Exploring Ethical Problems in Today's Technological World

Tamara Phillips Fudge
Purdue University Global, USA

A volume in the Advances in Human and Social Aspects of Technology (AHSAT) Book Series

Chapter 6
Privacy and Data Rights for Adult English as a Second Language (ESL) Students

Kimberly M. Rehak
Indiana University of Pennsylvania, USA

ABSTRACT

In the USA, instructors need to ensure the user privacy and data rights of their adult English as a second language (ESL) students. The ways in which educational technology (EdTech) companies track user activity and sell user data to third parties raises ethical concerns for student privacy and data rights. ESL students are particularly vulnerable because of the vague language in privacy policies and user agreements, differences in terms of state surveillance, and insufficient user privacy and data protections. In addition to a discussion on the ethical concerns within EdTech and higher education, one method and two tools to help ESL instructors and educators are provided. These assist with ESL or international students in their classrooms as a means to evaluate EdTech tools and make decisions on whether to adopt or require a digital tool.

INTRODUCTION

After downloading a new application to their phone or computer, users will—more often than not—quickly scroll to the bottom of the small-print terms and conditions to hit the "agree" button without a second thought. Similarly, when visiting a new website, there is a propensity to agree to "accept all cookies" and dismiss annoying pop-ups as quickly as possible.

Recent documentary films, such as *Coded Bias* (Kantayya, 2021) and *The Social Dilemma* (Orlowski, 2020), have exposed the American public to issues of data security, public surveillance, and the danger of unregulated tech. While both documentaries raise concerns that modern-day digital citizens (Ribble & Baley, 2007) should consider before engaging with technology, the effects of these stories on user behavior are underexplored. Rather, these documentaries highlight the small gains activists have made

DOI: 10.4018/978-1-6684-5892-1.ch006

in policy changes and show the need "to take on the massive amount of work still left to be done" (Han, 2020, para. 13).

Less attention has been given to similar issues in student data and users of educational technology (EdTech). EdTech is a term that encompasses software and applications with activities that allow for practice and lead to learning gains inside and out of the classroom (Lestari & Subriadi, 2021). The EdTech industry has expanded to an estimated market size of over $100 billion per annum ("Education Technology Market Size," 2022). Despite best intentions, EdTech companies perpetuate the educational achievement gap—making already marginalized populations even more so (Macgilchrist, 2019; Reich, 2020). Industry regulation varies significantly from country to country, meaning that research into the ramifications of EdTech's rapid expansion is usually contextualized by location in addition to grade level (i.e., K-12; higher education).

In the context of higher education in the United States of America, student digital records are protected under the Family Educational Rights and Privacy Act of 1974 (FERPA) (Checrallah et al., 2020). FERPA limits access to personal data in student records. More recently the Gramm-Leach-Bliley Act (GLB Act) has extended to protect the financial and financial aid records of post-secondary students from cyber attacks ("Gramm-Leach-Bliley Act," n d.). Additional laws protecting student data vary state by state (Gallagher et al., 2017), meaning student data privacy and protections are negligible at the federal level. Without proper protections and regulations, students' rights may be violated without their knowledge.

The ethics of using digital tools in learning environments with adult students is thus explored, as well as how educators can engage with pedagogical theories that ensure their students' privacy and data rights. While FERPA protection extends to international students studying in the USA, the unique concerns regarding the data rights of adult English as a Second Language (ESL) learners and the reasons why this subset of students is especially vulnerable will also receive consideration.

Some privacy and digital rights issues for tertiary-level ESL or international students include:

- Who is responsible for explaining and ensuring the comprehension of FERPA protections and privacy and digital rights to international students who speak English as a second language (ESL)?
- Which factors should instructors of ESL students consider before adopting an EdTech tool for their classroom?
- What should adult ESL students be taught with regards to their rights in a U.S. context and what does such instruction look like?

For the purposes of this publication, ESL will refer to students who are studying the English language in a location where English is common and used by the majority of the population. While the term has gone out of fashion in the Teaching English to Speakers of Other Languages (TESOL) field, this acronym has been used here to differentiate between ESL and English as a Foreign Language (EFL), referring to language instruction that takes place in locations where English is not routinely used by most of the population. As the context herein is within higher education institutions in the USA, ESL has been used to indicate international students whose native language is anything other than a form of English comparable to American English. This includes both English language learners (ELLs) matriculating to post-secondary institutions in the USA from K-12 settings and full-time international students arriving on an F-1 visa to study at the tertiary level.

Despite a focus on the rights of ESL students, any educator who has their adult learners engage with EdTech and/or has ELLs or international students in their classrooms with a first language incomparable with American English can benefit from this discussion.

EDTECH: ETHICAL CONCERNS, PEDAGOGICAL THEORIES, AND APPLICATIONS

Ethical Concerns Within EdTech and Higher Education

Two main ethical concerns with EdTech in higher education relate to user privacy and the anonymity of user data, or, rather, the lack thereof. User privacy refers to user tracking and encompasses not only activity tracking (e.g., search history, biometrics) but also the tracking of geolocation information and IP addresses. On the other hand, user data issues center around third parties accessing and using data without the knowledge or consent of the user and/or the selling of user data to third parties via data brokers. Myriad user privacy ethical issues within American post-secondary institutions raise questions concerning who is responsible for ensuring student privacy and data protection.

User Tracking

According to *The Social Dilemma* (Orlowski, 2020), gaining a person's attention is one of the biggest motivators for the use of tracking technology. Tech companies want to hook users into spending more time using digital tools, including applications (i.e., apps, for short) and other software, to provide companies with more data. More user tracking allows for better algorithms, which can inform private tech companies on ways to sell more targeted advertisements to feature on the "free" versions of their products.

