

# **Social Construction of Technology in Higher Education**

A Research Paper submitted to the Department of Engineering and Society  
Presented to the Faculty of the School of Engineering and Applied Science  
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree  
Bachelor of Science, School of Engineering

**Zane Alpher**

Spring 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

S. Travis Elliott, Department of Engineering and Society

## **Thesis Background**

As society has increased its use of technology, specifically software and the internet, people are subject to increased monitoring and companies are able to collect more and more data about users. At the same time, concerns are also increasing about what data companies are collecting and what data they should be able to collect legally and ethically. The public has become more concerned with the possibility of a data breach and the company itself using the data to target customers. This same pattern is happening in schools for students who use educational technology. Over the last few decades, technology has become more and more prevalent in the school system—especially in higher education. When Covid-19 forced schools to go online, the amount of technology used in schools skyrocketed. The amount of student data being collected has also increased, along with the use of student monitoring software. This paper will apply the Social Construction of Technology (SCOT) STS theory to case studies to examine the social factors that cause the use of these privacy breaching technologies.

## **Social Construction of Technology**

The SCOT framework examines how social interactions and relationships shape a technology and its adoption (or non-adoption) into society. Unlike technological determinism, which furthers the belief that technology shapes society, SCOT examines how different social groups interact to shape the technology. Different groups have different opinions and uses of the technology—the interactions between groups are what shape the technology and its adoption over time. The first phase of the SCOT framework is the interpretive flexibility of a new technology. Various groups interact with the technology in different ways which causes them to interpret aspects of the technology differently. Conflicts may arise between social groups about the specific form of the technology and how it should be used. Over time, this conflict will push

the development and use of the technology to a point where it reaches a stable state and is accepted by most. At this point the technology has reached closure, which is the second phase of the SCOT framework. Small incremental changes can still be made to the technology without drastically affecting its widely accepted status, but new or changing social groups can also push a technology out of closure.

When looking at the acceptance of technology into schools, the relevant social groups fall into four categories. These social groups are the **users** of the technology, the **choosers** of the technology, the **makers** of the technology, and the **outside social groups** that also shape technology and influence its adoption. When a new technology is introduced to a school, each user will use it differently, and the negative and positive effects will cause each social group to view the technology differently.

### ***Category 1: Users***

The users of the technology can be broken down further into the students who use the technology and the teachers who use the technology. In almost every case, if a class requires the use of a technology, the student is forced to use it if they want to participate to the fullest extent. No matter how the student feels about the privacy or data collection policy of the technology, they have no other options besides not taking the class (and even that is not possible in many cases). The other social group that uses education technologies is teachers who may not have the same priorities as the students. Often, technology will help teachers run their class more efficiently through testing, participation tracking, grading, and other features. Teachers do not enter as much personal information and are not tracked by the software as much as students, so they may have less of a personal problem using it. This dichotomy exemplifies how a piece of technology can have different meanings even within the same social group.

### ***Category 2: Choosers***

In some cases, teachers are also in the social group of the choosers of the technology depending on the school and department policy. If a teacher does decide to deviate from the school's technology choice, it may also require spending extra time or money. However, in other cases, the choosers of the technology are the school administrators and department chairs, who may or may not also be users themselves. School administrators set the rules about what technology can and cannot be used for all teachers, although they may set very relaxed policies and allow teachers to make their own decisions. Administrators and teachers have a completely different set of goals when selecting technology. School administrators want to please the teachers and the students with the policy they set, but they also need to minimize the overall cost of the software (time, money, and integrations with current systems) while ensuring it functions for faculty and students. Standardizing software helps students experience consistency between classes, but allowing teachers to use technology they prefer helps optimize their workflow. Balancing these factors is an important consideration for the adoption of a new technology in a school setting.

