Ethical Teaching Analytics in a Context-Aware Classroom: A Manifesto

Romain Laurent, Dominique Vaufreydaz, Philippe Dessus

Ethical Teaching Analytics in a Context-Aware Classroom: A Manifesto

Romain Laurent, Dominique Vaufreydaz, Philippe Dessus, Univ. Grenoble Alpes/Inria

Should Big Teacher be watching you? The Teaching Lab project at Grenoble Alpes University proposes recommendations for designing smart classrooms with ethical considerations taken into account.
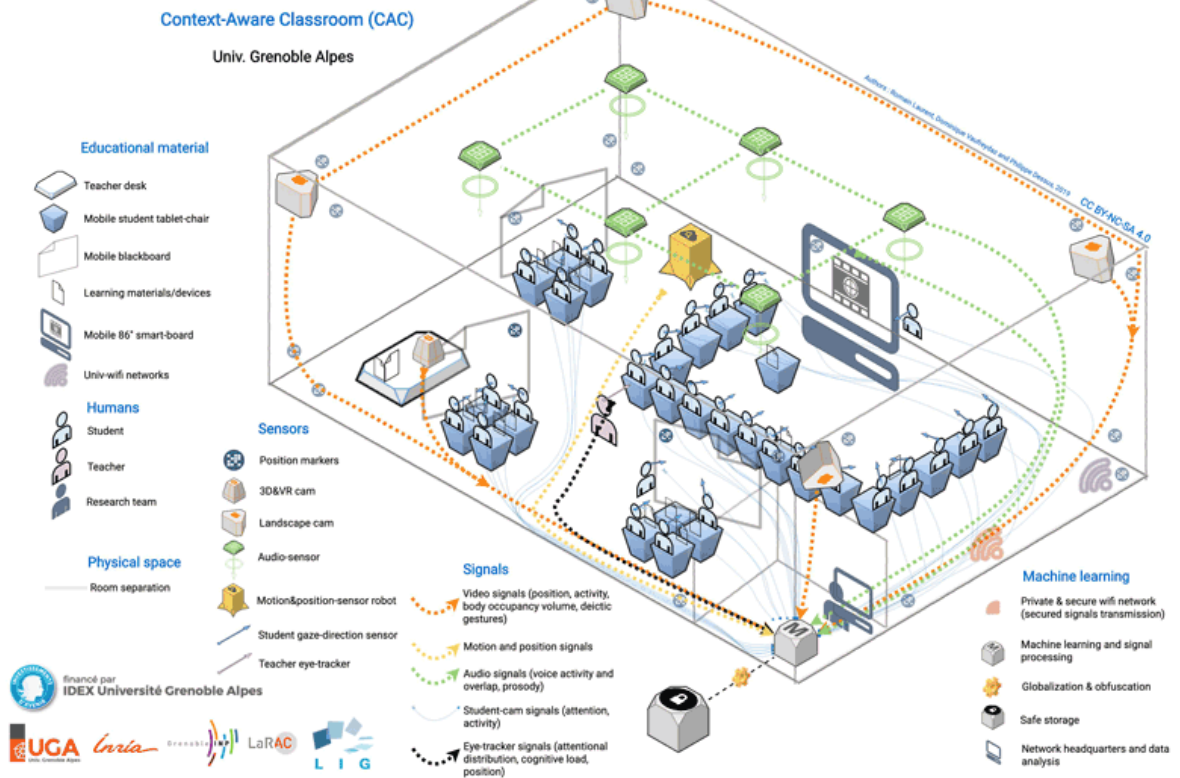
The smart education market is flourishing, with a compound annual growth rate regularly announced in double digits (+31% between 2014 and 2018, +18% between 2019 and 2025). Among these EdTech investments, smarts classrooms that combine AI and adaptive learning are in the spotlight. Although smart classrooms encompass a large range of different products, we can define them as physical environments in which teaching–learning activities are carried out using computerised devices and various techniques and tools: signal processing, robotics, artificial intelligence, sensors (e.g., cameras, microphones) and effectors (e.g., loudspeakers, displays, robots).

Despite all the hype around smart classrooms, it seems that the ethical and privacy aspects of these developments are seldom considered. This issue is not incidental: it conditions not only the classroom atmosphere and the ethics of the institution, but also the quality of interpersonal relationships within the classroom and teaching–learning processes — which universities often claim to support.