Despite the ethical gray area of using data to manipulate technology to steal consumer attention, in education, a larger concern deals with the tracking and selling of student user data. The lack of transparency in EdTech regulation is an additional complication. Student data tracking by EdTech companies, academic researchers, and/or universities compromises students' data rights.

Much of the academic research into student digital rights and the ethics of tracking technology centers around wearable fitness apps used in disciplines, such as dietary sciences or physical education.

While one might assume that research subjects wearing tracking devices as part of a research study would have concerns about the tracking of their data, research has shown otherwise. For instance, in a human kinetics research study using student focus groups for data collection, 83% of all respondents acknowledged their understanding that their data would be used for the study—but not by third parties (Clark & Driller, 2020). This suggests that students often fail to consider the long-term ramifications that come with relinquishing their data rights. Clark and Driller (2020) recommend that data privacy be explicitly explained to participants in briefing sessions and that research should only use tracking devices when necessary for data collection. Yet, there is little guidance on the extent that research subjects should be briefed on their data rights or how to determine whether using tracking tools for data collection is necessary.

Tracking Through Learning Management Systems and Learning Analytics

The surveillance of students through their technology use has become commonplace. As a result, students may not consider the larger consequences of universities, researchers, and private EdTech companies tracking their activity and data. Hope (2018) also suggests that the surreptitious nature in which tracking is performed could also contribute to a collective "formal indifference" (p. 67) towards surveillance activities.

Most higher education institutions subscribe to learning management systems (LMSs) that assist instructors in the tracking of student work and progress. In fact, learning analytics is a burgeoning topic in higher education predicted to make a significant impact on the future of the field. The higher education non-profit, EDUCAUSE, published a multidisciplinary study looking into current perceptions on learning analytics. They found less than a third of the student participants reported concerns about the tracking of student demographic data or the equity of tracking identity markers (Brown et al., 2022). Faculty were 10% less concerned than students about demographic tracking, suggesting that most instructors fail to consider the consequences of student surveillance and, consequently, have formal indifference to student data tracking.

Furthermore, LMS tracking data and the field of learning analytics raise the issue of student data ownership. Many LMS vendors offer learning analytics in their systems. These data challenge student autonomy by allowing universities to collect a vast amount of data points on registered students. Jones (2019) argues that higher ed institutions should adopt a model for gaining consent from students to use their data for educational purposes. Additionally, students should be informed of the data practices of their institution through data visualization and be allowed to opt out of sharing their data (Jones, 2019).

Other harmful ways learning management systems and EdTech tools track student users include measuring the time users spend on various webpages and using predictive algorithms for adaptive learning technology. By tracking user behavior and monitoring student activity, adaptive technology makes it easier to predict future user activity. While this technology has the capability to individualize learning for students, this educational innovation also has the tendency to pigeonhole students who either underperform or are slower to show learning gains (Goodman, 2015). While this might not seem like a blatant ethical violation, Regan and Jesse (2019) warn that the "more sophisticated prediction that is built into many big data analytics transforms tracking and surveillance into a more powerful tool that can be wielded in ways that have not yet been identified and understood" (p. 172). The scale of user data collection (i.e., *Big* Data) is what provides EdTech companies with power, influence, and capital gains. Furthermore, not knowing the potential use of data or the end game of EdTech companies raises ethical concerns, particularly when these companies are working in the confines of the law. This tracking of student users raises larger questions about the regulation of the EdTech industry.

Issues With User Data

When students use EdTech tools, their data have a high probability of being sold to third parties or getting into the hands of the companies that create digital tools. Although advocates can speak out or warn against using certain apps or software that collect user data more than others, student users are left with little autonomy if they are expected or required to use digital tools for coursework.

Student user data does not have full protection at the federal level. Regan and Jesse (2019) make a strong case against basing activism only on student privacy issues. They argue that, in the USA, the

emphasis on user privacy leads to "Band-aid fixes" at the policy level. In other words, focusing solely on privacy issues fails to address the complexity of the problem with student data collection. Not considering issues like student autonomy or the ramifications of Big Data prevent legislators from taking a more comprehensive approach to protecting student data (Regan & Jesse, 2019). This, in turn, leaves student data vulnerable. Other, more expansive efforts at user data advocacy have also had minimal effect as they have not united with broader social movements. For instance, technology employees formed Tech Workers Coalition (TWC) in 2016 to call for their employers to employ more equitable practices (Costanza-Chock, 2020). However, most of the examples of tech worker advocacy are centered around federal government contracts that might violate user's federal civil rights.

Although they might not be digital rights activists, educators need to be aware of student user data vulnerabilities. Students, instructors, and university administrators are beholden to the procurement practices of their university and the ramifications of agreements with private EdTech companies. Richter et al. (2021) provide review criteria to consider for selecting an appropriate LMS, including a transparent procurement process, adherence to state laws, and "ethical decision-making" (Richter et al., 2021, p. 92). Yet, university procurement can sign contracts with whichever vendors they choose—regardless of the recommendations from the informational technology department or university review committee. EdTech companies are "at least one step removed from the data subject" (Regan & Jesse, 2019, p. 171), meaning that universities or instructors, in particular, need to know how and through what means student user data can be compromised. Without proper legal protections codified within state and federal law, student data can be "owned" by universities (Regan & Jesse, 2019) or at the mercy of EdTech companies' self-regulation.

Although Hewson (2015) delves into ethics related to digital research, much of the ways that researchers approach subject data is comparable to issues with student user data. First, consent becomes problematic when researchers mine "anonymous" student data—even when researchers specifically try to gain consent (e.g., from public discussion forums). Second, it is difficult for subjects to withdraw from digital research, especially if no consent was given or if research subjects have no knowledge of their data being researched. When research subjects or, by extension, students have a username that is completely unrelated to their legal name with no directly identifiable information, confidentially in online environments is regularly disrupted. Not only can users be identified through e-mail or IP addresses; but if researchers print direct quotes from publicly available pages, identifying data sources is as easy as Googling the quote in parentheses. Researchers should perform a risk assessment (Hewson, 2015) before using user data, just like instructors should do before requiring their students use a digital tool. Threat modeling, a tool that assists with performing a risk assessment and can help instructors with their EdTech decision-making processes, is also important to investigate.