### ***Category 3: Makers***

The makers of the software can also be broken down into multiple sub groups—engineers who build the product, and product teams who design and market the product. In some cases (often in startups), the engineers drive the product and make the decisions, but in larger companies the design is often led by a product team, and the engineers are told what to make. In either case the engineers have a responsibility to build ethical software within the rules and regulations. The sales and marketing teams' objective is to get the software out to as many schools and users as possible. These teams have a responsibility to be truthful about the product,

but their primary motive is to convince school administrators and teachers to use their software in classes.

#### ***Category 4: Outside Social Groups***

One of the social groups outside the education technology ecosystem with the most influence over it are politicians. The government has control over what data schools can have from students, especially for public schools. In 1974, Congress passed FERPA, a set of regulations on educational data privacy (specifically for children under 18). Since the passage of FERPA, technology has changed drastically and that set of rules no longer provides comprehensive privacy protections. For example, regulators were not concerned with email in 1974, but FERPA was amended to include email as protected directory data in 2012 (Mendelsohn, 2012). Since then, more conversations have taken place within the government on “how emerging technology in the classroom affects student privacy” (U.S. Government Publishing Office, 2015). The other outside social group is parents, especially when technology is targeted towards younger children. During the period of online K-12 learning due to Covid-19, parents had more interactions with educational technologies than they would have while children were attending in-person classes.

#### ***Case Study: Piazza***

Piazza was founded in 2009 as a platform where students can ask questions about their classes and get answers from fellow students and teachers. It rapidly became popular among college classes due to its simple interface and efficiency for both students and teachers. Teachers no longer have to re-answer the same simple questions for multiple students in office hours. Students are no longer restricted to a few hours a week where they could ask questions; they can

post a question online and receive an answer at their teacher's convenience. Like many early stage startups, Piazza focused on developing the product and gaining users—not worrying about where their revenue would come from. Budgets in education are notoriously tight, and the Piazza team found that teachers and universities were either unwilling or unable to pay for their product directly. Eventually, they realized the value of the data they had collected from students and how much it could be worth to other companies (Hill, 2016). Piazza Careers launched as an adjacent product along with a new round of venture funding. They could collect a large amount of data on a student from their profile: name, email, class year, classes taken, and much more. This data alone can already be very useful, but when combined with the data from the rest of the product, it becomes more valuable (and more invasive). Imagine if a technology company could see that a student has answered a number of questions from a high level computer science class. Or, imagine the reverse—a company could find that a student had to ask a lot of questions to be able to complete even simple courses or assignments.

### *Interpretive Flexibility*

After Piazza launched Piazza Careers, they began to receive pushback due to unclear messaging about what data they do and do not sell. In a still posted tweet, Piazza claims that they “don't, and will never, sell student data” (Piazza, 2015). However, in their Terms of Service they say they will follow FERPA (Family Educational Rights and Privacy Act) unless consent is obtained from the student. However, the only place consent was actually obtained was a pre-checked box with a short description and a link to learn more (Hill, 2016). Three university administrations found this setup unacceptable and attempted to contact Piazza to resolve their concerns. UC Berkeley tried to come to a new agreement regarding the opt-in/out but were initially unable to come to a resolution. UC Davis took another step and recommended that

teachers not use Piazza in their courses. Similarly, University of Toronto had concerns over the ownership of their students' data and what oversight Piazza was taking. Although they did not go as far as UC Davis, they shared the privacy concerns with their faculty and let them make their own choice about whether to use Piazza for their classes (Hill, 2016).

### *Closure*

Academia, more than many other industries, has a very tight knit network and community. Many professors have studied and worked at other universities, and they collaborate and discuss research with members outside of their own institutions. The concerns and pushback surrounding Piazza spread to other universities and soon Piazza had many of their partner institutions requesting legal agreements as well as administrators reaching out for more information. Piazza quickly responded to these concerns in a public statement agreeing they had done a poor job and would work with the schools to better their privacy compliance (Hill, 2016). In some cases, sweeping changes were made. Piazza began to create formal contracts and agreements with universities to allow the administration to dictate some of the data policy. Today, Piazza's FERPA guidelines provide schools with a generic data privacy agreement while also allowing them to add their own terms and assurances (Piazza, 2021). Eventually, after even more pushback from school administrators, Piazza also switched from an opt-out to an opt-in system for student data collection.

