

University of Massachusetts Amherst
ScholarWorks@UMass Amherst

Teacher Education and Curriculum Studies
Educational Materials

Department of Teacher Education and
Curriculum Studies

2020

Teaching with Digital Tools and Apps

Torrey Trust
University of Massachusetts Amherst

Follow this and additional works at: https://scholarworks.umass.edu/tecs_ed_materials

Recommended Citation

Trust, Torrey, "Teaching with Digital Tools and Apps" (2020). *Teacher Education and Curriculum Studies Educational Materials*. 1.
https://scholarworks.umass.edu/tecs_ed_materials/1

This Book is brought to you for free and open access by the Department of Teacher Education and Curriculum Studies at ScholarWorks@UMass Amherst. It has been accepted for inclusion in Teacher Education and Curriculum Studies Educational Materials by an authorized administrator of ScholarWorks@UMass Amherst. For more information, please contact scholarworks@library.umass.edu.

Teaching with Digital Tools and Apps

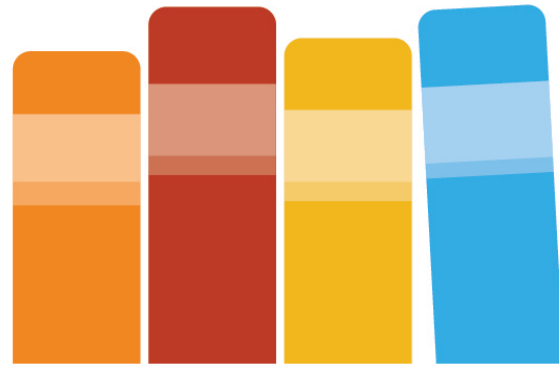
Torrey Trust



Torrey Trust

Version: 1.2

This book is provided freely to you by



Ed *Tech* Books.org



EdTechBooks.org



CC BY-NC-SA: This book is released under a CC BY-NC-SA license, which means that you are free to do with it as you please as long as you (1) properly attribute it, (2) do not use it for commercial gain, and (3) share any subsequent books under the same or a similar license.

Table of Contents

<i>Introduction</i>	2
<i>Evaluating Cost, Privacy, and Data</i>	6
Back Matter	20
<i>Author Information</i>	21
<i>Citation Information</i>	22

Introduction

With the abundance in education technology (edtech) tools and apps currently available, and new ones popping up in app stores daily, how do you find the right ones for your practice? How do you ensure the digital tools and apps that you select for use in your classroom will enrich and extend your teaching, provide an accessible learning experience, and protect students' privacy? What should you look for when evaluating the user experience of apps and tools?

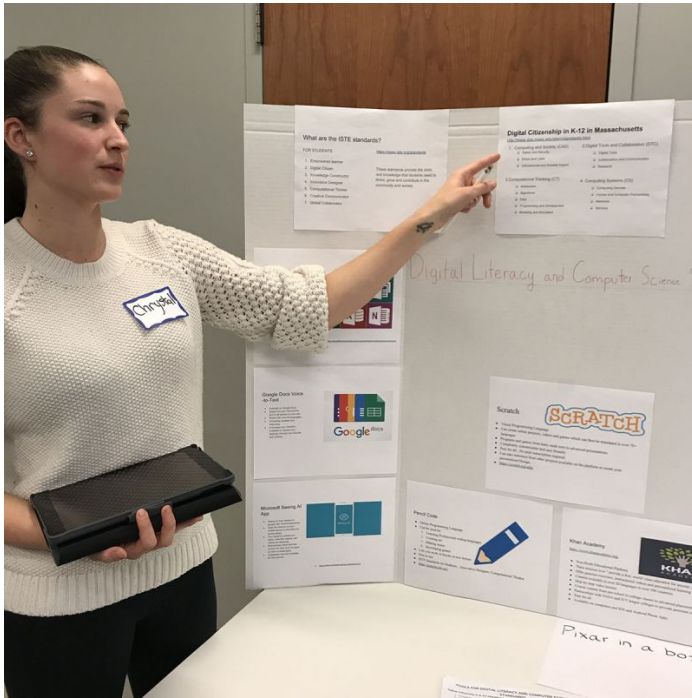
This free, open access eBook highlights the key steps and considerations for finding, evaluating, and teaching with digital tools and apps.

The book was designed as part of a class project for EDUC 593A: Teaching & Learning with Technology at the [University of Massachusetts Amherst](#). The following undergraduate and graduate students contributed to the book: Michelle Barrett, Matthew Checallah, Jacob Desgres, Alyssa Federico, Kiel Maurath, Madeleine Olson, Shaunak Shah, Khizar Shaikh, Alexander Shum, Caroline Sonnett, Isabelle Manrong Wang, Chenyang Xu, Chrystal Zajchowski, and Fred Zinn.

