
CPIQ
Consumer Privacy & Identity Quarterly
The Transformative Impact of eLearning
How personalized, on-demand learning shapes modern society and privacy
Welcome to the 21st Century Classroom!
Check out new high-tech features
Illusion of Privacy
Is online learning more "public" than public school?
VOLUME 4 ISSUE 4

In this Issue

When School is Always in Session:

Learning in the Modern Age

For decades, our cultural perceptions of schools and classrooms remained mostly unchanged. Popular Hollywood hits such as *The Breakfast Club* (1985), *Clueless* (1995), and *Mean Girls* (2004) all capture familiar educational environments—public spaces where students gather to learn under the watchful eyes of teachers and administrators. Students socialize in hallways, take notes with pens and paper, carry books from class to class, and occasionally stress about homework or tests. For many readers, this notion still holds true today.

In the early 2000s, the education industry started to undergo a significant shift. Thanks to the advent of Internet accessibility and consumer computing technologies, learning became electronic. Over time, we've incorporated more high-tech gear and digital enrichment into standard learning activities. Modern eLearning presents a complex landscape containing many types of devices, apps, Internet-based services, and online communities that support the pursuit of knowledge for users of every age. Kids today can start using eLearning tools as infants, and for most, educational technology will accompany their learning endeavors through high school or college and into the working world.

Online learning frees education from the confines of the classroom, enabling us to study any subject, anytime, anywhere—whether for academic achievements or just for fun. Feel overwhelmed or socially anxious navigating your massive college campus? Try a virtual course instead. Hectic work schedule? Register to take a semester's worth of online classes at your own pace. Looking for a niche community of language learners? There's an app for that! eLearning services strive to accommodate all users and enable an unprecedented level of learning customization and ease.

Along with online learning, we've seen an uptick in the types of technology used in schools. It's common to issue tablets or laptops to students—to use both in class and at home—and to administer tests and manage coursework through online platforms. Classrooms are filled with smartboards (interactive touch screens rather than blackboards), smart visualizers (today's high-end take on the traditional projector), and then, of course, there are the cameras. Cameras installed at school entry points to screen students and visitors, in hallways to monitor activities between classes, and cameras in the classroom to track attendance and even student attentiveness.

Are all these devices helpful? Advocates argue eLearning tools make sense—that next-generation, technology-infused study programs help educators precisely cater educational material to each student's needs, ensure academic integrity, and provide clear insights on how to make classes better. Schools that don't embrace technology are pegged as "under-resourced" or seen as deliberately, and perhaps suspiciously, bucking the norm, such as the "low-tech" Waldorf Schools favored in Silicon Valley.

Interacting with eLearning technologies can, however, significantly increase our digital footprint. Educational tools capture a wealth of information about each learner, ranging from mundane registration details to faces, from communication metadata to video viewing histories. Collectively, these bits of background information can create detailed pictures of one's personal life. Read on to learn more about eLearning—what today's education landscape looks like, the devices and services therein, and how you can protect your privacy while learning.

Early Learning Apps are Early Opportunities for Online Safeguarding

Digital learning apps cater to kids of every age—even infants. To entice parents, early learning apps promise to help develop cognition, problem-solving, and motor skills. But are they always beneficial?

Some offer little educational value and are arguably games masquerading as academic tools, or even just channels for advertising. Worse, they may emotionally influence young users into making in-app purchases. For example, Doctor Kids shows characters that express sadness or cry when a child closes-out of pop-up ads. In such cases, children are exposed to manipulative marketing techniques.

Many popular apps pair users with other learners and encourage them to share messages, pictures, voice and video clips, and location data with in-app "friends." For example, language-learning tool Tandem—rated "E Everyone" and tagged as an "Education" app in the Google Play store—encourages multimedia exchange and even offers a "members near me" feature in the Pro version. Prior to downloading early learning apps, parents should always review what permissions are requested.

