

The Temptation of Data-enabled Surveillance: Are Universities the Next Cautionary Tale?

Alan Rubel
Information School
Center for Law, Society & Justice
University of Wisconsin-Madison
arubel@wisc.edu

Kyle M. L. Jones
School of Informatics and Computing, Department of Library and Information Science
Indiana University-Indianapolis (IUPUI)
kmlj@iupui.edu

I. Intro

There is increasing concern about “surveillance capitalism,” whereby for-profit companies generate value from data, while individuals are unable to resist (Zuboff 2019). Non-profits using data-enabled surveillance receive less attention. Higher education institutions (HEIs) have embraced data analytics, but the wide latitude that private, profit-oriented enterprises have to collect data is inappropriate. HEIs have a fiduciary relationship to students, not a narrowly transactional one (see Jones et al, forthcoming). They are responsible for facets of student life beyond education. In addition to classrooms, learning management systems, and libraries, HEIs manage dormitories, gyms, dining halls, health facilities, career advising, police departments, and student employment.

HEIs collect and use student data in all of these domains, ostensibly to understand learner behaviors and contexts, improve learning outcomes, and increase institutional efficiency through “learning analytics” (LA). ID card swipes and Wi-Fi log-ins can track student location, class attendance, use of campus facilities, eating habits, and friend groups. Course management systems capture how students interact with readings, video lectures, and discussion boards. Application materials provide demographic information. These data are used to identify students needing support, predict enrollment demands, and target recruiting efforts.

These are laudable aims. However, current LA practices may be inconsistent with HEIs’ fiduciary responsibilities. HEIs often justify LA as advancing student interests, but some projects advance primarily organizational welfare and institutional interests. Moreover, LA advances a narrow conception of student interests while discounting privacy and autonomy. Students are generally unaware of the information collected, do not provide meaningful consent, and express discomfort

This is a pre-print. Please cite to final, published version: Rubel, A., & Jones, K. M. L. (2020). The temptation of data-enabled surveillance: Are universities the next cautionary tale? *Communications of the ACM*, 63(4), 22–24. <https://doi.org/10.1145/3382741>.

and resigned acceptance about HEI data practices, especially for non-academic data (see Jones et al. forthcoming).

The breadth and depth of student information available, combined with their fiduciary responsibility, create a duty that HEIs exercise substantial restraint and rigorous evaluation in data collection and use. Consider several recent examples.

II. Three cases

(1) Movement tracking. Based on student ID card swipes, a university researcher mapped student movements and social networks and built student retention models. It plans to use Wi-Fi router data to form even more detailed understandings and to share this information with advisors (Blue 2018). It is unclear whether students are aware that their data is collected, have opted in, or provided informed consent. To act in students' interests, this HEI could have provided substantial information before the study started (including its rationale), the ability for students to easily opt-out, and a clear policy about collection and use of movement tracking data. This university is one of many engaging in intensive student tracking, either by dedicated beacons, Wi-Fi check-ins, or phone apps (Harwell 2019).

(2) Third-parties. In April 2018, researchers from Pearson publishing revealed that they had conducted an experiment by incorporating encouraging, "growth mindset" messages into a learning software interface and testing (without students' knowledge or consent) whether they affected students' performance (Herold 2018). This demonstrates the value of student information to third parties for non-educational goals, including corporate profit. Similarly, Piazza, maker of a popular question-and-answer app required by many instructors, has sold student data based on students "opting-in" through a pre-checked box on the app sign-up page. Acting in students', rather than vendors' interests demands that HEIs develop stronger controls to protect students and avoid learner data becoming part of surveillance capitalism. At the beginning of the relationship with vendors, HEIs should require that edTech companies make opting-in difficult. If the data collection involves interventions or data sales, HEIs should re-evaluate the relationship, and perhaps require that the companies compensate students for their data.