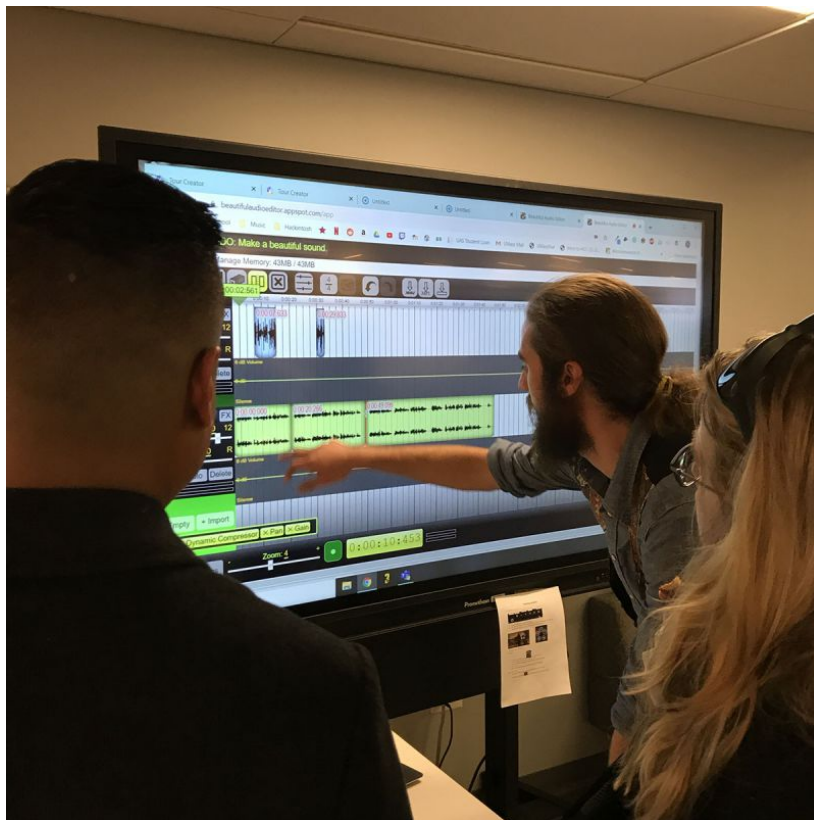


Kiel, Michelle, and Fred (authors) at the College of Education Tech Tools Showcase

Teaching with Digital Tools and Apps



Chrystal, one of the book authors, discussing Digital Literacy and Computer Science at the College of Education Tech Tools Showcase



Jacob, one of the book authors, showcasing Beautiful Audio Editor at the College of Education Tech Tools Showcase

Using This Book

We hope that you find this book to be a valuable resource. Feel free to share it or use it in your class or training! This book is released under a [CC BY-NC-SA license](#), which means that you are free to do with it as you please as long as you (1) properly attribute it, (2) do not use it for commercial gain, and (3) share any subsequent books under the same or a similar license.

Acknowledgements

I would like to thank the following individuals for their contributions to the book:

- **Royce Kimmons** for making this OER book design platform available and providing ongoing support throughout the design process.
- **Sara Henry** (founder of [Heartful Editor](#)) for providing extensive and exceptional copyediting.
- **Matthew Checrallah** for assisting with the building of the book on the edtechbooks platform.
- **Rachelle Dene Poth & Jennifer Stadtmiller** for serving as subject matter experts

Teaching with Digital Tools and Apps

for the Finding Digital Tools & Apps chapter.

- **Susan Poyo & Sam Fecich** for serving as subject matter experts for the Evaluating the Learning Experience chapter.
- **Jennifer Courduff & Luis Perez** for serving as subject matter experts for the Evaluating Accessibility chapter.
- **Toni Hoehn, Amy Fowler, & Lois Paul** for serving as subject matter experts for the Evaluating Privacy, Cost, and Data chapter.
- **Jeff Zilch & Meagan Bubulka** for serving as subject matter experts for the Teaching with Digital Tools & Apps chapter.
- **Dennis McElroy & Peter Hessling** for serving as subject matter experts for the Finding Digital Tools & Apps chapter.
- **Marisa Catalina Casey** for sharing her photos of the book authors (pictured above).

Evaluating Cost, Privacy, and Data

By: Matthew Checrallah, Caroline Sonnett, and Jacob Desgres

In today's advanced technological landscape, can you really have privacy? Do you currently have a GPS, a smartphone or tablet, or apps that track your location? Do you have an artificial intelligence (AI) device, like SIRI, Alexa, or Cortana, that records what you say? Have you ever had your password stolen or your personal information hacked from a site that you joined? Have you ever signed up for a tool or downloaded an app without reading the terms of service or privacy policy?

In this chapter, we will explore how educational technology (edtech) tools are constantly collecting, using, and sharing personal information, what this means for you as an educator, and how you can better protect your students.