Finally, early learning apps may not adequately safeguard children's data. In December 2015, a rogue security researcher hacked eLearning platform VTech, a leading supplier of children's early educational toys and games. The researcher-turned-hacker accessed over 316,000 accounts, collecting profile information with names, birth dates, pictures, chat logs, and account information with parents' names, billing addresses, and email addresses; he was later fined for privacy violations. VTech's response focused on the fact that no credit card information was collected, but downplayed the overall privacy implications. A hacker can sell a child's bundled app data (including photo and address) to predators or identity thieves.

Early learning applications help kids get a head start on new topics. They also provide an excellent opportunity to learn how to engage with online technology while protecting personal privacy and digital wellbeing.

ILLUSION OF PRIVACY

Taking courses online can seem like a safer and more private alternative to learning in traditional school settings. Students learn from the comfort of home, at their own pace, without directly interacting with peers and teachers. Are online educational pursuits truly more private, or are eLearners inadvertently sharing a wealth of digital information? Let's compare and contrast information sharing in traditional and online classrooms.

Physical ID cards	**IDENTIFICATION**	Face recognition
In-person relationships	**SOCIAL CONNECTIONS**	Online relationships
Verbal discussion (not usually recorded)	**COMMUNICATION**	Digital communication including email, chats, voice or video conferencing, and forum posts, (all can be recorded)
Students submit work on paper or digitally to a teacher, who returns or disposes of it when a lesson is complete	**CLASSWORK SUBMISSIONS**	Students submit work online privately to a teacher or publically to a class; the work may be accessible long-term
Schools are public settings	**LOCATION DATA**	Online learning applications may track student IP addresses, revealing residential locations and other frequented places
Teachers and School Administrators monitor student activities	**MONITORING**	Suites of software sensors track students continually, and much more precisely

What are eLearning Tools Learning about YOU?

For a modern-day learner, education often happens online. Interested in learning about a topic? The Internet provides plenty of options—a simple Google search for the busy, a podcast for users on-the-go, or a free online course offered by a top-tier university for the intellectually curious. From Wikipedia, YouTube tutorials, to virtual classes, the opportunities seem boundless—but at what cost? Read on to find out about the most popular types of eLearning platforms and how they may harvest your data.

Massive Open Online Courses (MOOCs)

MOOCs refer to open-access online courses. The popularity of MOOC platforms like Coursera and edX has made the term nearly synonymous with eLearning. In addition to traditional class materials such as filmed lectures, readings, and tests, MOOCs provide interactive forums where students and teachers can communicate and comment on each other's work. In addition to personally identifying information collected during registration, MOOCs gather session data such as IP address and geographic location to track attendance. They also collect student-generated content, including correspondence and homework submissions. Depending on the nature of the course and assignments, tracked data may reveal the user's educational preferences, history, and skill levels.

Gamified Learning Platforms

Gamified learning platforms use game principles such as points, progression, and competition, to make learning activities fun. They are interactive by design and adapt courses based on user performance and feedback. Popular examples include Duolingo (a language learning app) and CodeAcademy (which offers free online software development classes). Due to their interactive features, gamified platforms may process sensitive data including voice and video. For instance, Duolingo records users' voices to test language pronunciation and provide feedback. Additionally, users may be pushed to submit documents such as government-issued ID to obtain official certifications.

Learn-It-Yourself (LIY) Resources

LIY resources refer to any educational content users can access outside dedicated eLearning platforms. Popular examples include websites, blogs, video tutorials, and podcasts. A social networking service (SNS) becomes a LIY resource when used to share educational content and connect with other learners. This form of eLearning takes place on platforms owned and operated by tech giants such as Google, Apple, and Facebook. Therefore, the data created while interacting with LIY resources—such as browsing and search history—have a higher likelihood of being aggregated with users' existing digital trails. Watching a woodworking tutorial on YouTube, for example, may generate ads for workshop tools on other Google services.

