Safeguarding student privacy in an age of analytics

Royce Kimmons¹

Published online: 25 January 2021

© Association for Educational Communications and Technology 2021

Abstract

In this special issue, we have collected three responses from scholars who are currently doing work in learning analytics to react to, better explain, and expound upon the Ifenthaler and Schumacher's findings in their own settings as researchers and practitioners.

Keywords Student privacy · Research ethics · Learning analytics

One truism that has become increasingly clear in the age of digital technologies is that technological development far outpaces the evolution of responsible policy and ethics. This has resulted in many current situations and scandals that once would have been thought only possible in a dystopian science fiction novel. In 2014, Cambridge Analytica harvested data from around 200,000 Facebook accounts to build psychological profiles of 87 million users in an attempt to “target their inner demons” and sway their voting behaviors (Cadwalladr and Graham-Harrison 2018). Advances in machine learning and big data have now enabled the use of heretofore low-risk data, like what one posts publicly on Twitter, to be used to predict likelihood of medical conditions (Schneble et al. 2020), contact with a pathogen (Keeling et al. 2020), or mental illness (Kim et al. 2019). Further, constant surveillance (empowered in part by mobile devices and social media) has enabled governments and corporations to develop social management infrastructures to control citizens', employees', and consumers' behaviors through social credit, targeted influence, or fear of discovery (Kostka 2019; West 2019).

In education, the potentials and risks of similar practices with student data represent cause for concern, as student behaviors are increasingly tracked, analyzed, and studied to draw conclusions about learning, attitudes, and future behaviors. Yet, a recent review of the top 10 universities in the U.S., U.K., and Switzerland found that “only a small minority of academic institutions has developed guidelines for data science” in large part because “IRBs in many countries are not required by law to review such research” (Schneble et al. 2018). Couple this with the fact that more than 91–97% of consumers accept terms and conditions of apps and websites without reading them (Deloitte 2017), and the threat to students seems clear: their data are increasingly being used in ways that they are not aware of and that they might not willingly consent to. This occurs

✉ Royce Kimmons
roycekimmons@byu.edu

¹ Instructional Psychology & Technology, Brigham Young University, Provo, UT 84602, USA

even though internet users generally claim to care deeply for their privacy (Paine et al. 2007) and will often experience pressures to adopt technologies that they otherwise would consider to be creepy (Shklovski et al. 2014), leading to various ethical dilemmas regarding student privacy that educational institutions must grapple with if they are to ethically engage in learning analytics or related activities with student data (Slade and Prinsloo 2013).

To help address this problem, Ifenthaler and Schumacher (2016) conducted a quasi-experimental study surveying students about their preferences for learning analytics systems, their attitudes toward privacy as they relate to specific types of data, and how their attitudes influence learning analytics system acceptance. The results are valuable in multiple ways but seem to clearly show that (a) students considered some types of data to be much more important to keep private than others (e.g., medical data vs. email addresses) and (b) students' willingness to accept learning analytics systems was moderately predicted by their attitudes toward data control and sharing. One suggestion provided in the article is that students and their voices should be involved in decision making regarding learning analytics systems and that approaching student privacy in an omnibus manner (wherein all types of data are treated with equal levels of privacy consideration) is overly simplistic. Rather, if learning analytics systems are to be ethically used and accepted by students, then professionals should start by identifying and using data types that introduce minimal risk to students and that also are reasonably well-connected to the intended purpose and learning objectives of the system.

In this special issue, we have collected three responses from scholars who are currently doing work in learning analytics to react to, better explain, and expound upon the Ifenthaler and Schumacher's findings in their own settings as researchers and practitioners. Provided responses include the following:

- Rosenberg and Staudt Wilet approach the article from a research perspective, informed by open science practices, and provide guidance on how to navigate the balance between student risk and scientific potential, which "begins with a deep understanding of the specifics of the context."
- Corrin approaches the article from a policy perspective, highlighting potential limitations of the study and difficulties of implementing policies that adequately account for student voice without first having a shared vocabulary and understanding of benefits and also considering other ethical factors beyond privacy that might shape policy.
- Ochoa and Wise approach the article from a practitioner perspective and highlight three general trends in learning analytics that may help safeguard privacy: (a) involving students in tool creation, (b) developing "analytics that are contextualized, explainable and configurable," and (c) empowering student agency with analytics as part of a "larger process of learning."

Collectively, these responses show a unified call for researchers, practitioners, and policy makers to be more aware of and responsive to student privacy in learning analytics systems, underscoring the fact that professional standards in this space remain somewhat nebulous at present and require ongoing leadership, thoughtfulness, and sensitivity to ensure ethical behavior. Indeed, as learning analytics systems introduce ever-increasing potential to benefit students, they also introduce concomitant potentials for harm that must be addressed quickly if we are to avoid any number of dystopian futures.

References

- Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million facebook profiles harvested for Cambridge analytica in major data breach. *The Guardian*, 17, 22.
- Deloitte. (2017). 2017 Global mobile consumer survey (US edition): The dawn of the next era in mobile. Deloitte
- Ifenthaler, D., & Schumacher, C. (2016). Student perceptions of privacy principles for learning analytics. *Educational Technology Research and Development*, 64(5), 923–938.
- Keeling, M. J., Hollingsworth, T. D., & Read, J. M. (2020). Efficacy of contact tracing for the containment of the 2019 novel coronavirus (COVID-19). *Journal of Epidemiology & Community Health*, 74(10), 861–866.
- Kim, J. Y., Kim, G. Y., & Yacef, K. (2019). Detecting depression in dyadic conversations with multimodal narratives and visualizations. In J. Liu & J. Bailey (Eds.), *Australasian joint conference on artificial intelligence* (pp. 303–314). Cham: Springer.
- Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society*, 21(7), 1565–1593.
- Paine, C., Reips, U. D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions.' *International Journal of Human-Computer Studies*, 65(6), 526–536.
- Schneble, C. O., Elger, B. S., & Shaw, D. (2018). The Cambridge analytica affair and internet-mediated research. *EMBO Reports*, 19(8), e46579.
- Schneble, C. O., Elger, B. S., & Shaw, D. M. (2020). All our data will be health data one day: the need for universal data protection and comprehensive consent. *Journal of Medical Internet Research*, 22(5), e16879.
- Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In Proceedings of the SIGCHI conference on human factors in computing systems. pp. 2347–2356.
- Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. *American Behavioral Scientist*, 57(10), 1510–1529.
- West, E. (2019). Amazon: Surveillance as a service. *Surveillance & Society*, 17(1/2), 27–33.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Royce Kimmons Dr. Royce Kimmons is an Assistant Professor of Instructional Psychology and Technology at Brigham Young University where he studies open education, social media, data mining, and technology integration. More information about his work may be found at <http://roycekimmons.com>.