The Underlying Costs of Free Tools

Although free edtech tools and applications (apps) can be used to enrich, and even transform, teaching and learning, it is important to remember the old adage, "If something seems too good to be true, it probably is." This is not to say free edtech tools have no place in the classroom, but it is important to understand the true cost behind employing such technology when it is presented as being "free." To get started, watch the following video [Adam Ruins Everything - The Terrifying Cost of "Free" Websites](#):



Watch on YouTube <https://edtechbooks.org/-ovcW>

Apps and digital tools targeted to teachers as “free” often come with underlying costs. Many tools used in the classroom, such as Canva, a graphic illustrator tool, or Wakelet, a digital curation app, require you to register for an account to use the tool. When you register for an account, you are usually asked to share **personally identifiable information**, like your name, email address, age, and/or gender. You will also be asked to review and accept the **end-user license agreement** or **terms of service**, which may involve giving away even more data, such as your IP address, device information, browser information, geolocation, and Internet browsing data.

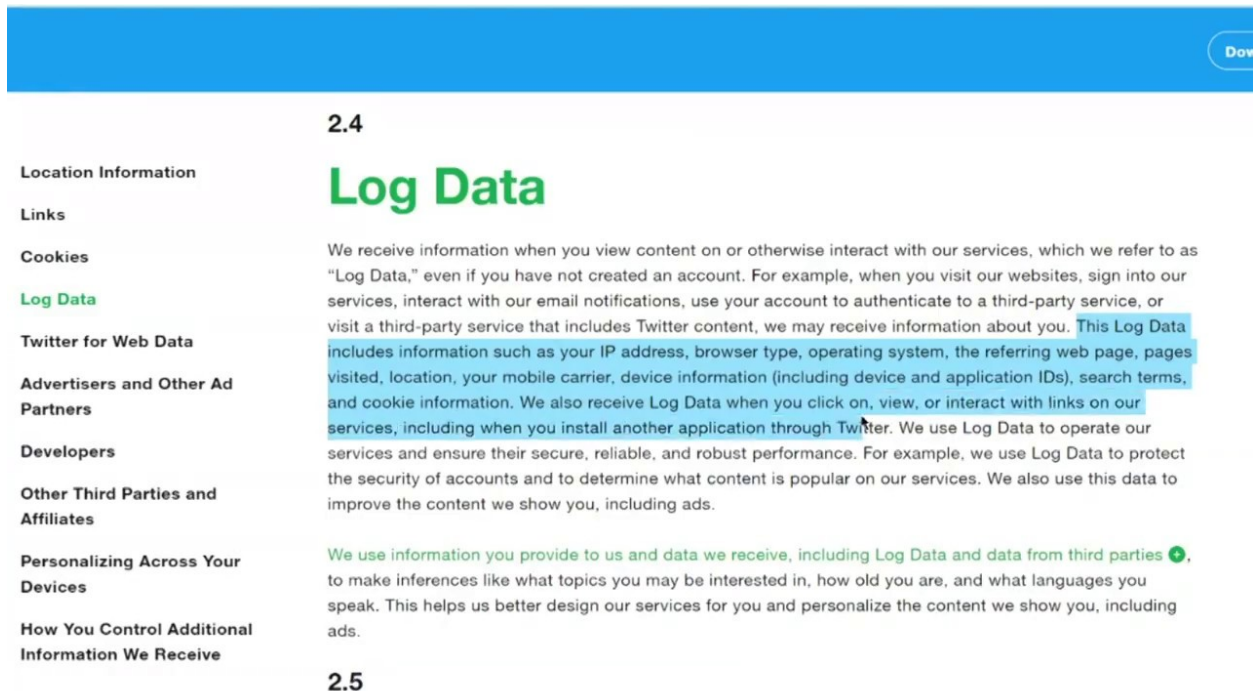
Some tools allow you to use a **single sign on** from third party companies, such as Google or Facebook, to create an account, which gives the tool partial or full access to the data from these third party companies. This can be especially problematic when you ask students to use their school gmail account to login to a tool, as that tool may gain access to private information from the students’ gmail accounts. For example, when the augmented reality game Pokemon Go first launched in 2016, the only way to create an account was through Google single sign on. However, this process granted the app “**full access to your Google account**.” That means the developer of Pokemon Go, Niantic, may have access to your emails, Google Drive, calendar, contacts, photos, Chrome browsing history, search history, Maps data... and, well, anything else linked to your Google account” (Cipriani, 2016, para. 3). As educators, it is important to understand that asking students to use apps or digital tools for learning activities **gives companies the opportunity to collect data on them**.