This leads to a series of questions. Which signals will be captured and stored? How will the consent of the individuals be gathered? Should the machine monitor everything that happens in the classroom? Will unduly collected signals be excluded (e.g., a camera-captured personal message, a microphone-captured conversation, an inappropriate behaviour)? If yes, how? *Ex ante* (by the machine) or *ex post* (by the operators)? Will the machine remain spectator or will it act in real time using effectors? How will the system thenceforth react to learners' and even teachers' behaviours that might be considered dilatory? What outcomes are we likely to see from the highly delicate interpretation of features inferred from data? In response and to counter any surveillance, what opacifying behaviours or layers will be implemented by the interactors? What trust can then be established between the teacher enhanced (and possibly monitored) by technology, the student under scrutiny and the institution receiving this dataveillance [1]?

Teaching and learning are fragile activities that rely *above all* on the commitment of participants. This mutual commitment is rooted in trust and respect, which can only flourish and prosper on the integrity of the relationship between the teachers, the students and the institution that oversees it. This integrity paves at last the way for *relatedness*, known as critical in student's achievement [2]. The introduction of smart technologies to the classroom, if not framed by explicit ethical and privacy-compliant principles and purposes, could easily be used for dataveillance of its participants, jeopardizing classroom interactions and corrupting the effectiveness of teaching/learning processes [1].

We designed a smart classroom (*Teaching Lab* project at Grenoble Alpes University, funded by the "PIA 2 IDEX formation program"), with essential ethical safeguards in mind that respect individuals' privacy as a prerequisite for the physical, technological and theoretical development of these spaces. The class smartness is exploited in two directions. On the one hand, it authorises the basic collection of educational data (in particular the distribution of attention between teacher, students and learning materials), and their processing by machine learning techniques. On the other hand, it subordinates them to an ethical framework that respects the protagonists, following the safeguards for privacy and data protection in ambient intelligence [3]. To do so, we will use advanced machine learning techniques to shed light on global features while obfuscating local ones. Our objective is twofold. First, we owe privacy to each participant to the extent that everyone's privacy is interwoven with that of everyone else. Secondly, we aim to not bias the genuineness of observed behaviours. We assume there that each individual's protection is a good way to strengthen the global gathered information (e.g. interactions, relatedness).

For this purpose, we propose four key guidelines as the core of the *Teaching Lab* design:

1. We develop an ethics-by-design approach: beyond their common contribution in terms of signal processing, machine learning techniques will be used to anonymise, at their source, attendees' data and filter any item likely to alter the confidence of the protagonists in the instructional flow. Thus, the *Teaching Lab* obfuscates all participants, while focusing on meaningful events and constructs (gaze, teacher cognitive load, hand, deictic, gesture, non-personal devices, voice activity and overlap, prosody).

2. We promote a global rather than local methodology: students' behaviours will never be individually traceable; the machine learning being limited to restore a globalised picture of the occurrence of behaviours. In other words, our data reports about the whole classroom but ignores individuals.

3. Finally, machine learning will be intentionally constrained to a delayed feedback, filtered by the research team, excluding any real-time monitoring or *ad hominem* reports. Our aim is only to support interactors' possible professional development (students included), by studying and providing feedback about the factors reinforcing or weakening attention in class.
4. The Teaching Lab will not make high-stakes decisions, monitor staff performance or student insulation. Following the University of Edinburgh's Learning Analytics' principles and purposes, we contend that data and algorithms can contain and perpetuate biases, and that they never provide the whole picture about human capacity or likelihood of success.

These guidelines are intended to ensure the privacy, security and trust of every individual within the smart classroom, thereby preserving relationships, interactions, and the research for improving teaching and learning processes.

Links:

[L1]: University of Edinburgh Principles and purposes for Learning Analytics: https://www.ed.ac.uk/academic-services/policies-regulations/learning-and-assessment/learning-analytics/principles

[L2]: Teaching Lab Project website: https://project.inria.fr/teachinglab/

References:

[1] R. Crooks, "Cat-and-Mouse games: Dataveillance and performativity in urban schools," *Surveillance and Society*, vol. 17, no. 3/4, pp. 484–498, 2019.

[2] G. Hagenauer and S. E. Volet, "Teacher-student relationship at university: an important yet under-researched field," *Oxford Review of Education*, vol. 40, no. 3, pp. 370–388, 2014.

[3] P. De Hert, S. Gutwirth, A. Moscibroda, D. Wright, and G. González Fuster, "Legal safeguards for privacy and data protection in ambient intelligence," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 435–444, 2008.

Please contact:

Romain Laurent

Univ. Grenoble Alpes / LaRAC, France

romain.laurent@univ-grenoble-alpes.fr

Dominique Vaufreydaz,

Univ. Grenoble Alpes, CNRS, Inria, Grenoble INP, LIG, 38000 Grenoble, France

dominique.vaufreydaz@inria.fr

Philippe Dessus

Univ. Grenoble Alpes / LaRAC, France

Philippe.Dessus@univ-grenoble-alpes.fr