(3) Intensive advising. Like many HEIs, Georgia State University (GSU) has struggled to ensure that students (in particular those from underrepresented backgrounds) complete their degrees. In 2011, GSU developed a system tracking academic and financial information that alerts advisors about risk factors (e.g., an unsatisfactory grade in a key course). GSU's six-year graduation rate rose from 48% in 2011 to 55% in 2018 (Hefling 2019). Moreover, students of color, Pell-eligible, and first-generation students now graduate at higher rates than the student body overall (Ekowo and Palmer 2016). The GSU case is often described as a LA success. However, GSU simultaneously hired dozens of new advisors and substantially increased student advising. Hence, it is not just an analytics program; it is an advising program informed by data.

Certainly, the improved student outcomes are important, but it is not clear how much is due to LA, exactly what GSU's advising interventions actually are, and whether they provide the best outcomes for each student or just for GSU. Do they steer students away from challenging courses, reducing agency and potential for excellence, or provide tutoring services for at-risk students—increasing their agency and capabilities? It is unclear that the increased student surveillance improved social good, or that GSU considered all of the relevant moral trade-offs. It is crucial to ensure that we don't learn the

This is a pre-print. Please cite to final, published version: Rubel, A., & Jones, K. M. L. (2020). The temptation of data-enabled surveillance: Are universities the next cautionary tale? *Communications of the ACM*, 63(4), 22–24. <https://doi.org/10.1145/3382741>.

wrong lesson and retain the analytics at the expense of the advising. Acting in students' best interests would require a robust, ongoing evaluation.

III. Doing it differently

The above cases illustrate a range of issues in LA, and each demonstrates how HEIs can better fulfill their responsibilities to advance student interests. HEIs have responsibilities before developing LA programs, while student data is collected and analyzed (especially by third parties), and after analytics have been incorporated. Here, we make explicit some of the specific responsibilities of HEIs have as information fiduciaries that can guide their actions.

(1) Diverging interests. Fiduciaries have a responsibility to act in the best interests of their clients, although not necessarily to act *only* to advance client interest. Data analytics may provide insights for HEIs, and help them fulfill their responsibilities to educate students and marshal resources effectively. However, it is an open question whether LA will live up to that promise or that primarily *student* interests motivate LA research. The tracking and third-party data use cases do not advance student interests.

Moreover, universities collect and use data somewhat indiscriminately because it is potentially relevant to their educational and custodial missions. Yet this "relevance condition" is insufficient to justify data collection, analysis, and use (see Rubel and Jones 2016). Any student data is potentially relevant to educational objectives and it is impossible to tell *a priori* which will actually be useful. Hence, a collection principle based solely on potential relevance is no limitation at all.

(2) Fostering trust and trustworthiness. Students attend HEIs believing they are trustworthy, will respect students as individuals, and will not implement systems that subordinate student rights and interests for the sake of institutional or third-party goals. Yet systems currently being built and deployed create opportunities for greater privacy intrusions (the tracking case) and for institutional benefit (movement tracking, third party use). Students have little knowledge of how they are surveilled, typically have no ability to opt out, are uneasy about data collection by HEIs, and cannot control use of their data. It is worth asking whether their trust is misplaced, or whether they must simply acquiesce because of the social and economic value of a college education (see Harwell 2019).

(3) The right benefits. The benefits of LA may be quite limited. The exemplary LA system (GSU) rests substantially on advising resources, not data, with small increases in student success. It is unclear whether success stems from funneling students into easier courses or from collecting and analyzing troves of student data.

HEIs do have obligations to advance the educational interests of at-risk students. However, it does not follow that HEIs should subordinate students' privacy and autonomy interests for the sake of (speculative) retention and achievement rates. Student support (social, advising, tutoring, financial, mental health) should come first, and long before impinging on other interests.

(4) Full account of student interests. We should also be wary of narrowly construing student interests. The above cases focus on student academic achievement, but students have other interests as well, including privacy. They should not have to forego that interest for a marginal (and speculative) return in academic achievement. This should seem familiar to professionals who bristle at overweening surveillance by supervisors.