Responsibility for User Privacy and Data Rights

In the USA, the EdTech industry is primarily self-regulated, meaning the responsibility of data protection falls on the end user. While there are some concerted efforts for company transparency and a pledged commitment to student data ("Student Privacy Pledge," n.d.), these efforts are focused on K-12 EdTech. EdTech marketed towards post-secondary students has less governmental and industry oversight, which calls accountability and responsibility for these students' data rights into question. For instance, if an end user is assigned to use a digital tool to complete an assignment, it is unclear whether the teacher or

the school should be held accountable if student data is collected and used unethically. Accountability issues for ELL and ESL student populations receive even less attention.

The Teaching English to Speakers of Other Languages (TESOL) International Association addresses the responsibility question in their 2008 publication *TESOL Technology Standards Framework*. With goals for both students and adult educators, the technology standards center around the use of technology to enable ESL learners to become responsible digital citizens. The TESOL technology standards put the onus of responsibility for student privacy and data rights on the instructors, as Goal 1, Standard 4, reads, "language teachers use technology in socially and culturally appropriate, legal, and ethical ways" (Healey et al., 2008, p. 31). Although ESL educators might be liable for the misuse of technology, such as the tracking of student user data, none of the student technology standards address privacy or data rights. Perhaps this is because user tracking, Big Data, and user surveillance were less prominent issues when the standards were written in 2008.

The ethical dilemma around student data collection is related to the type of EdTech being used in the classroom. For instance, LMSs are usually purchased through a contract with a private vendor, meaning that any data gathered from the LMS would be effectively "owned" by the university (Regan & Jessie, 2019). What actions universities take with LMS data will most likely be an ethical concern for learning analytics researchers in the coming years. On the other hand, if instructors ask their students to use a publicly available digital tool, such as Flipgrid or Edpuzzle, student user data will be proprietary to private EdTech companies. Rooksby (2020) warns that EdTech companies can meet the spirit of the law rather than the letter of the law (p. 1). If companies are tracking students in ways that are technically legal yet ethically questionable, teachers should be cautious when requiring digital tools in their classrooms.

Pedagogical Theories for the Instruction of Adults in Digital Learning Environments

Beliefs and experiences shapes instructors' attitudes towards utilizing EdTech in their classrooms. Similarly, instructors who adopt EdTech can apply a number of pedagogical theories that shape their practice. These theories guide instructors in their approach to both the instruction and application of digital tools to various learning environments. Two theories for instructors of adult ESL students to consider are digital citizenship (Ribble & Bailey, 2007) and critical digital pedagogy (Stommel, 2014). These theories shape the responsibilities of the instructor and the goals and/or outcomes of student engagement with EdTech as part of their learning.

Digital Citizenship

For their concept of digital citizenship, Ribble and Bailey (2007) outline nine elements, including digital literacy and digital rights and responsibilities, which claim to create responsible student users of digital technology. The main goals in the advocacy for digital citizens are to equip students with 21st century skills and improve their learning outcomes. Ribble and Bailey (2007)'s nine elements aim to meet those goals through a three-tiered model that moves from the personal (i.e., student performance) to the school-level to the life outside of the school (p. 44).

Davis (2017) recommends two approaches for teaching digital citizenship (Ribble & Bailey, 2007): the proactive and the experiential. The former includes the nine elements, like passwords, private and personal information, and professionalism; whereas the latter refers to providing students with the oppor-

tunity to apply and test out their learning. For instance, Davis (2017) mentions having students practice recognizing facts and allowing for collaborative learning.

As an extension to digital citizenship, Bhargava et al. (2015) argue that instructors and students gain data literacy. Currently, most training in data literacy focuses on training teachers how to interpret student performance data (Bhargava et al., 2015), missing an opportunity to empower students by showing them how to use data for good, such as engaging with community issues happening right outside of the classroom walls.

Critical Digital Pedagogy

Critical digital pedagogy (Stommel, 2014) has derived to account for critical pedagogy in digital learning environments. Central to critical pedagogy is getting students to think beyond the walls of the classroom and consider how "they, as students, fit into broader social and cultural context" (Young, 2019, para. 2). Furthermore, critical pedagogy implies action—students engaging in their communities, out in "the real world." The *critical* in critical pedagogy implies instructor advocacy and the empowerment of students. Power is distributed equitably in the classroom, which is seen when instructors provide students with the language, tools, and context in which the instructor and students find themselves in.

Bradshaw (2017) investigates the intersection of critical pedagogy and educational technology, stating that culture is key and often missing when EdTech is used by educators who adhere to a positivist philosophy (p. 16). Culture can dictate how technology is created, designed, and used (Bradshaw, 2017, p. 20). Rorabaugh (2012) also recognizes the influence of culture in the classroom centered around critical pedagogy. "If students live in a culture that digitizes and educates them through a screen, they require an education that empowers them in that sphere, teaches them that language, and offers new opportunities of human connectivity" (Rorabaugh, 2012, para. 7). Critical digital pedagogy takes these ideas one step further.

Moreover, critical digital pedagogy engages students beyond their phone or computer screen. Community, collaboration, and communication are used in tandem to unite students "across cultural and political boundaries" (Stommel, 2014, What is Critical Digital Pedagogy section). Critical digital pedagogy calls for instructors to unite student voices in online learning environments and facilitate knowledge construction that is applicable beyond the "screens" of a typical digital learning environment. In sum, critical digital pedagogy asks instructors to connect students with the outside world in a meaningful way, to spark curiosity in learning itself and to get them to ask critical questions within a community of practice (CoP) (Lave & Wenger, 1991)—a tenet of adult education.