Companies use the data they collect in a variety of ways, including tailoring advertisements

Teaching with Digital Tools and Apps

(ads) to you, marketing, developing or improving services offered within the app, and sharing or selling the data to third-party companies. Take a look at the [Snapchat Privacy Policy](#) (2019), for example, and you'll see that Snapchat is collecting a significant amount of data, including usage, content, device, and location information, and using that data to "Develop, operate, improve, deliver, maintain, and protect our products and services," "personalize our services," and "provide and improve our advertising services, ad targeting, and ad measurement" (para. 20). Additionally, the privacy policy indicates that **Snapchat may share your data** with other Snapchatters, business partners, the general public, affiliates, and third parties.

Similar to Snapchat, Twitter collects, uses, and shares a significant amount of data from users. Take a look at [Kaputnickstudios' overview of the Twitter Privacy Policy](#) and you'll see that Twitter even collects and analyzes "private" direct messages with other users.



The screenshot shows a privacy policy page with a blue header. On the right side of the header, there is a button labeled "Down". The page is divided into two main sections. The first section is titled "2.4 Log Data" in green. To the left of this section is a vertical list of menu items: "Location Information", "Links", "Cookies", "Log Data" (highlighted in green), "Twitter for Web Data", "Advertisers and Other Ad Partners", "Developers", "Other Third Parties and Affiliates", "Personalizing Across Your Devices", and "How You Control Additional Information We Receive". The main text of section 2.4 explains that "Log Data" is collected when users interact with services, even if they are not logged in. It lists various types of data collected, such as IP address, browser type, operating system, and search terms. The second section is titled "2.5" and begins with the text: "We use information you provide to us and data we receive, including Log Data and data from third parties" followed by a small green icon.

Watch on YouTube <https://edtechbooks.org/-mty>

Ultimately, companies use the information and data they collect from you **to make money**, whether through advertisements, developing or improving services, or creating a profile with your data to sell to other companies. So, while it may be free to register and use a digital tool or app, you are paying for it by sharing your data and giving up your privacy. Even if you as an individual user may be okay with sharing your data for "free" tools, when you assign a tool to students you are asking them to share their data, whether they want to

or not.

Additional Resources to Explore

- [2018 State of Edtech Privacy Report](#)
- [Educator Toolkit for Teacher and Student Privacy](#)

Data Collection & Privacy

Privacy is the “freedom from unauthorized intrusion” ([Merriam-Webster, 2020](#), para 2). The **right to privacy** means “a person has the right to determine what sort of information about them is collected and how that information is used” ([Sharp, 2013](#), para. 14). Yet, in today’s digital age, apps, websites, and online tools are collecting, using, and sharing private personal data to make money. The companies that make these digital tools and apps get away with infringing on peoples’ right to privacy by using confusing legal jargon, obscure terms, and abstract statements in their privacy policies ([Moretti & Naughton, 2014](#)). According to Moretti and Naughton, “Taken together, the way America’s most popular websites write their privacy policies makes it almost **impossible in practice for people to be fully informed** about their Internet use and how their data is collected” (para. 13).

Similarly, end-user license agreements (EULA) and terms of service (TOS) agreements feature opaque language that may cause you to give away your right to privacy without truly understanding what you are doing when you click “I agree.” A EULA or TOS is a contract with which you have to agree to use an app, tool, or website. You may come across one when downloading an app, opening an app for the first time, reinstalling or updating an app, registering to use a digital tool, or at the bottom of a webpage. The methods used to ask for user consent differ, as there is no national standard for how to acquire consent. It can either be attained in “browsewrap” where you never click any “I Agree” buttons, but there is text on the screen that states, “By using this site, you agree to our Terms of Service.” In a clickwrap form, the site will prevent you from entering until you check the “I Agree” button. Browsewrap may not be as intrusive, but they may still be capturing data from the user (Pegarella, 2016).

It is common practice to give consent (“I Agree”) without reading the EULA, TOS, or privacy policy. However, this can have negative consequences for you and your students’ privacy. Reading through the EULA or TOS and privacy policy is always good practice and can raise **red flags**, like Snapchat - here is a statement from their [Terms of Service](#) (2019):


When you appear in, create, upload, post, or send Public Content, you also grant Snap Inc., our affiliates, and our business partners the **unrestricted**, worldwide, **perpetual right** and license to use your name, likeness, and voice, including in connection with






Teaching with Digital Tools and Apps

commercial or sponsored content.


This kind of blank check usage of your data is not unusual for agreements and should be a warning sign for you as an educator when examining how the use of a tool might affect your students' privacy.