(5) Full range of higher education's aims. Higher education has a number of aims, including developing communication, critical thinking, understanding and appreciation of diversity, and

This is a pre-print. Please cite to final, published version: Rubel, A., & Jones, K. M. L. (2020). The temptation of data-enabled surveillance: Are universities the next cautionary tale? *Communications of the ACM*, 63(4), 22–24. <https://doi.org/10.1145/3382741>.

development of rewarding employment and careers (see Bok 2006). These are fostered by helping students develop their autonomy. Yet close monitoring of student movement, social networks, and daily habits is an imposition on student privacy, a key element in developing and exercising individual autonomy. If we value student autonomy, we ought to curtail student surveillance (Rubel and Jones, 2016).

(6) Third parties. Students' social networks, their travel around campus, their health, political, and religious activities are inferable from movements. If that information is valuable for HEIs, it will be of interest to others: potential employers, the FBI (pursuant to business records requests under Patriot Act section 215), software vendors, and more. Student privacy protections under FERPA are limited. Moreover, the more student data collected the greater the risk for data breaches. Hence, LA carries risks that we should consider in determining whether it advances student interests overall.

IV. Conclusion

To be clear, we are *not* opposed to LA tout court. Some student data collection will advance legitimate educational and custodial goals while respecting student privacy and fostering autonomy. However, LA and data-enabled surveillance can begin as tools for social good but slide into morally suspect territory, especially in immersive institutions with fiduciary responsibilities like HEIs. Institutional interests and student interests are not identical, and we should not assume that they align. Governments, corporations, and HEIs should avoid data collection and analysis as a matter of convenience and for specious reasons. When HEIs aim to advance student educational interests, they should primarily do so in ways that are consistent with interests in privacy and autonomy. In short, HEIs should conduct LA in ways that justify the substantial trust that students place in them. That will require restraint and evaluation at the beginning, during, and at the end of LA projects.

References

Blue, A. (2018, March 7). Researcher looks at 'digital traces' to help students. University of Arizona News. Retrieved from <https://uanews.arizona.edu/story/researcher-looks-digital-traces-help-students>

Bok, D. C. 2006. Our underachieving colleges: A candid look at how much students learn and why they should be learning More. Princeton, NJ: Princeton University Press.

Ekowo, E. & Palmer, I. (2016, Oct. 24) The Promise and Peril of Predictive Analytics in Higher Education: A Landscape Analysis, New America).

Harwell, D. (2019, December 24). Colleges are turning students' phones into surveillance machines, tracking the locations of hundreds of thousands. Washington Post. Retrieved from <https://www.washingtonpost.com/technology/2019/12/24/colleges-are-turning-students-phones-into-surveillance-machines-tracking-locations-hundreds-thousands/>

Hefling, K. (2019, January 16). The 'Moneyball' solution for higher education. Politico.

Herold, B. (2018, April 17). Pearson tested 'social-psychological' messages in learning software, with mixed results. Education Week. Retrieved from http://blogs.edweek.org/edweek/DigitalEducation/2018/04/pearson_growth_mindset_software.html

This is a pre-print. Please cite to final, published version: Rubel, A., & Jones, K. M. L. (2020). The temptation of data-enabled surveillance: Are universities the next cautionary tale? *Communications of the ACM*, 63(4), 22–24. <https://doi.org/10.1145/3382741>.

Jones, K. M. L., Rubel, A., & LeClere, E. (forthcoming). 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 & Technology*. <https://doi.org/10.1002/asi.24327>

Rubel, A. & Jones, K. M. L. (2016). Student privacy in learning analytics: An information ethics perspective. *The Information Society*, 32(2), 143–159. doi: 10.1080/01972243.2016.1130502

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: PublicAffairs.

This is a pre-print. Please cite to final, published version: Rubel, A., & Jones, K. M. L. (2020). The temptation of data-enabled surveillance: Are universities the next cautionary tale? *Communications of the ACM*, 63(4), 22–24. <https://doi.org/10.1145/3382741>.