): 1044–1059. https://doi.org/10.1002/asi.24358.

Jones, K. M. L., Rubel, A., and LeClere, E. *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 (2020) 71 (10): 1227–1241. https://doi.org/10.1002/asi.24327.

Klein, C., Lester, J., Rangwala, H., and Johri, A. *Learning Analytics Tools in Higher Education: Adoption at the Intersection of Institutional Commitment and Individual Action*. The Review of Higher Education (2019) 42 (2): 565–593. https://doi.org/10.1353/rhe.2019.0007.

Lane, J. E., and Zimpher, N. L. "Fostering Smarter Colleges and Universities." In J. E. Lane (Ed.), *Building a Smarter University: Big Data, Innovation, and Analytics* (2014), pp. 3–26. State University of New York Press. https://www.sunypress.edu/p-5994-building-a-smarter-university.aspx.

Larrabee Sønderlund, A., Hughes, E., and Smith, J. *The Efficacy of Learning Analytics Interventions in Higher Education: A Systematic Review*. British Journal of Educational Technology (2019) 50 (5): 2594–2618. https://doi.org/10.1111/bjet.12720.

Mangaroska, K., and Giannakos, M. *Learning Analytics for Learning Design: A Systematic Literature Review of Analytics-Driven Design to Enhance Learning*. IEEE Transactions on Learning Technologies (2019) 12(4): 516–534. https://doi.org/10.1109/TLT.2018.2868673.

Nissenbaum, H. *Privacy as Contextual Integrity*. Washington Law Review (2004) 79 (1): 119–158. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/.

Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. (2009). Stanford: Stanford University Press. https://www.sup.org/books/title/?id=8862.

Paquette, Luc, Ocumpaugh, Jaclyn, Li, Ziyue, Andres, Alexandra, and Baker, Ryan. *Who's Learning? Using Demographics in Edm Research*. Journal of Educational Data Mining (2020) 12 (3): 1–30. https://doi.org/10.5281/ZENODO.4143612.

Pardo, A., and Siemens, G. *Ethical and Privacy Principles for Learning Analytics*. British Journal of Educational Technology (2014) 45 (3): 438–450. https://doi.org/10.1111/bjet.12152.

Park, J., and Vance, A. *Data Privacy in Higher Education: Yes, Students Care*. EDUCAUSE Review. (February 11, 2021). https://er.educause.edu/articles/2021/2/data-privacy-in-higher-education-yes-students-care.

Rachels, J. *Why Privacy Is Important*. Philosophy & Public Affairs (1975) 4 (4): 323–333. http://www.jstor.org/stable/2265077.

Reidenberg, J. R., and Schaub, F. *Achieving Big Data Privacy in Education*. Theory and Research in Education (2018) 16 (3): 263–279. https://doi.org/10.1177/1477878518805308.

Richards, N. *Intellectual Privacy*. Texas Law Review (2008) 87 (2): 387–446. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1108268.

Richards, N. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Reprint edition). (2017). Oxford: Oxford University Press.

Rosé, C. P. *Monolith, Multiplicity or Multivocality: What Do We Stand for and Where Do We Go From Here?* Journal of Learning Analytics (2019) 6 (3): 31–34. https://doi.org/10.18608/jla.2019.63.6.

Rubel, A., and Jones, K. M. L. *Student Privacy in Learning Analytics: An Information Ethics Perspective*. The Information Society (2016) 32 (2): 143–159. https://doi.org/10.1080/01972243.2016.1130502.

Scholes, V. *The Ethics of Using Learning Analytics to Categorize Students on Risk*. Educational Technology Research and Development (2016) 64 (5): 939–955. https://doi.org/10.1007/s11423-016-9458-1.

Selwyn, N. *Re-imagining 'Learning Analytics' ... A Case for Starting Again?* The Internet and Higher Education (2020) 46*:* 1–5. https://doi.org/10.1016/j.iheduc.2020.100745.

Slade, S., and Prinsloo, P. *Learning Analytics: Ethical Issues and Dilemmas*. American Behavioral Scientist (2013) 57 (10): 1510–1529. https://doi.org/10.1177/0002764213479366.

Solove, D. J. *Conceptualizing Privacy*. California Law Review (2002) 90, 1087. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2086&context=faculty_publications.

Solove, D. J. *A Taxonomy of Privacy*. University of Pennsylvania Law Review (2006) 154 (3): 477–564. https://doi.org/10.2307/40041279.

Sun, K., Mhaidli, A. H., Watel, S., Brooks, C. A., and Schaub, F. *It's My Data! Tensions Among Stakeholders of a Learning Analytics Dashboard*. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. (2019). Association for Computing Machinery. https://doi.org/10.1145/3290605.3300824.