Unique Learner Needs for ESL Students

Over one million international students are enrolled in American colleges and universities in any given year (Israel & Batalova, 2021). Universities will set required minimum scores on language proficiency tests (usually the Test of English as a Foreign Language (TOEFL) for institutions in the USA) for international student admission. Individuals with lower proficiency scores are usually placed in language support classes and considered ESL students. These students will then work to improve their English proficiency, with an emphasis on academic English vocabulary and productive skills required for post-secondary studies (i.e., speaking, writing, and notetaking).

Even with a high proficiency in English, many international students are experiencing instruction both in English and within American academic culture for the first time (Bergey et al., 2018). Without proper institutional attention and support programs, these students are often left on their own to navigate their new "education norms, communication habits, and classroom participation structures" (Bergey et al. 2018, p. 4). In addition to orientation sessions, international students require help and support from higher ed institutions to succeed. Unless instructors have training or certification to work with ESL students, educators are oftentimes unaware of the unique circumstances affecting ESL, ELL, and/or international students highly proficient in English. Because of this, it is important for all educators in post-secondary institutions to consider the digital tools and rights for this subset of the student population.

Digital Tools for Adult English Language Learners

The goal of ESL classes is to equip students with the cultural know-how and language skills needed to communicate effectively in a variety of the English language—primarily academic English or English for Specific Purposes (ESP).

Some ESL students might be informed digital citizens in their native language or home country. For instance, they might be active on global platforms, such as Twitter or Instagram, or social media outlets created by technology firms in their home countries. However, ESL instructors should not assume their students have similar competency with digital tools in an educational or American context. Critical digital pedagogy (Stommel, 2014) explains the need for ESL instructors to utilize digital tools to have students interact with one another in digital and non-digital spaces. This means that while being advocates for student engagement with the digital world beyond the classroom, instructors also must ensure the rights and digital privacy of their students.

Few would argue against the use of digital tools for learning and in foreign language learning. Digital tools, such as Snapchat, FlipGrid, or VoiceThread, allow students to record themselves and engage with one another as well as users around the world. Students can practice their productive skills, making audio or video recordings and writing comments, which allow for situated learning (Goodwin-Jones, 2017, p. 6) and interaction in a CoP. Adaptive technology allows for personalized learning that meets the unique needs of learners, using spaced retrieval practice for correcting student errors and encourages learners to learn, as reported by Bourekkache & Kazar (2020), on their own outside of the classroom.

Anecdotally speaking, teachers who are early adopters of tech may not be able to realize or measure the ramifications of having students use a new digital tool. The new use or potential for student engagement might overshadow the risk that the adoption of the new product. For instance, Duolingo is a platform that uses gamification in a mobile-assisted language learning (MALL) context to allow user to study an additional language with an approximate 15-minutes-per-day commitment. Despite the popularity of the platform in the mainstream and as a topic of academic research, the effectiveness of the program and the outcomes of users are rarely measured. In a systematic review of research on the Duolingo platform, Shortt et al. (2021) found that the majority of the 35 research studies focused on the design of the app rather than its effect. This suggests a trend in the EdTech industry to focus more on the making and design of digital tools rather than "the process and outcomes of language learning from using these tools" (Shortt et al., 2021, p. 1). These mirror, in many ways, the actions of instructors who are early adopters of EdTech, who place more attention on the novelty and potential of digital tools instead of the risks and efficacy that come along with them.

DATA RIGHTS FOR ESL STUDENTS

Language in Terms and Conditions

Despite the advantages that digital tools can provide to ESL classes, instructors need to be careful before requiring any for student use. In the American context, most free tools come with hidden costs to students' privacy. As there is "no national standard for how to acquire consent" (Checrallah et al., 2020, p. 138), it is essential for instructors to read and understand the language in privacy policies and end-user license agreements or terms of service. ESL students are particularly vulnerable to privacy rights because of the complicated and intentionally vague language contained in these statements, which are difficult for educated native English speakers to understand (Checrallah et al., 2020). In a study of the transparency of language in privacy and digital security policies in mental health apps for individuals with depression, five out of the 116 apps investigated used transparent language (O'Loughlin et al., 2019). Perhaps even more concerning is that O'Loughlin et al. (2019) also found that only 49% had privacy policies and, of those, the vast majority (nearly 80%) were apps that collected identifiable user data.

According to LePan (2020), the average American, non-ESL reader (at 250 words per minute (wpm) would need ten minutes to read Instagram's terms of service, which is one of the shortest user agreements, while the user agreement from Microsoft is estimated to take an entire day to get through. In addition to the length of privacy and end-user agreements, the language complexity of these agreements also makes it more difficult for ESL students to read and comprehend the entirety of their digital rights. The results of a quantitative research study conducted by Mora et al. (2021) show that reading speed and reading comprehension are influenced by a few factors, such as English level, profession, and gender. While a highly proficient ESL reader can read common, everyday reading materials, such as newspaper or magazine articles, at a rate of around 50 fewer words per minute (wpm) than the average American non-ESL reader, more complex reading materials that contain advanced, specialized vocabulary and more complex grammatic structures, require deeper language processing. This means that the average reading speed is reduced significantly—to 70 fewer wpm. Therefore, it would take a proficient ESL reader an extra four minutes to read Instagram's terms and services and an extra nine hours and 20 minutes to get through Microsoft's policies.