Terms of Service; Didn't Read Ratings About Follow us @tosdr Donate: [On OpenCollective](#)

 **Google** Class C


-  This service may collect, use, and share location data
-  The service can read your private messages
-  You agree to defend, indemnify, and hold the service harmless in case of a claim related to your use of the service
-  This service tracks you on other websites
-  Limited copyright license to operate and improve all Google Services






[More details](#)

 **YouTube** Class D


-  Terms may be changed any time at their discretion, without notice to the user
-  Processes a personal information (email, id but also device info, location)
-  Users should revisit the terms periodically, although in case of material changes, the service will notify
-  If you are the target of a copyright claim, your content may be removed
-  The service is not responsible for linked or (clearly) quoted content from third-party content providers






[More details](#)

 **Amazon** Class C

-  Terms may be changed any time at their discretion, without notice to the user
-  The service can delete your account without prior notice and without a reason
-  This service tracks you on other websites
-  This service forces users into binding arbitration in the case of disputes
-  Blocking cookies may limit your ability to use the service

[More details](#)

 **twitter** Class D

-  Very broad copyright license on your content
-  Third party cookies
-  This service ignores the Do Not Track (DNT) header and tracks users anyway even if they set this header.
-  The service can delete your account without prior notice and without a reason
-  This service reserves the right to disclose your personal information without notifying you

[More details](#)

The Terms of Service; Didn't Read Extension/Add-On allows you to quickly assess a digital tool or website before using it (<https://tosdr.org/index.html>)

Before you download or use another app or digital tool:

1. Read the Terms of Service or End-User License Agreement

- What rights are you granting the company?
- How might the company infringe on your privacy? (e.g., [Snapchat TOS](#) states: "While we're not required to do so, we may access, review, screen, and delete your content at any time and for any reason")

2. Read the privacy policy

Teaching with Digital Tools and Apps

- What data are collected? Take a look at [UMass Amherst's Data Classification categories](#) to help you evaluate the type of data collected by the app or tool (e.g., restricted, confidential, operational use only, or unclassified).
- How are data used?
- How are data shared?
- How does the company ensure the security of your data?
- What happens if there is a data breach and your data is stolen?

3. Follow the money

- How does the company make money?
- Does the company buy your data from third-party companies to improve its own services and ads?
- Does the company sell your data to others?

4. Examine the purpose

- To whom is the digital tool or app catered?
- Does the tool or company have a specific goal?

5. Check with your district tech/IT support professionals

- Does your school or district have a contract with the tool or app that protects student data and privacy (see [K-12 School Service Provider Pledge to Safeguard Student Privacy](#))?
- Or, if you ask students to use single sign on their their school email accounts, will that protect students when they use the tool or put their educational records at risk?
- If not, would your school or district tech/IT support professionals be willing to review the privacy policy/TOS of the edtech tool and let you know whether/how you should use the tool in your classroom?

6. Look for alternatives

- Is there another tool/app that will do the same job that is more protective of your students' privacy? For example, [Pencil Code](#), a coding tool, does not collect or allow the sharing of any personally identifiable information. Tools funded by external sources (e.g., grants) may not collect personally identifiable data because they are not expecting a return on investment.

7. Ask the Company to Protect Your Students' Personal Information

- "Thanks to a California law that went into effect in January 2020, you and your family have new rights to protect your personal information if you are California residents" (Common Sense, 2020, para. 1). Learn more: <https://edtechbooks.org/-TPCd>

Educator's Guide to Student Data Privacy

In the [Educator's Guide to Student Data Privacy](#) by ConnectSafely you will find a list of questions to help you quickly evaluate an edtech tool for student privacy.

As an educator, it is important to know what type of data will be collected when using an educational app, digital tool, or AI device (e.g, Amazon Echo) in your classroom. It is equally important to understand the privacy concerns that exist as a result of that data being used and/or shared. In a [New York Times](#) interactive feature, "[Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret](#)," Valentino-DeVries, Singer, Keller, and Krolik (2018) described how a math teacher with multiple **location-tracking apps on her phone had her location recorded more than 8,600 times in fourth months**, including when she was in school, how long she was at her dermatologist's office, and when she went to a Weight Watchers meeting.

It seems like nowadays most apps, websites, and digital tools ask for permission to use your location, whether it's to locate the closest store for you, track your running or biking route, or to provide local news or weather alerts. However, what you may not realize is that the **geolocation data collected about you is often shared or sold to other companies**. For instance, Valentino-DeVries and colleagues described how a sports app that used location data to identify local sports teams, "passed precise [user location] coordinates to 16 advertising and location companies" (para. 37). App developers "make money by directly selling their data, or by sharing it for location-based ads, which command a premium. Location data companies pay half a cent to two cents per user per month" (Valentino-DeVries et al., para. 50).

Many users give apps permission to use their location with the understanding the data will be anonymized. However, Paul Ohm, a law professor and privacy researcher at the Georgetown University Law Center, noted that "really precise, longitudinal geolocation information is absolutely impossible to anonymize" (as cited in [One Nation, Tracked](#) by Thompson & Warzel, 2019). And, while individual apps may indicate that they anonymize your data, they often send the data to the same location data companies that curate the data into large databases. When these companies receive multiple pieces of information from the various apps installed on your device, it is easy to connect the dots of your habits and routines. Should this data get breached or used in the wrong way (e.g., monitoring who attended a protest), **imagine the impact it might have on your own life or your students' rights and freedom**.