Tavani, H. T. "Informational Privacy: Concepts, Theories, and Controversies." In *The Handbook of Information and Computer Ethics*. (2008). Hoboken, New Jersey: John Wiley & Sons. Inc.

Tsai, Y. S., Whitelock-Wainwright, A., and Gašević, D. *The Privacy Paradox and Its Implications for Learning Analytics*. Proceedings of the Tenth International Conference on Learning Analytics and Knowledge. (2020). https://doi.org/10.1145/3375462.3375536.

Viberg, O., Hatakka, M., Bälter, O., and Mavroudi, A. *The Current Landscape of Learning Analytics in Higher Education*. Computers in Human Behavior (2018) 89: 98–110. https://doi.org/10.1016/j.chb.2018.07.027.

Williamson, B. *The Hidden Architecture of Higher Education: Building a Big Data Infrastructure for the 'Smarter University.'* International Journal of Educational Technology in Higher Education (2018) 15 (1): 12. https://doi.org/10.1186/s41239-018-0094-1.

Williamson, B., Bayne, S., and Shay, S. *The Datafication of Teaching in Higher Education: Critical Issues and Perspectives*. Teaching in Higher Education (2020) 25 (4): 351–365. https://doi.org/10.1080/13562517.2020.1748811.

Young, E. *Educational Privacy in the Online Classroom: FERPA, MOOCs, and the Big Data Conundrum*. Harvard Journal of Law & Technology (2015) 28 (2). http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech549.pdf.

Zeide, E. *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*. Drexel Law Review (2016) 8 (2): 339–394. https://drexel.edu/law/lawreview/issues/Archives/v8-2/zeide/.

ENDNOTES

[1] d boyd and K. Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly phenomenon*, Information, Communication & Society (2012) 15 (5), 662–679, https://doi.org/10.1080/1369118X.2012.678878; B. K. Daniel, “Big Data in Higher Education: The Big Picture,” In B. Kei Daniel (Ed.), *Big Data and Learning Analytics in Higher Education: Current Theory and Practice* (2017), pp. 19–28, Springer International Publishing, https://doi.org/10.1007/978-3-319-06520-5_3; J. E. Lane and N. L. Zimpher, “Fostering Smarter Colleges and Universities,” in J. E. Lane (Ed.), *Building a Smarter University: Big Data, Innovation, and Analytics* (2014), pp. 3–26, State University of New York Press, https://www.sunypress.edu/p-5994-building-a-smarter-university.aspx.

[2] B. Williamson, *The Hidden Architecture of Higher Education: Building a Big Data Infrastructure for the ‘Smarter University,’* International Journal of Educational Technology in Higher Education (2018) 15 (1): 12, https://doi.org/10.1186/s41239-018-0094-1.

[3] J. Jarke and A. Breiter, *Editorial: The Datafication of Education*, Learning, Media and Technology (2019) 44 (1): 1–6, https://doi.org/10.1080/17439884.2019.1573833; B. Williamson, S. Bayne, and S. Shay, *The Datafication of Teaching in Higher Education: Critical Issues and Perspectives*, Teaching in Higher Education (2020) 25 (4): 351–365, https://doi.org/10.1080/13562517.2020.1748811.

[4] See A. Pardo and G. Siemens, *Ethical and Privacy Principles for Learning Analytics*, British Journal of Educational Technology (2014) 45 (3): 438–450, https://doi.org/10.1111/bjet.12152; S. Slade and P. Prinsloo, *Learning Analytics: Ethical Issues and Dilemmas*, American Behavioral Scientist (2013) 57 (10): 1510–1529, https://doi.org/10.1177/0002764213479366; E. Young, *Educational Privacy in the Online Classroom: FERPA, MOOCs, and the Big Data Conundrum*, Harvard Journal of Law & Technology (2015) 28 (2), http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech549.pdf; E. Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*, Drexel Law Review (2016) 8 (2): 339–394, https://drexel.edu/law/lawreview/issues/Archives/v8-2/zeide/.

[5] 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 (2016) 20 (2): 13–29, https://eric.ed.gov/?id=EJ1105911; M. Bienkowski, M. Feng, and B. Means, *Enhancing Teaching and Learning Through Educational Data Mining and Learning Analytics*, (2012), US Department of Education. http://www.ed.gov/edblogs/technology/files/2012/03/edm-la-brief.pdf.

[6] K. Mangaroska and M. Giannakos, *Learning Analytics for Learning Design: A Systematic Literature Review of Analytics-Driven Design to Enhance Learning*, IEEE Transactions on Learning Technologies (2019) 12(4): 516–534, https://doi.org/10.1109/TLT.2018.2868673, p. 517.