The vague language in the terms and conditions allows the EdTech companies to track and sell user data with user consent and disadvantages ESL learners. Instructors of ESL, ELL, and international students should also be reviewing the terms and conditions of tools used in their classroom. Additionally, individuals at post-secondary institutions responsible for EdTech procurement should be equipped to understand and advocate for student user rights before agreeing to contracts with private vendors.

Privacy and User Tracking

When instructors require students to register for a digital tool, they are asking the students to provide private information (e.g., demographic information, e-mail address) to tech companies that often do not have the best interest of the students in mind. Depending on the language in the user agreement, user information, like the IP address or geolocation coordinates, is provided to companies directly (Checrallah et al., 2020) or sold to external parties through third-party data brokers. Data points can be used to find users' locations, meaning that online anonymity is near impossible (Thompson & Warzel, 2019). For instance, Snapchat users agree to location tracking and facial recognition software is used in their filters.

Companies also sell location data to third parties for a return on investment for their services. This selling of data is the hidden cost of free software and applications. ESL instructors should avoid assigning work in digital tools that make it easy to track ESL students' activity. Additionally, ESL instructors need to consider the unique aspects of their students' lives that might make them particularly susceptible to tracking and surveillance.

Since U.S. government agencies, like Immigration and Customs Enforcement (ICE), have purchased tracking data to surveil individuals at the USA-Mexican border (Molla, 2020), requiring ESL students to use apps that track user data, which, in turn, can be sold to federal government agencies, could be harmful for students whose immigration status is questionable or unknown. Furthermore, instructors should not encourage or require ESL students to do anything that makes their students susceptible to surveillance or internment by a foreign government (in this case, a U.S. federal agency).

Students or teachers who think they "have nothing to hide" are still vulnerable to Big Tech and EdTech companies. Data is a profitable resource for figuring out user behavior to exploit it through targeted ads or using it for more nefarious ends, such was the case of Cambridge Analytical and the 2016 U.S. election. Importantly,

This data is immensely valuable to those who know what to do with it – and that value has a lot to do with scale. The more data that a company or group has to play with, the higher its chances of achieving its goals, either by identifying a larger number of people who might be interested in what it has to say, or by figuring out exactly what they are thinking, and speaking to their views specifically. (Ghosal, 2018, para. 6).

ESL instructors should consider their students' privacy and data rights a top priority, especially as the learning analytics field continues to grow.

Different Experiences With State Surveillance

Depending on their home country, the experiences of ESL students with state surveillance can be an extremely disparate situation than the one in the USA. Students from countries with more state surveillance may be unaware of their digital rights under U.S. federal law (i.e., FERPA) which could also lead to different attitudes towards user tracking and data brokering.

To illustrate such a difference of opinion, Zhu & Yang (2019) used an online survey method to investigate the perceptions of digital ownership and digital rights of American and Chinese students at the tertiary level. While American students were more likely to report a sense of ownership of their digital property, Chinese students were concerned with understanding digital rights, which could be attributed to the difference in China's and the USA's digital cultures. While China has been regulating its digital EdTech markets and their delivery, the American federal government provides less regulation of EdTech companies. This suggests that when Chinese students attend American universities, they may not realize their data rights are different than they are at home and that they might have fewer protections than they realize.

ESL educators can raise this issue outright in their classrooms by having students compare the situation in the USA with that of their home country. Dedicating part of a lesson to have students compare and contrast the level of state surveillance in different countries can raise awareness of the extent that governments protect the privacy of their citizens and regulate their tech companies. Instructors can

use Comparitech's ranking of surveillance states at https://www.comparitech.com/blog/vpn-privacy/surveillance-states/ to facilitate this exercise. Additionally, instructors can have their students hypothesize reasons that explain the various rankings of the countries from Comparitech's website. ESL instructors can turn this activity into an exercise for practicing both digital citizenship as well as grammatical structures, such as comparative and superlative adjective forms.

TEACHING PRACTICES AND TOOLS THAT INFORM AND PROTECT ESL STUDENTS

ESL instructors should be sure that they are equipping students with the right tools to facilitate communication while protecting their students' rights. Unfortunately, research has shown that student privacy and data rights are a low priority for educators in multiple disciplines. Lupton (2020)'s survey looking into the considerations and practices of health and physical education instructors in Australia found that educators rarely think about who has access to student data when using digital tools in the classroom. Similarly, only 10% of respondents to an educator survey on data privacy were aware of what happens with student data ("Educator Toolkit," 2018). Marín et al. (2021)'s mixed-methods study of 148 preservice teachers from 3 different countries (i.e., Germany, Spain, and the USA) also found that avid social media users, so-called "digital natives" (Prensky, 2001), knew little about data privacy from their own social media use. Digital natives are individuals who have grown up with modern technology integrated into their lives, and the priorities of digital citizenship curricula tend to vary by age group. For example, cyberbullying affecting K-12 students more than adult learners. Many adult learners and adult educators are "digital immigrants" (Prensky, 2001) whose experiences with digital technology differ from younger generations of digital natives. The result from Marín et al. (2021) suggest that it is difficult to get "digital native" educators to think about their students' data rights if they are not considering their own.

Instructors should use a reference, like The Common Sense Media evaluation tool at https://privacy.commonsense.org/evaluations/1 to ensure they are assigning digital tools, which are minimally detrimental to students' privacy and digital rights. Taking a few minutes to visit the Common Sense Media resource might have a big impact on the data privacy of ESL students in the USA.

While it is important for ESL students to engage in the world beyond their devices, they must be shown how to do so in a way in which their digital rights are protected. Instructors should dedicate time to explaining to their students what they are agreeing to, what information tech companies are collecting, and what rights they might be relinquishing. As privacy rights differ from country to country, some students might need to learn what rights they have before they agree to consent to an end-user license agreement or terms of service or a privacy policy. Furthermore, instructors should be prepared to provide alternative assignments if students choose not to consent. With the vast majority of educated Americans not reading terms and conditions, it is safe to assume that ESL students are not fully aware of their privacy and user data rights when using digital tools while studying in the USA.