Privacy risks are not limited to consenting adults. The Federal Trade Commission (FTC) recently fined Google $136 million for collecting children's data without parental consent, after determining that Google illegally tracked children's watch histories and collected personally-identifying device information through YouTube Kids, its video app for users under age 13. Regulations are improving to protect users from harmful data collection practices, but companies are searching for loopholes to monetize data—even children's.

While eLearning platforms can provide quality education with unprecedented convenience and accessibility, remember that they are technology companies first and foremost. Their primary goal will always be the same: attract users and monetize user data.

Learning to Learn with Educational Technology:

Best Practices for Privacy Protection

Schools are increasingly high-tech. Gone are the days of specialized computer labs. Now, it's typical for a whole campus to have Wi-Fi, and for each student to have a tablet or laptop. Schools may use services like Blackboard or G Suite to deliver coursework, assign homework, and publish grades.

Educational technology encompasses most aspects of school life and carries over into a student's home life as well. Because modern learning tools seamlessly blend with existing school activities, students, teachers, parents, and school administrators may not have a complete understanding of associated privacy or security risks. All parties must critically consider how educational technology is being used, and raise concerns accordingly.

Let's review a few best practices to help protect student data.

Do's and Don'ts for Students:

- DON'T connect personal devices, like smartphones, to school Wi-Fi.
- DON'T share passwords with friends.
- DON'T disclose unnecessary information on online educational platforms (leave that "About Me" section blank!).
- DO tell a parent or teacher if your school device breaks, or if you download something you are not supposed to.
- DO keep the webcam covered when it's not in use.

Advice for Parents:

- Emphasize that school-issued devices should only be used for schoolwork (...not Fortnite!). Devices may be monitored, and misuse may result in negative consequences like suspension.
- Help your child set default permissions on school-issued tools to minimize data collection
- Know your laws—such as the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA)—which protect student information and children's data.

These practices outline just a few ways parents and students can help protect personal data when using educational technology. Learning how to use technology safely and take responsibility for online data sharing is a complex subject in its own right, and critical for a student's future.

Biometrics in Schools:

Improving Security or Risking Privacy?

We expect public spaces to be as secure as possible. At first glance, it seems entirely reasonable to use cutting-edge technology, like face recognition (FR), to keep people safe. Supporters cite several desirable benefits, while critics point out risks for privacy invasion or unnecessary surveillance. In school settings, especially those involving children, this debate is particularly contentious.

As reported by *The Buffalo News*, in 2018, the Lockport City School District in New York approved the installation of Aegis facial recognition systems in 10 public school buildings. Three hundred cameras were placed at critical points throughout the properties to help screen for suspended students and teachers, non-custodial parents, and registered sex offenders. After installation, however, the State Education Department blocked the use of FR due to privacy concerns. The school district continues to lobby for the system to be turned on, citing $2.75 million in sunk costs and tangible security benefits.

In the digital world, systems like Gaggle (which plugs into a school's G Suite or Microsoft 365 platform) constantly monitor a school's online content, looking for text or images that could indicate a student is contemplating suicide, perpetrating violence, or breaking school rules. Homework submissions aren't the only thing being monitored online. In 2017, ESG Business School in Paris announced plans to use software from Nestor. The product pairs FR and artificial intelligence to track student engagement during online video lectures, specifically examining students' facial expressions and movements through webcams. Any sign of inattentiveness—scrolling news sites or chatting—triggers a pop-up quiz.

So what pros and cons are at play when it comes to using biometrics and cutting-edge tracking technologies in educational facilities?

Biometric Benefits

- **Improve security:** identify authorized and banned individuals. Biometric sensors such as cameras can also alert administrators to fights or bullying.
- **Track attendance:** scanning student fingerprints or faces when they enter or exit classrooms helps monitor attendance and time missed when students step out. Extend learning opportunities: biometrics help certify digital learning and testing, allowing students to keep pace with coursework outside a physical classroom
- **Ensure academic integrity:** biometrics help educators identify students during exams. Keystroke recognition used during computer-based testing ensures students don't help each other, or copy and paste responses.