[7] S. J. Buckingham Shum and R. Luckin, *Learning Analytics and AI: Politics, Pedagogy and Practices*, British Journal of Educational Technology (2019) 50 (6): 2785–2793, https://doi.org/10.1111/bjet.12880.

[8] Ibid, p. 2785.

[9] K. M. L. Jones, A. Rubel, and E. LeClere, *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 (2020) 71 (10): 1227–1241, https://doi.org/10.1002/asi.24327.

[10] O. Viberg, M. Hatakka, O. Bälter, and A. Mavroudi, *The Current Landscape of Learning Analytics in Higher Education*, Computers in Human Behavior (2018) 89: 98–110, https://doi.org/10.1016/j.chb.2018.07.027.

[11] L. L. Baer and D. M. Norris, “Unleashing the Transformative Power of Learning Analytics,” in C. Lang, G. Siemens, A. Wise, and D. Gasevic (Eds.), *Handbook of Learning Analytics* (2017), pp. 309–318, Society for Learning Analytics Research (SoLAR), https://doi.org/10.18608/hla17.026, p. 309.

[12] E. Goffman, *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates*, (1961), Anchor Books/Doubleday.

[13] K. D. Haggerty and R. V. Ericson, *The Surveillant Assemblage*, The British Journal of Sociology (2000) 51 (4): 605–622, https://doi.org/10.1080/00071310020015280.

[14] M. Galič, T. Timan, and B. J. Koops, *Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation*, Philosophy & Technology (2017) 30 (1): 9–37, https://doi.org/10.1007/s13347-016-0219-1, p. 22.

[15] W. Greller and H. Drachsler, *Translating Learning into Numbers: A Generic Framework for Learning Analytics*, Journal of Educational Technology & Society (2012) 15 (3): 42–57, https://www.jstor.org/stable/jeductechsoci.15.3.42.

[16] S. Dawson, J. Jovanovic, D. Gašević, and A. Pardo, *From Prediction to Impact: Evaluation of a Learning Analytics Retention Program*, Proceedings of the Seventh International Learning Analytics and Knowledge Conference, (2017), https://doi.org/10.1145/3027385.3027405.

[17] S. Dawson, D. Gašević, G. Siemens, and S. Joksimovic, *Current State and Future Trends: A Citation Network Analysis of the Learning Analytics Field*, Proceedings of the Fourth International Conference on Learning Analytics And Knowledge, (2014), https://doi.org/10.1145/2567574.2567585.

[18] K. M. L. Jones, *Advising the Whole Student: Eadvising Analytics and the Contextual Suppression of Advisor Values*, Education and Information Technologies (2019) 24 (1): 437–458, https://doi.org/10.1007/s10639-018-9781-8.

[19] A. Larrabee Sønderlund, E. Hughes, and J. Smith, *The Efficacy of Learning Analytics Interventions in Higher Education: A Systematic Review*, British Journal of Educational Technology (2019) 50 (5): 2594–2618, https://doi.org/10.1111/bjet.12720.

[20] Luc Paquette, Jaclyn Ocumpaugh, Ziyue Li, Alexandra Andres, and Ryan Baker, *Who’s Learning? Using Demographics in Edm Research*, Journal of Educational Data Mining (2020) 12 (3): 1–30, https://doi.org/10.5281/ZENODO.4143612.

[21] K. Holstein and S. Doroudi, *Fairness and Equity in Learning Analytics Systems (FairLAK),* Companion Proceedings of the Ninth International Conference on Learning Analytics and Knowledge, (2019), https://www.solaresearch.org/wp-content/uploads/2019/08/LAK19_Companion_Proceedings.pdf.

[22] N. Selwyn, *Re-imagining ‘Learning Analytics’ … A Case for Starting Again?* The Internet and Higher Education (2020) 46: 1–5, https://doi.org/10.1016/j.iheduc.2020.100745, p.2.

[23] V. Scholes, *The Ethics of Using Learning Analytics to Categorize Students on Risk*, Educational Technology Research and Development (2016) 64 (5): 939–955, https://doi.org/10.1007/s11423-016-9458-1, p. 940.

[24] A. Rubel and K. M. L. Jones, *Student Privacy in Learning Analytics: An Information Ethics Perspective*, The Information Society (2016) 32 (2): 143–159, https://doi.org/10.1080/01972243.2016.1130502.

[25] See C. Haythornthwaite, *An Information Policy Perspective on Learning Analytics*, Proceedings of the Seventh International Learning

Analytics and Knowledge Conference, (2017), https://doi.org/10.1145/3027385.3027389; A. Pardo and G. Siemens, *Ethical and Privacy Principles for Learning Analytics*; S. Slade and P. Prinsloo, *Learning Analytics: Ethical Issues and Dilemmas*; Y. S. Tsai, A. Whitelock-Wainwright, and D. Gašević, *The Privacy Paradox and Its Implications for Learning Analytics*, Proceedings of the Tenth International Conference on Learning Analytics and Knowledge (2020), https://doi.org/10.1145/3375462.3375536; E. Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*.