Teaching Students to Protect Their Privacy

The onus of protecting the privacy and digital rights of ESL students is in the hands of instructors or curriculum developers who require their students to use various language learning apps and digital tools. However, digital citizenship (Ribble & Bailey, 2007), data literacy (Bhargava et al., 2015) and

critical digital pedagogy (Stommel, 2014) all call for instructors to empower students by helping them help themselves. Threat modeling is one way that instructors can show their students how to protect their data rights. Instructors should consider using this method for themselves as well as their students.

Threat Modeling

As explained by members of the privacy advocate group Electronic Frontier Foundation (EFF), threat modeling is a way to protect what is important to users and which individuals or organizations they need protection from ("How to Protect Your Online Privacy," 2017). Instructors can get students to think about what aspects of their user data they need to keep secure and the individuals or organizations from which they should protect it. The latter should warrant a longer conversation with students who come from countries with a tradition of heavy state surveillance, like China (Bischoff, 2019) or the United Arab Emirates (Mackenzie, 2020). The remaining three steps to threat modeling involve, considering the likelihood of the threat, the consequences if the threat is violated, and the amount of work it would take to avoid negative consequences ("How to Protect Your Online Privacy," 2017). A decision-making tool, which incorporates many of the considerations included in threat modeling, is provided in the appendix.

In addition to threat modeling, instructors can show their ESL students some practical tips to secure their user privacy both in the USA and in general. First, passwords should contain a list of completely randomized words to avoid hacking. Second, free tools or plugins, such as Adblock or DuckDuckGo, can help to block web tracking. Instructors should get in the habit of testing any digital tool or plugin prior to recommending it to students. If there is a teacher or paid version of any app or piece of software, instructors should be sure to check out the privacy and user experience on the free and/or student versions before they have students download them.

Instructors should also educate their students on issues related to school surveillance and encryption. EdTech tools, such as Chromebooks, have lenient default settings that allow for more user data collection by tech firms (e.g., Google, in this case) ("How to Protect Your Online Privacy," 2017). Accessing and changing default settings can become a classroom activity that might even result in students teaching their peers or family members about their own data rights. Finally, students should learn how to protect their data using encryption. One easy way to do this is to inform students to look for the "S" in https:// to know they are using encrypted sites. Students should also avoid using open Wifi networks or learn how to use encryption tools if they must use open networks to prevent others from tracking their data.

Tools for Instructors to Make Informed Decisions About EdTech

In addition to threat modeling, two tools are offered to help the decision-making process of educators who want to use EdTech and also protect their students' privacy and digital rights. It is also recommended that educators limit the amount of EdTech tools that are used in their classrooms. Sometimes the novelty of a new app or platform will take attention away from the actual usefulness of the tool or the learning gains it might facilitate.

Instructors need to be mindful that they and their students have time to investigate and learn the system. Additionally, instructors need to set aside time to explain the benefits and risks that the new tool can have on their students' privacy and data rights. Not only will this time and attention allow for well-informed digital citizens, but these capture the ethic and advocacy considerations engrained in critical digital pedagogy

Should I Use This Edtech Tool? Decision Making Guide for Instructors

To help ESL instructors make more informed decisions on whether to include EdTech tools in their classroom, Figure 1 includes a decision-making tool with ten questions and various ranking scores to determine if a tool is more or less likely to violate user privacy and data rights. This decision-making guide was created using input from Gallagher et al. (2017) and Rooksby (2020) with the intention of nudging educators to think about ways in which they can protect the privacy and data of their students.

Common Sense Media Evaluation Tool

One step embedded in the decision-making tool is the Common Sense Media Evaluation Tool at https://privacy.commonsense.org/evaluations/1, which determines the probability that a tech company will sell user data to third parties. The Common Sense website should be the first stop of any educator concerned for their students data privacy rights.

CONCLUSION

There are many concerns about the privacy and data rights of ESL adult students. When instructors require students to use various digital tools for learning, they should ensure they are protecting and the data rights of their students and properly explaining these rights to them. However, instructors have reported knowing very little about the content of privacy and data user agreements—if they even consider this information at all. Digital tools raise ethical concerns as they can track user behavior, their personal information, their geolocation, and other identity markers. This could make ELL and ESL students vulnerable to tracking, which could unintentionally affect students with questionable immigration status.

Concerns for ESL instructors include the complicated language in terms and conditions and their students' reading speed, proficiency, and comprehension. Additionally, instructors should explicitly teach ESL students about differences in data privacy and state surveillance between the local context and their home countries by using a website that ranks countries on the amount of state surveillance. Finally, using threat modeling and/or decision-making tools, such as the *Common Sense Media Evaluation Tool and the Should I Use This EdTech Tool? Decision-Making Guide for Instructors* found in the appendix can help to guide instructors to using EdTech that will support the learning of their students while protecting their students' privacy and data rights.