Potential Risks

- **Mandatory participation:** For a system to work correctly, everyone in a school setting—students, parents, teachers, staff, and visitors—must participate. Those who opt-out may find it harder to come and go or use certain services.
- **Surveillance and tracking:** Beyond identification, it's possible to trace people's movements and social interactions in school spaces.
- **Ambiguous data management policies:** Backend biometric data storage practices can be complex and unclear. Where is data stored? Who can access it—school officials? Police? What happens to students' data after graduation?
- **Cybersecurity vulnerabilities:** Implementing biometric systems in school properties creates another type of digital information that is only as safe as the facility's overall cybersecurity infrastructure.

Going forward, it will be necessary to gauge how much biometric technologies benefit school security. While these systems offer numerous opportunities, it remains to be seen if the benefits outweigh the call for collecting more personal data.

Welcome to the 21st Century Classroom!

Schools are in the midst of a technology transition, and it doesn't stop with laptops replacing textbooks. Educators invest in connected technologies to innovate classrooms. From smart tables to biometric devices and artificial intelligence (AI), the next generation of "smart" classrooms are poised to create personalized and collaborative learning experiences for all students.

Principles of a Modern Classroom

- Shared Purpose
- Interest-Powered
- Peer-Supported
- Community-Centered
- Openly-Networked

Wireless Access Points

Robust and reliable Internet connections are crucial to modern classrooms. Schools are replacing outdated ethernet cables with wireless access points to ensure seamless connectivity between students and the learning material.

Education Applications (e.g., Google Classroom)

Classroom applications help teachers utilize material from outside their school and integrate it into lesson plans. Functions such as remote scheduling, linked event planners, and administrative access enhance organization and classroom management.

The New Blackboard

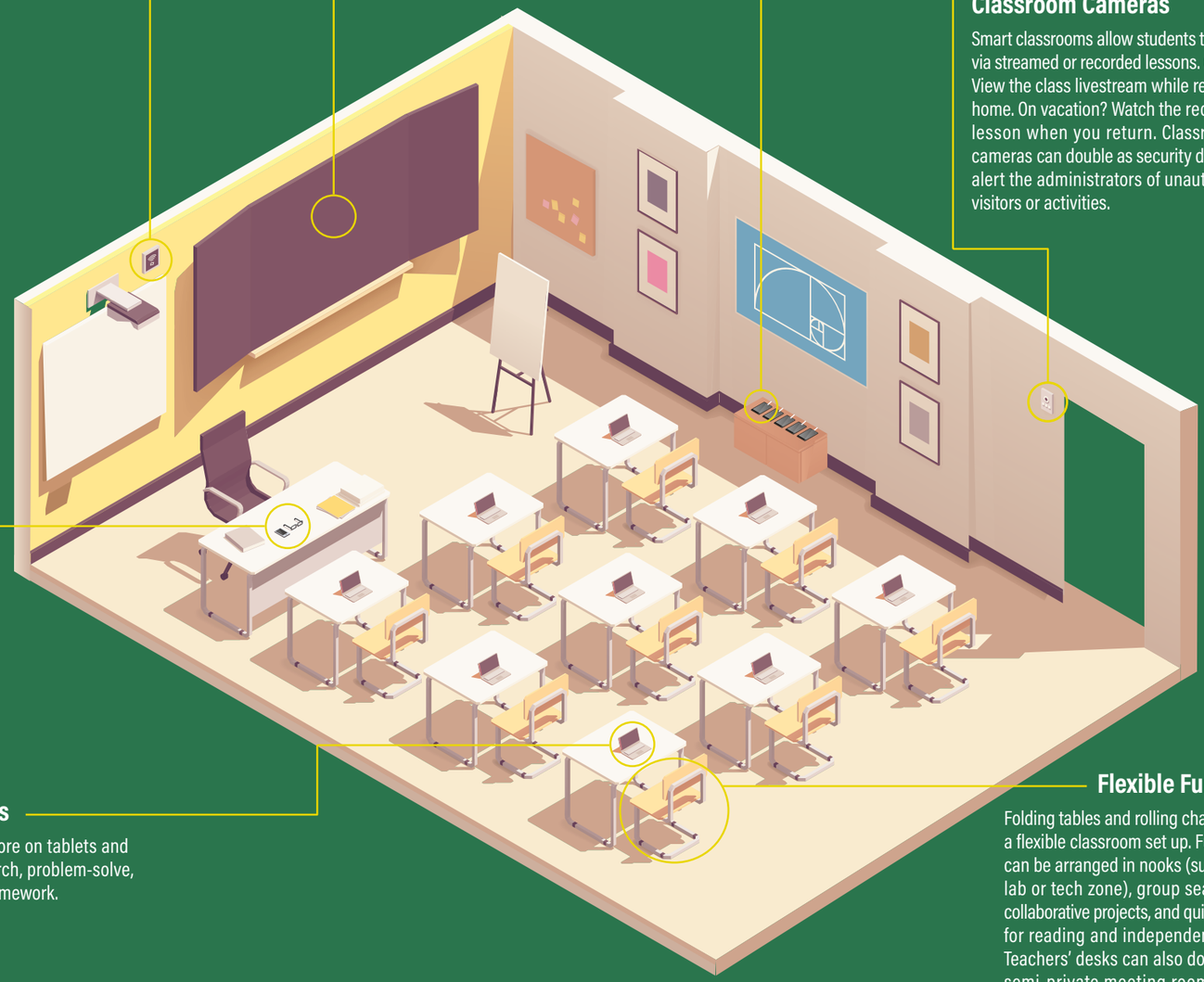
Interactive screens and digital whiteboards offer students a crisp view of course material. Smartboards also connect to other classroom devices, allowing teachers to showcase learning material at the front of the room and on individual student laptops.