ONE NATION, TRACKED

An Investigation into the Smartphone Tracking Industry from Times Opinion

“It originated from a location data company, one of dozens quietly collecting precise movements using software slipped onto mobile phone apps. You’ve probably never heard of most of the companies — and yet to anyone who has access to this data, your life is an open book. They can see the places you go every moment of the day, whom you meet with or spend the night with, where you pray, whether you visit a methadone clinic, a psychiatrist’s office or a massage parlor” ([para. 7](#)).

Placed at the Scene of a Crime due to the use of a Location Tracking App

In the article, "[Google tracked his bike ride past a burglarized home. That made him a suspect.](#)" Zachary McCoy discusses how his use of the exercise tracking app, RunKeeper, to track his bike rides resulted in him being considered a suspect in a crime. When the local police obtained a geofence warrant ("a police surveillance tool that casts a virtual dragnet over crime scenes, sweeping up Google location data — drawn from users’ GPS, Bluetooth, Wi-Fi and cellular connections — from everyone nearby") it tied McCoy to the scene of a local robbery even though he had simply just been on a bike ride near the robbery at the same time (Schuppe, 2020, para. 9).

Student Data Collection and Use

Data are commonly collected about students through administrative management systems, tracking systems, and learning management systems. Systems like these collect personally identifiable information, such as names, addresses, dates of birth, grades, location, behavior, and/or attendance. School-assigned devices, such as laptops or tablets, as well as school wifi, can potentially collect additional data, including location, device usage data, browsing history, and communications with other students. Data collection can be beneficial in schools because it gives educators the ability to tailor educational programming to the specific needs of students and reduce negative outcomes, like dropout numbers and

Teaching with Digital Tools and Apps

cyberbullying.

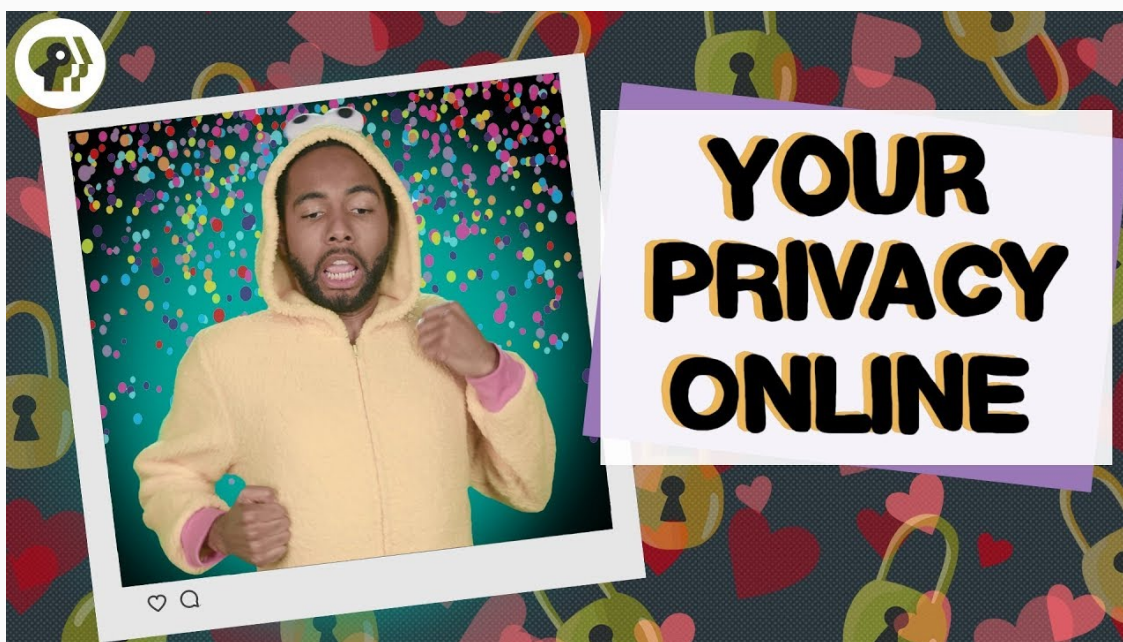
However, there is a tradeoff when collecting information on students. With more data collected on students than ever before, educators can track the progress of students, design personalized learning experiences, and project where students may encounter difficulty in schools. However, this same data could be **misinterpreted, perpetuate stereotypes** about certain student profiles, and even be used to limit opportunities for students in the future ([Educator Toolkit for Teacher and Student Privacy, 2018](#)). Even worse, when algorithms are used to analyze student datasets, it is “even more likely that they will **reinforce the education system’s existing biases** rather than radically upend them” (Watters, 2017, para. 39). Ultimately, the data collected on students could actually **negatively impact student learning** - the opposite of the intended purpose.