REFERENCES

Bergey, R., Movit, M., Baird, A. S., & Faria, A.-M. (2018). *Serving English language learners in higher education: Unlocking the potential.* American Institutes for Research. https://www.air.org/sites/default/files/downloads/report/Serving-English-Language-Learners-in-Higher-Education-2018.pdf

Bhargava, R., Deahl, E., Letouze, E., Noonan, A., Sangokoya, D., & Shoup, N. (2015, September). *Beyond data literacy: Reinventing community engagement and empowerment in the age of data.* Data-Pop Alliance (Harvard Humanitarian Initiative, MIT Media Lab and Overseas Development Institute) and Internews. https://dspace.mit.edu/bitstream/handle/1721.1/123471/Beyond%20Data%20Literacy%202015.pdf

Bischoff, P. (2019, October 15). *Data privacy laws & government surveillance by country: Which countries best protect their citizens?* Comparitech. https://www.comparitech.com/blog/vpn-privacy/surveillance-states/

Bourekkache, S., & Kazar, O. (2020). Mobile and adaptive learning application for English language learning. *International Journal of Information and Communication Technology Education*, *16*(2), 36–46. doi:10.4018/IJICTE.2020040103

Bradshaw, A. C. (2017). Critical pedagogy and educational technology. In A. D. Benson, R. Joseph, & J. L. Moore (Eds.), *Culture, learning, and technology: Research and practice* (pp. 8–27). Routledge. doi:10.4324/9781315681689-2

Brown, A., Croft, B., Dello Stritto, M. E., Heiser, R., McCarty, S., McNally, D., Nyland, R., Quick, J., Thomas, R., & Wilks, M. (2022, February 9). *Learning analytics from a systems perspective: Implications for practice.* EDUCAUSE. https://er.educause.edu/articles/2022/2/learning-analytics-from-a-systems-perspective-implications-for-practice

Checrallah, M., Sonnett, C., & Desgres, J. (2020). Evaluating cost, privacy, and data. In T. Trust (Ed.), *Teaching with Digital Tools and Apps.* EdTech Books. https://edtechbooks.org/digitaltoolsapps/evaluatingcostprivacydata

Clark, M. I., & Driller, M. W. (2020, February). University students' perceptions of self-tracking devices, data privacy, and sharing digital data for research purposes. *Journal for the Measurement of Human Behaviour*, *3*(2), 128–134. doi:10.1123/jmpb.2019-0034

Costanza-Chock, S. (2020). *Design justice: Community-led practices to build the worlds we need*. The MIT Press. doi:10.7551/mitpress/12255.001.0001

Davis, V. (2017, November 1). *What your students really need to know about digital citizenship: Ideas on how to guide students to the knowledge and experience they need to act responsibly online.* Edutopia. https://www.edutopia.org/blog/digital-citizenship-need-to-know-vicki-davis

Education technology market size, share & trends analysis report, by sector (preschool, k-12, higher education), by end-user (business, consumer), by type, by deployment, by region, and segment forecasts, 2022 – 2030. (2022, April). Grand View Research Publishers. https://www.marketresearch.com/Grand-View-Research-v4060/Education-Technology-Size-Share-Trends-31517238

Educator toolkit for teacher and student privacy: A practical guide for protecting personal data. (2018, October). Parent Coalition for Student Privacy & the Badass Teachers Association. https://cdn.ymaws.com/www.a4l.org/resource/resmgr/files/sdpc-publicdocs/PCSP_BATS-Educator-Toolkit.pdf

Gallagher, K., Magid, L., & Pruitt, K. (2017, May 4). *The educator's guide to student data privacy.* Connect Safely. https://www.connectsafely.org/wp-content/uploads/2016/05/Educators-Guide-Data-.pdf

Ghosal, A. (2018, April 25). *Why we should collectively worry about Facebook and Google owning our data.* The Next Web. https://thenextweb.com/news/why-should-you-care-if-google-and-facebook-own-your-data

Goodman, E. (2015, April 28). *Privacy in the classroom: What you need to know about educational software.* The International Association of Privacy Professionals. https://iapp.org/news/a/privacy-in-the-classroom-what-you-need-to-know-about-educational-software/

Goodwin-Jones, R. (2017). Smartphones and language learning. *Language Learning & Technology*, *21*(2), 3–17.

Gramm-Leach-Bliley Act (GLB Act). (n.d.). *EDUCAUSE*. https://library.educause.edu/topics/policy-and-law/gramm-leach-bliley-act-glb-act

Han, A. (2020, December 30). *Two Sundance docs sound the alarm on the dangers of modern AI: Is the tech industry... bad?* Mashable. https://mashable.com/article/coded-bias-social-dilemma-documentary-review

Healey, D., Hegelheimer, V., Hubbard, P., Ioannou-Georgiou, D., Kessler, G., & Ware, P. (2008). *TESOL technology standards framework*. Teachers of English to Speakers of Other Languages, Inc. https://www.tesol.org/docs/default-source/books/bk_technologystandards_framework_721.pdf

Hewson, C. (2015). Ethics issues in digital methods research. In H. Snee, C. Hine, Y. Morey, S. Roberts, & H. Watson, (Eds.) Digital methods for social science: An interdisciplinary guide to research innovation. Palgrave Macmillan.

Hope, A. (2018, May). Creep: The growing surveillance of students' online activities. *Education and Society*, *36*(1), 55–72. doi:10.7459/es/36.1.05

How to protect your online privacy with threat modeling [Video]. (2017, November 15). Above the Noise. https://www.youtube.com/watch?v=VlYjtWg4Thw&ab_channel=AboveTheNoise

Israel, E., & Batalova, J. (2021, January 14). *International students in the United States*. Migration Policy Institute. https://www.migrationpolicy.org/article/international-students-united-states-2020

Jones, K. M. L. (2019, July 2). Learning analytics and higher education: A proposed model for establishing informed consent mechanisms to promote student privacy and autonomy. *International Journal of Educational Technology in Higher Education*, *16*(24), 24. Advance online publication. doi:10.118641239-019-0155-0

Kantayya, S. (2021). *Coded bias* [Film; online video]. Independent Lens. https://www.codedbias.com

Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation*. Cambridge University Press. doi:10.1017/CBO9780511815355

LePan, N. (2020, April 18). *Visualizing the length of the fine print, for 14 popular apps.* Visual Capitalist. https://www.visualcapitalist.com/terms-of-service-visualizing-the-length-of-internet-agreements