### ***Case Study: Online Proctoring Software***

As online learning has expanded, so have online assignments and tests. Several companies, such as ProctorU, Examity, Honorlock, and Proctorio, have begun offering online test taking services for teachers and schools. Students install a piece of software from the company, and when it is time to take the test, a remote proctor watches the student's screen and

webcam to ensure no cheating occurs. Although online testing services have existed for a number of years, their use has expanded rapidly with the increase in online learning. In the past, Proctorio has added around 100 new clients a year, but this year they have been working with over 100 new clients a day. The forced switch to online learning also caused universities to acquire the software quicker than they normally would, potentially missing oversight or approval (Harwell, 2020).

### *Interpretive Flexibility*

Universities also overlooked software access issues as they forced its rollout. Some students lack access to stable internet or webcams, which can make it look like they are cheating even if they are not. Some of the online testing services require the student to be alone in the room, which can cause issues for students with roommates, partners, or children. The rapid expansion of the software has also caused a number of technical issues without the necessary support from the company to handle them. Some companies have added artificial intelligence to the software to support their limited staff of proctors, but the use of AI in the context has been found to falsely flag students as cheating in many cases causing them further trouble. These issues were enough for some schools to reject the software, such as Fordham University and the University of Oklahoma, but other schools were unfazed (Lawson, 2020).

Although there are many concerns about proctoring software, the biggest concern is regarding students' privacy. The features of the proctoring software, such as the ability to watch a student, view their screen, and interact with their computer, are similar to those found in the worst malware. Among the data collected from students is personally identifiable information (name, address, etc.), physical characteristics, and recorded videos. All of this information is passed on to the proctor to verify the student but a nefarious actor could spread that information



outside the company (ProctorU, 2021). The CEO of ProctorU even admitted to editing together clips of cheating students into an internal “hall of fame” video (Harwell, 2020). Complaints about privacy have come from every social group involved: students, teachers, administrators, and even outside groups. Students are forced to use the software to complete the class and are not given the option to opt out of any tracking or recording.

### *Closure*

Students from dozens of schools across the country started petitions rallying against the use of proctoring software, or at least requesting that their universities provide alternatives. One such petition at the University of Illinois Urbana-Champaign received over 1000 signatures and caused the university to discontinue their contract with Proctorio for the next year (Chin, 2021). Teachers have also been instrumental in discontinuing online proctoring services due to privacy concerns. At the University of California Santa Barbara, the faculty board wrote an open letter to the administration requesting that ProctorU not be used by the school. They cited privacy and accessibility concerns for students as the biggest problems with the service. Although the school did not completely remove ProctorU for the following semester, they did encourage teachers to re-design assessments to be more conducive to online learning as well as provide an option for students who do not wish to have their privacy violated with a proctored exam. At other schools, such as Duke and University of California Berkeley, the administrators stepped in to protect their students’ privacy and opted out of using the software at their schools (Lawson, 2020).

### *Case Study Review*

Both examples, Piazza and the online proctoring software, give insight as to how a technology can eventually be adopted into a school (or not) and the social interactions that affected its adoption. In both cases, an outside company tries to convince a school to use their

product which they have shown to be an effective technology. In Piazza's case, they were able to work with the schools and students to find a solution to the privacy concerns. Eventually, Piazza worked directly with the administrators to make sure they could change their product in a way to fit the schools' needs. Small changes were made over time and the software continued to spread in usage. On the other hand, online proctoring services were quickly rolled out to universities during Covid-19, but now some schools have discontinued their use as more and more privacy concerns arise. Unlike Piazza, online proctoring services have not been responsive in reacting to privacy concerns. In one case, ProctorU sued the University of California Santa Barbara Teachers Association for defamation for publishing a letter raising their privacy concerns (Harwell, 2020). The adoption of online proctoring services also gives insight into how students, teachers, and administrators interact to adopt technology into schools. The students pushed back on the proctoring services in most cases, but the teachers and administrators were much more divided on whether or not to use the services. In many cases, online proctoring services do help prevent cheating, which they might appreciate, but in some cases teachers and administrators understood the severity of privacy violations, even though they were not using the services themselves.