Charging Solutions

Charging cabinets and carts power multiple devices via a single outlet. Recent variations are equipped with high-end charging technologies, like a smart cycle or intelligent charging. These features optimally power devices and protect them from charging overloads to help increase the life of classroom devices.

Classroom Cameras

Smart classrooms allow students to engage via streamed or recorded lessons. Out sick? View the class livestream while resting at home. On vacation? Watch the recorded lesson when you return. Classroom cameras can double as security devices to alert the administrators of unauthorized visitors or activities.



Smartware for Teachers

Smart technology is helping teachers support students with unprecedented levels of efficiency. Examples include microphones that help distribute learning material to those in need of hearing assistance, and smart glasses that signal when students need extra help, even if they don't raise their hands.

Digital Student Devices

Teachers have begun to rely more on tablets and laptops to help students research, problem-solve, ask questions, and complete homework.

Flexible Furniture

Folding tables and rolling chairs create a flexible classroom set up. Furniture can be arranged in nooks (such as a lab or tech zone), group seating for collaborative projects, and quiet spaces for reading and independent study. Teachers' desks can also double as semi-private meeting rooms for student-teacher discussions and individual instruction.

The Transformative Impact of eLearning

Electronic learning, or eLearning, delivers educational and training content through popular devices such as computers, tablets, smartphones, and smart speakers connected to the Internet. Today's eLearning paradigms aim to free users from the restrictions of traditional classroom settings, making it easy to learn anytime, anywhere.

The term "eLearning" was coined in 1999 by educational and technology expert Elliott Maisie, one of the most well-known figures in the industry. In the 20 years since, eLearning has become extremely popular, primarily due to significant advances in the hardware, software, and Internet infrastructures that underpin it. Mobile devices and laptops are more affordable than ever, enabling learning on-the-go. Interactive media delivers rich, gamified content at the click of a button, keeping learners more engaged. It's now common practice for schools to use cloud-based Learning Management Systems (LMS)—software applications that create, store, and deliver online course material. Many LMSs also use Experience Application Program Interfaces (xAPIs), which track on—and offline user experiences. Collected data helps educators govern study plans and understand how to enhance online educational activities.