The sensitive data collected on students, whether from management systems, school devices, or classroom apps/tools, can put students in a **vulnerable position** if the data collected are not adequately protected. For instance, in 2017, a hacker group called “The Dark Overlord” engaged in ransomware attacks on student systems and gained access to personal information of many students. With this information, they sent threatening texts to students until demands were met ([Educator Toolkit for Teacher and Student Privacy, 2018](#), p. 2). Cyber attacks on schools tripled in 2019 (Klein, 2020). According to Klein, “Schools were most likely to experience data breaches and other unauthorized disclosures” (para. 4). Additionally, hackers stole user data and passwords from more than 77 million teachers, students, and parents/guardians who were using Edmodo ([Cluley, 2017](#)).

When using data collection systems and edtech tools, educators and administrators should carefully examine the EULA/TOS and privacy policy to identify what information might be collected, used, shared, sold, or stolen and how that information is protected from misuse or data breaches.

Data Protection

If you are concerned about a data breach, the loss of your (or your students') data, or the sharing of your (or your students') information without permission, watch the Above the Noise's [5 Tips to Protect Your Privacy Online](#) video. This video discusses threat modeling, passwords, online tracking, surveillance at schools, encryption, and open wifi networks.



Watch on YouTube <https://edtechbooks.org/-NFob>

Laws About Privacy and Data

There are a number of laws in place to protect students' privacy. If you, or your school district, were to use a digital tool, website, or app that violates one of these laws, it can cause serious legal trouble. Similarly, if companies violate these laws, they too must face the consequences. For instance, Google and YouTube had to pay a \$170 million fine for illegally collecting, using, and sharing personal information from children under 13 years old without their consent, violating the Children's Online Privacy Protection Act ([FTC, 2019](#)). In the following section, we will detail some of the most important laws to keep in mind when evaluating the privacy, cost, and data use of apps and online sites/tools.

The Family Educational Rights and Privacy Act

The [Family Educational Rights and Privacy Act](#) (FERPA), passed in 1974 and last updated in 1992, **protects a student's personal information and educational records from unauthorized disclosure**. This law gives students "access to their education records, an opportunity to seek to have the records amended, and some control over the disclosure of information from the records " ([Drake, 2014](#), para. 12). Educators and administrators must have the consent of the student and their guardian (if they are under 18 years old) before they can share student information or records.

Returning to the Pokemon Go example earlier in this chapter, this could have been a potential FERPA violation since Niantic was given full access to students' school Google accounts through the single sign on process. While Niantic was quick to change what data they collected from Google to provide more protections to users, you can't assume companies have the users' best interests or right to privacy in mind when you ask students to register or sign in to a tool or app.

FERPA can also potentially be violated when requiring students to use social media for a class assignment. You must ensure that students' personal information and education records are protected from the public. For example, don't require them to post on Twitter with their actual name using a school hashtag, instead allow them to use a pseudonym and then submit screenshots of their tweets to you for assessment. You also shouldn't ever post information related to students' grades, course enrollments, classes, or other educational records on social media (i.e., don't post a student's grade directly on their public blog) (for more information, read [Is Your Use of Social Media FERPA Compliant?](#)).

The Children's Online Privacy Protection Act (COPPA)

The [Children's Online Privacy Protection Act](#) (COPPA, 1998) was created to **regulate technology companies' collection and use of data from children under the age of 13**. According to the [Federal Trade Commission](#) (2015), "The primary goal of COPPA is to place parents in control over what information is collected from their young children online" (para. 4). Under COPPA, website operators, online services, and app developers need to:

- Post a detailed privacy policy that indicates how personal information is collected online from kids under 13;
- Giving parents direct notice and obtain consent before collecting information from their children;
- Give parents the option of consenting to the companies' collection and use of information about their children;
- Prevent the disclosure of information collected from children to third-party companies (unless it's necessary for the site or service; in this case it has to be made clear to parents);
- Allow parents to review the information collected about their children, request the

Teaching with Digital Tools and Apps

- data be deleted, and opt out of future collection; and
- Keep the information secure and delete it once it is no longer necessary.

Schools can provide consent for the parent when sites, services, tools, or apps are used for educational purposes only and the personal information collected about students is not used for commercial purposes.

Before you introduce an app, online site, or tool into your classroom, do a quick Internet search for the name of the app/site/tool + “COPPA” to see if it has a COPPA policy in place or adheres to COPPA. While most edtech tools are not COPPA compliant (e.g., [Thousands of apps in Google Play Store may be illegally tracking children, study finds](#)), some educational tools are starting to indicate their compliance with COPPA in their privacy policies or EULA/TOS or on their website. Some edtech companies make it clear and easy to understand their COPPA compliance (e.g., [Pencil Code Privacy Policy](#)), however, others are less transparent or put the responsibility on the educator or school to adhere to COPPA (e.g., [Adobe & Student Privacy](#), [Lucidchart](#), [Flipgrid Privacy Policy](#)).