[26] D. J. Solove, *Conceptualizing Privacy*, California Law Review (2002) 90, 1087, https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2086&context=faculty_publications; D. J. Solove, *A Taxonomy of Privacy*, University of Pennsylvania Law Review (2006) 154 (3): 477–564, https://doi.org/10.2307/40041279; H. T. Tavani, "Informational Privacy: Concepts, Theories, and Controversies," in *The Handbook of Information and Computer Ethics,* (2008); H. Nissenbaum, *Privacy as Contextual Integrity*, Washington Law Review (2004) 79 (1): 119–158, https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/; H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, (2009), Stanford: Stanford University Press, https://www.sup.org/books/title/?id=8862.

[27] See M. Brown and C. Klein, *Whose Data? Which Rights? Whose Power? A Policy Discourse Analysis of Student Privacy Policy Documents*, The Journal of Higher Education (2020) 91 (7): 1149–1178, https://doi.org/10.1080/00221546.2020.1770045; J. R. Reidenberg and F. Schaub, *Achieving Big Data Privacy in Education*, Theory and Research in Education (2018) 16 (3): 263–279, https://doi.org/10.1177/1477878518805308; E. Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*.

[28] J. Park and A. Vance, *Data Privacy in Higher Education: Yes, Students Care*. EDUCAUSE Review, (February 11, 2021), https://er.educause.edu/articles/2021/2/data-privacy-in-higher-education-yes-students-care.

[29] H. Nissenbaum, *Privacy as Contextual Integrity;* and *Privacy in Context: Technology, Policy, and the Integrity of Social Life*.

[30] N. Richards, *Intellectual Privacy*, Texas Law Review (2008) 87 (2): 387–446, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1108268; N. Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Reprint edition), (2017), Oxford: Oxford University Press.

[31] J. Rachels, *Why Privacy Is Important*, Philosophy & Public Affairs (1975) 4 (4): 323–333, http://www.jstor.org/stable/2265077.

[32] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, p. 141.

[33] K. M. L. Jones, A. Asher, A. Goben, M. R. Perry, D. Salo, K. A. Briney, and M. B. Robertshaw, *"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 (2020) 71 (9): 1044–1059, https://doi.org/10.1002/asi.24358; Y. S. Tsai, A. Whitelock-Wainwright, and D. Gašević, *The Privacy Paradox and Its Implications for Learning Analytics.*

[34] N. Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, p. 95.

[35] J. Rachels, *Why Privacy Is Important*, p. 326.

[36] Campus Labs, *Case Study: Northern Arizona University–Using Data to Improve Student Retention*, (2014), https://web.archive.org/web/20150919204541/http://www.campuslabs.com/pdf/caseStudy-NAU; Campus Labs, *Using Engage for Residence Life*. Engage Help Center, (2020), https://engagesupport.campuslabs.com/hc/en-us/articles/360000454103-Using-Engage-for-Residence-Life; J. A. Howell, L. D. Roberts, K. Seaman, and D. C. Gibson, *Are We On Our Way to Becoming a "Helicopter University"? Academics' Views on Learning Analytics*, Technology, Knowledge and Learning (2018) 23 (1): 1–20, https://doi.org/10.1007/s10758-017-9329-9; K. M. L. Jones, *Advising the Whole Student: Eadvising Analytics and the Contextual Suppression of Advisor Values*; C. Klein, J. Lester, H. Rangwala, and A. Johri, *Learning Analytics Tools in Higher Education: Adoption at the Intersection of Institutional Commitment and Individual Action*, The Review of Higher Education (2019) 42 (2): 565–593, https://doi.org/10.1353/rhe.2019.0007; K. Sun, A. H. Mhaidli, S. Watel, C. A. Brooks, and F. Schaub, *It's My Data! Tensions Among Stakeholders of a Learning Analytics Dashboard*, Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, (2019), Association for Computing Machinery, https://doi.org/10.1145/3290605.3300824.

[37] J. Rachels, *Why Privacy Is Important*, p. 329.

[38] C. P. Rosé, *Monolith, Multiplicity or Multivocality: What Do We Stand for and Where Do We Go From Here?* Journal of Learning Analytics (2019) 6 (3): 31–34, https://doi.org/10.18608/jla.2019.63.6, p. 32.

[39] N. Selwyn, *Re-imagining 'Learning Analytics' … A Case for Starting Again?*, p. 4.

FUTURE OF
PRIVACY
FORUM