## **Conclusion**

The Social Construction of Technology framework demonstrates how pressures from each social group involved in educational ecosystems shape not only the adoption of a technology but also the technology itself. While the technology adopted in the end may not be superior, it becomes widely used because it was the version that was most flexible between the social groups. In the future, it is likely that more innovative technologies will be used in the classroom. Each new piece of technology in a school is initially adopted to benefit at least one

group, but other social groups will have very different opinions of how and where it should be used. As social groups resolve conflicts regarding technology, the technology will change or be repurposed to benefit every group and promote widespread use.

## References

- Basilon, Salvatore. (Feb 1, 2016). What are they doing with your data? The Varsity. <https://thevarsity.ca/2016/02/01/what-are-they-doing-with-your-data/>
- Chin, Monica. (Jan 29, 2021). University will stop using controversial remote-testing software following student outcry. The Verge. <https://www.theverge.com/2021/1/28/22254631/university-of-illinois-urbana-champaign-proctorio-online-test-proctoring-privacy>
- Harwell, Drew. (Apr 1, 2020). Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance. The Washington Post. <https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/>
- Hill, Phil. (Nov 10, 2016). Popular Discussion Platform Piazza Getting Pushback For Selling Student Data. eLiterate. <https://eliterate.us/popular-discussion-platform-piazza-getting-pushback-selling-student-data/>
- Hill, Phil. (Nov 13, 2016). Piazza Response To Blog Post On Student Privacy. eLiterate. <https://eliterate.us/piazza-response-blog-post-student-privacy/>
- Lawson, Sean. (Apr 24, 2020). Are Schools Forcing Students To Install Spyware That Invades Their Privacy As A Result Of The Coronavirus Lockdown? Forbes. <https://www.forbes.com/sites/seanlawson/2020/04/24/are-schools-forcing-students-to-install-spyware-that-invades-their-privacy-as-a-result-of-the-coronavirus-lockdown/#536aa909638d>
- Mendelsohn, Stephen A. (Jan 2, 2012). U.S. Department of Education Amends its FERPA Regulations to Allow for Certain Additional Student Disclosures. The National Law Review. <https://www.natlawreview.com/article/us-department-education-amends-its-ferpa-regulations-to-allow-certain-additional-student-disclosures>
- NetImperative. (Jan 29, 2018). 91% of startups admit to collecting personal data (but most aren't data compliant). NetImperative. <http://www.netimperative.com/2018/01/29/91-startups-admit-collecting-personal-data-arent-data-compliant/>
- Piazza. (Feb 7, 2015). "We don't, and will never, sell student data. Please email me if you'd like to chat" (@Piazza). Tweet <https://twitter.com/piazza/status/567776259363459073>
- Piazza. (July 30, 2018). FERPA Compliance. Piazza. <https://piazza.com/legal/ferpa>
- ProctorU. (July 1, 2020). ProctorU CCPA Privacy Policy. ProctorU. <https://www.proctoru.com/ca-privacy-policy>
- UCSB Faculty Association Board. (Mar 13, 2020). ProctorU Concern. UC Santa Barbara Faculty Association. [https://cucfa.org/wp-content/uploads/2020/03/ProctorU\\_2020-1.pdf](https://cucfa.org/wp-content/uploads/2020/03/ProctorU_2020-1.pdf)
- U.S. Government Publishing Office. (Feb 12, 2015). How Emerging Technology Effects Student Privacy. U.S. Government Publishing Office. <https://www.govinfo.gov/content/pkg/CHRG-114hhrg93208/html/CHRG-114hhrg93208.htm>
- Vescera, Zak. (Mar 27, 2019). Canvas is tracking your data. What is UBC doing with it? The Ubysey. <https://www.ubyssey.ca/features/double-edged-sword/>