Lestari, N. D. I., & Subriadi, A. P. (2021, September). EdTech investment: Optimism, pessimism, and uncertainty. *2021 International Conference on Electrical and Information Technology (IEIT)*, 239-245. 10.1109/IEIT53149.2021.9587429

Lupton, D. (2020, March 3). 'Honestly no, I've never looked at it': Teachers' understandings and practices related to students' personal data in digitised health and physical education. *Learning, Media and Technology*, *46*(3), 281–291. doi:10.1080/17439884.2021.1896541

Macgilchrist, F. (2019). Cruel optimism in edtech: When the digital data practices of educational technology providers inadvertently hinder educational equity. *Learning, Media and Technology*, *44*(1), 77–86. doi:10.1080/17439884.2018.1556217

Mackenzie, L. (2020, January 21). *Surveillance state: How Gulf governments keep watch on us.* Wired. https://wired.me/technology/privacy/surveillance-gulf-states

Marín, V. I., Carpenter, J. P., & Tur, G. (2021, September 20). Pre-service teachers' perceptions of social media data privacy policies. *British Journal of Educational Technology*, *52*(2), 519–535. doi:10.1111/bjet.13035

Molla, R. (2020, February 7). *Law enforcement is now buying cellphone location data from marketers.* Vox. https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration

Mora, F., Quito, R., & Macías, L. (2021). Reading comprehension and reading speed of university English language learners in Ecuador. *Journal of English Language Teaching and Applied Linguistics*, *3*(11), 11–31. doi:10.32996/jeltal.2021.3.11.3

Orlowski, J. (2020). *The social dilemma* [Film; online video]. Exposure Labs. https://www.thesocialdilemma.com

Prensky, M. (2001, October). Digital natives, digital immigrants. In *On the Horizon, 9* (Vol. 5). MCB University Press.

Regan, P. M., & Jesse, J. (2019, September 15). Ethical challenges of edtech, big data and personalized learning: Twenty-first century student sorting and tracking. *Ethics and Information Technology*, *21*(3), 167–179. doi:10.100710676-018-9492-2

Rehak, K. (2022, May 29). *Should I Use This EdTech Tool? Decision-Making Guide for Instructors* [Image]. Academic Press.

Reich, J. (2020). *Failure to disrupt: Why technology alone can't transform education*. Harvard University Press. doi:10.4159/9780674249684

Ribble, M., & Bailey, G. (2007). *Digital citizenship in schools*. International Society for Technology in Education.

Richter, S., Rhode, J., Arado, T., & Parks, M. (2021, Fall). Principles for conducting a comprehensive LMS review. *The Community College Enterprise*, *27*(2), 89–94.

Rooksby, J. H. (2020, January 13). Consider impact of institution's tracking apps on privacy, best interest of students. *Campus Legal Advisor: Interpreting the Law for Higher Education Administrators*, *20*(66), 1–3. doi:10.1002/cala.40173

Rorabaugh, P. (2012, August 6). *Occupy the digital: Critical pedagogy and new media.* Hybrid Pedagogy. https://hybridpedagogy.org/occupy-the-digital-critical-pedagogy-and-new-media

Shortt, M., Tilak, S., Kuznetcova, I., Martens, B., & Akinkuolie, B. (2021, July 5). Gamification in mobile-assisted language learning: A systematic review of Duolingo literature from public release of 2012 to early 2020. *Computer Assisted Language Learning*, 1–38. Advance online publication. doi:10.1080/09588221.2021.1933540

Stommel, J. (2014, November 17). *Critical digital pedagogy: A definition.* Hybrid Pedagogy. https://hybridpedagogy.org/critical-digital-pedagogy-definition

Student privacy pledge. (n.d.). *Student Privacy Compass*. https://studentprivacycompass.org/audiences/ed-tech

Thompson, S. A., & Warzel, C. (2019, December 19). *Twelve million phones, one dataset, zero privacy*. The New York Times. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

Young, J. R. (2019, June 4). *What is critical digital pedagogy, and why does higher ed need it?* EdSurge. https://www.edsurge.com/news/2019-06-04-what-is-critical-digital-pedagogy-and-why-does-higher-ed-need-it

Zhu, X., & Yang, T. (2019, October 18). Do I own it?: US and Chinese college students' digital ownership perceptions. *Proceedings of the Association for Information Science and Technology*, *56*(1), 346–355. doi:10.1002/pra2.28

APPENDIX

Figure 1. Should I Use This EdTech Tool? Decision-Making Guide for Instructors
Source: Rehak, 2022

Should I use this EdTech tool?: Decision-making guide for instructors

1) List how the EdTech tool will serve students in terms of its benefits and drawbacks.

Benefits for students (+1 for every benefit)	Drawbacks (-1 for every major drawback)

2) Are you able to measure the benefit of the tool? Yes (+1) No (+0)

List how you are able to measure the benefits of this tool.

3) Do the benefits of this tool outweigh the drawbacks? Yes (+1) No (+0)

Explain your answer.

4) The company or group that makes the EdTech tool has been verified by my school or institution. Yes (+1) No (+0)

5) The Common Sense Media Evaluation Tool shows the company or group that makes the EdTech tool is trustworthy. Pass (+3) Warning (+1) Fail (-1)

6) If applicable, the company complies with my state's data privacy laws and/or the EU's General Data Protection Regulation? Yes (+1) No (+0)

7) The EdTech tool forces students to register with an e-mail address. No (+1) Yes (-1)

8) The EdTech tool will publicly display user content. No (+1) Yes (-1)

9) The company or group that makes the EdTech tool has explicitly said they will not sell user data. Yes (+1) No (-1)

10) The learning benefits of the EdTech tool cannot be achieved through other means. Yes (+1) No (+0)

TOTAL POINTS=

10+ points	4-10 points	under 4 points
Yes, definitely!	Maybe, but consider other options.	No! Do not use this tool!