The eLearning Landscape: Something for Everyone

The eLearning industry offers a diverse range of tools specially designed to meet unique learner needs and educational requirements. eLearning tools can broadly be described as synchronous or asynchronous. Synchronous eLearning involves real-time interaction, communication, and feedback between students and teachers, and is commonly found in virtual classrooms and chat-based courses. Asynchronous eLearning—the most common form of eLearning used by today's workforce—is self-paced and completed independently.

The Student Learner

Modern pupils of all ages, from pre-k to Ph.D. students, can access eLearning tools. Children start using computers and online resources in school early on. Teachers may supplement classroom time with online materials, such as nursery rhymes or documentaries. Many middle and high schools provide student laptops along with online platforms, which teachers use to assign homework, share additional study resources, report grades, and proctor online testing.

By the time today's students reach college, they are familiar with numerous eLearning formats. Many colleges offer blended in-person and online courses—a significant shift from traditional classroom learning, as it offers teachers and students more flexibility. Many colleges and universities partner with Massive Open Online Course (MOOC) platforms where classes can be taken for free, or in a certified format for a fee.

The On-the-Job Learner

Online learning and training tools permeate modern workplaces. Employees typically complete some form of initial or annual training through LMSs. Working professionals may be particularly attracted to eLearning tools, which accommodate work schedules and offer the chance to chart a customized learning plan that fulfills individual career needs.

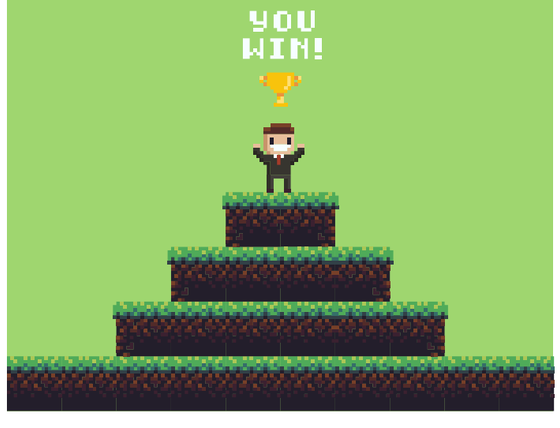
For example, the professional social networking site LinkedIn acquired eLearning platform Lynda in 2015. Lynda offers a wide range of professional development and certification courses through its website. Social platforms such as Google+ serve as popular eLearning tools for corporate education and collaboration, offering employees a place to network, develop, troubleshoot, collaborate, discuss, and visualize projects they are working on.

What is Gamification?

Gamification applies game design concepts to make educational content more appealing, interactive, and memorable. Strategies abound, but most gamified services dole out rewards when learners complete tasks or achieve goals. Points, badges, mastery levels, in-game virtual currency—all compensate a user's time and interest. Rewards are often publicly visible (for example, via a leaderboard); this encourages learners to connect, socialize, and directly complete. Gamification also delivers an immersive sensory experience that potentially includes sounds, flashing content, and animations to drive user engagement. Traditional books and flashcards seem dull in comparison, no?

Gamification is increasingly popular in eLearning and viewed as a more effective and enjoyable way to deliver content that may otherwise be boring or difficult. It also provides novice learners with an encouraging experience that shepherds them through the study material while building confidence and providing positive feedback. Gamification is not just a feature strictly for children or school settings either—it's used in the workplace too. By turning mundane annual compliance or onboarding training into a fun and interactive means of learning, employees may demonstrate higher levels of engagement and better retain training content.

Of course, this raises the question of how much fun is too much—and whether all learning needs to be enjoyable in order to be effective. Critics argue that incorrect use of gamification techniques may actually stunt students' natural, internal motivations to learn, and also create unrealistic expectations. Gamification is a perk of modern learning, but it can't be added to every educational scenario.



The Self-taught Learner

Formal educational platforms aren't the only option though. Many people turn to online resources like YouTube or Reddit to learn how to complete do-it-yourself projects, pick up new hobbies, or simply explore topics of interest.

Never cooked a Thanksgiving Day turkey? No worries—just pull up a smartphone or smart speaker and follow step-by-step instructions right in your own kitchen. If a recipe doesn't explain enough about proper turkey prep techniques, track down a video tutorial. Have international friends visiting for the holiday? Download a language learning app to pick up basic words and phrases to explain the dishes and entertain your guests.

The eLearner's Digital Footprint

Engaging with eLearning technology creates a wealth of digital data, and eLearners must consider what kinds of information can be collected. For example, in addition to a student's standard profile information such as name, date of birth, address, phone number, and perhaps a photo, LMSs also collect details on course progression, report cards, curriculum schedules, number of sessions, log-in times, and the number and types of materials downloaded. Educators assert these data points help them get to know students and figure out ideal learning models. But what about eLearning's social collaboration and networking aspects?

Many eLearning platforms and apps encourage online engagement in discussion forums and collaborative workspaces. Participation can be problematic, as it may reveal a learner's friends and classmates, location, interests, habits (e.g., what time of day they post), or the type of work they do. Analytical tools may be employed to track and profile online engagement—whether learners post in class discussion pages, how long and detailed those discussions are, and what social connections are formed along the way.

Taken as a whole, data associated with online learning can provide an intrusive look into learners' behavior and interests—which can be very useful to advertisers targeting specific marketing campaigns, or to anyone profiling students. The eLearning market is highly profitable. According to Global Industry Analysts, Inc., the industry is expected to be worth $406 billion globally by 2024. Involved service providers understand that student learning data is everywhere and that it can be harnessed to sell products to students. Vendors may bury consent to private user information within terms of service, causing users to overlook or ignore those key points.

At the most basic level, it is essential to consider the IT security infrastructure before using specific eLearning tools. Has an eLearning vendor or tool been hacked before? Is student data being shared? With whom, and for what purpose? Or even, is a student's data visible to other users? It's easy to consider schools as "safe" spaces, or online classrooms as "private," when they may be anything but.

eLearning offers numerous benefits to all parties involved, and innovative educational tools are continuously showing up in our app stores. As eLearning becomes more engaging, learners of all types must consider how their educational pursuits augment online identity.

When the Real World is not Enough:

How Immersive Technologies will Shape Education

So-called immersive technologies promise to disrupt every major industry, and education is no exception. Augmented reality (AR) overlays, digital information onto real-life environments using smart hardware. Virtual reality (VR) simulates an entirely new environment through a headset. Mixed reality (MR) functions as a combination, providing a higher level of interactivity than AR without the complete immersion of VR.

How are immersive technologies pushing educational boundaries beyond the confines of computer screens and to our 3D world?

Virtual Field Trips

Apps like Google Earth VR and Unimersiv use head-mounted displays to help students tour sites like the Egyptian Pyramids or Stonehenge without leaving the classroom. Along with a 360° view, virtual field trips provide educational content through narration, pop-up text, and images during the journey. Trips are not limited to real-world destinations; much like a real-world version of *The Magic School Bus*, these technologies make a trip inside the human body or Mars possible. Similarly, virtual science labs allow students to run experiments without laboratory risks.

Next-Generation Student Management

Lumilo, a MR smart glasses product developed by Carnegie Mellon University, pairs with an AI-powered "cognitive tutor" app to offer real-time analytics on every student present. The app projects students' engagement levels above their heads using visual cues—smiley faces, question marks, or exclamation points. The AR cues help teachers identify which students require extra help (?) or are about to cheat on the quiz (!). Like in a sci-fi movie, the teacher can see more details about each student by tapping on the student's in-air status.

While these scenarios are technologically within reach, privacy concerns and funding remain significant barriers to mainstream use. Immersive technology enables even more intimate and pervasive user data collection and tracking. It is up to lawmakers, administrators, and parents to prioritize the safety and privacy of students and their data above immersive technology's flashy capabilities.

Test Your Knowledge: What have You Learned about eLearning?

1. True or false: Free e-Learning courses are unable to collect your user data if you do not need to provide a name to register.

2. A school can do all of the following with student-issued learning devices, except:

   a. Remotely monitor webcams and microphones
   b. Log users' keystrokes and software downloads
   c. Allow third-parties to collect data
   d. Remotely wipe device memory
   e. Conduct parent-teacher meetings

3. Early learning apps target audiences as young as:

   a. Infants
   b. Age 2
   c. Age 3
   d. Age 5
   e. Age 13, due to legal restrictions

4. Digital learning platforms can require what information for user identification:

   a. Government-issued photo ID
   b. DNA
   c. Geolocation
   d. All of the above
   e. A and C only

5. Potential risks of biometric surveillance systems in schools do not include:

   a. Mandatory participation
   b. Consent-based parenting
   c. Surveillance and tracking
   d. Ambiguous data management policies
   e. Cybersecurity vulnerabilities

6. All of the following are companies in the growing e-learning industry except:

   a. Google
   b. Nestor
   c. Lockport
   d. Blackboard
   e. VTech
   f. Tandem
   g. Lynda

7. Protections for child data privacy include:

   a. COPPA
   b. SAFR
   c. LMS
   d. FTC
   e. USDA

8. Student data cannot be transmitted via:

   a. xAPIs
   b. MOOCs
   c. Wi-Fi
   d. LMSs
   e. AR/VR
   f. IAPM
   g. SNS

9. Early learning apps have been observed manipulating children by...

   a. ...requesting children input their parents' credit card number.
   b. ...taking photos with the device's camera for targeted marketing.
   c. ...promoting in-app purchases using emotions of the game characters.
   d. All of the above

10. True or false: Elliott Maisie coined the term "eLearning" in 1999.

Answer Key 1. False 2. e 3. a 4. e 5. b 6. c 7. a 8. f 9. c 10. True

The Last Word

State-of-art eLearning tools help us access information in new, innovative ways. They deliver educational content to physical and virtual classrooms, in a way that can be highly personal and optimized for each learner. Overall, it's easy to argue that eLearning tools create value. Students learn, not just about a given subject, but how to use technology in general—and how to use it safely.

However, the popularity of eLearning tools raises critical questions. We tend to think of school environments as generally safe and protected—but when eLearning tools are involved, are reasonable protections in place? Furthermore, learning via a MOOC or an app may create an illusion of privacy. You might be taking a course from the comfort of your living room rather than in a crowded lecture hall, after all. Still, this engagement creates a broad digital footprint that we don't normally associate with privacy or cybersecurity. For today's learners, this footprint can be life-long and encompass many vital aspects of life—from school to work, home, and leisure. As eLearning technologies become more immersive and data-driven, it will be critical for learners of all types to consider how educational pursuits add to their digital identities.

In the Next Issue...

First, an exciting announcement—the next issue of CPIQ will feature a new "Trending in Consumer Privacy" section that captures essential news and developments about technologies covered in earlier issues. Consumer privacy is an ever-changing area, and the CPIQ Team hopes the new addition will help keep readers up to speed throughout the year.

The upcoming Winter issue of CPIQ will discuss the Modern Traveler—hopefully just in time to inform your plans for spring break. What state-of-art technologies do today's travelers encounter? If you haven't ventured abroad in the last few years, some changes may surprise you (read: who's ready to ditch tickets, passports, and airport screening lines in favor of using facial recognition?). The issue will cover the ins and outs of some cutting-edge smart travel accessories that may help smooth your travel experience, and discuss how you can make the most of online resources such as location-based apps, vacation rental services, and social engagement tools—all while protecting your privacy while on the road.

For more detailed information on protecting and managing other key elements of your identity footprint online please check out the:

IDENTITY AWARENESS, PROTECTION AND MANAGEMENT GUIDE