Children’s Internet Protection Act

The [Children’s Internet Protection Act](#) (CIPA), passed in 2000, **protects children from obscene or harmful content on the Internet**. CIPA is the reason sites like YouTube, social media, and even Internet searches may be blocked or filtered in schools. Schools and libraries that are part of the [E-rate program](#) (discounted telecommunications and Internet access) must comply with CIPA. According to the Federal Communications Commission (2019), schools and libraries subject to CIPA must create and adhere to an Internet safety policy addressing how they:

- Restrict students from accessing obscene or harmful information/materials and child pornography;
- Ensure the safety and security of minors when they engage in digital communications (email, chat rooms);
- Prevent unauthorized disclosure of students’ personal information;
- Prevent minors from engaging in illegal behaviors, such as hacking.

CIPA may impact whether you can use certain digital tools, websites, and apps. For instance, you might want to show a YouTube video in class, only to find out that YouTube is banned on the school network. Or, you might ask your students to search for an image, but Google image search is blocked. Thus, when evaluating a digital tool, online resource, or app, you should test whether it can be used on the school network. You may also want to explore whether the tool violates CIPA. For example, even though [Pixabay](#) (a website featuring high quality free stock photos) has a SafeSearch feature, the website states that the SafeSearch filter isn’t 100% accurate. Also, viewing adult content on Pixabay is easily done with the click of a button. While Pixabay may not be banned by your school administrators or IT staff, the use of it in your classroom could potentially violate CIPA.

State Laws on Privacy

Be sure to familiarize yourself with your state's laws on privacy. Many new state privacy laws have been passed since 2014, including the Student Online Personal Information Protection Act (SOPIPA) and the [California Consumer Privacy Act \(CCPA\)](#).

Explore the [Privacy Bills by State Chart](#) from the Parent Coalition for Student Privacy.

Conclusion

Before you introduce a new tool, online resource, or app into your classroom, start by reading the end-user license agreement/terms of service and privacy policy (don't just click "I Agree" without actually reading the terms!). Knowing what personal rights and private data you have to give up to use a new tool or app in your classroom can help you weigh the pros and cons of whether the new technology is actually worth it. It will also help you protect your own and your students' privacy.

In this chapter, we discussed the underlying costs of using "free" tools, how to assess edtech tools to protect student privacy, and federal and state privacy laws that impact the use of edtech tools in classrooms and school. The goal of this chapter was to provide a brief overview of student privacy, data, and the cost of tools. We hope that you continue to build your knowledge of this topic by exploring resources and keeping up to date on the latest changes in privacy laws.

References

Above the Noise. (2017, November 15). 5 tips to protect your privacy online [Video]. YouTube. Retrieved from <https://edtechbooks.org/-Hrj>

American Bar Association. (n.d.). Customer information and privacy. Retrieved from <https://edtechbooks.org/-VhbS>

Cambridge Public Schools. (2019). Student data privacy. Retrieved from <https://edtechbooks.org/-iEp>

Cipriani, J. (2016, July 12). Pokemon Go can see everything in your Google account. Here's

Teaching with Digital Tools and Apps

how to stop it. CNET. Retrieved from <https://edtechbooks.org/-Mzq>

Common Sense. (2020). Ask companies not to sell your data. Retrieved from <https://edtechbooks.org/-kDrd>

Farrar, L. (2018, March 13). Protecting students' online privacy in the classroom. KQED Education. Retrieved from <https://edtechbooks.org/-FdBN>

Federal Communications Commission. (2019, June 10). E-rate: Universal service program for schools and libraries. Retrieved from <https://edtechbooks.org/-Ydouniversal-service-program-schools-and-libraries-e-rate>

Federal Communications Commission. (2019, June 12). Children's Internet Protection Act (CIPA). Retrieved from <https://edtechbooks.org/-xvy>

Gallagher, K., Magid, L., & Pruitt, K. (2019). The educator's guide to student data privacy. Connect Safely. Retrieved from <https://edtechbooks.org/-yLQv>

Ghoshal, A. (2018, December 11). Those free apps on your phone are selling your location data [Web log post]. The Next Web. Retrieved from <https://edtechbooks.org/-sqQr>

Gussis, G. G. (2018). Software license agreements checklist. Retrieved from <https://edtechbooks.org/-prk/>

Klein, A. (2020). Cyber attacks on schools tripled in 2019, report finds. Education Week. Retrieved from <https://edtechbooks.org/-AdB>

Mamaysky, I. (2019, October 8). The FTC has its sights on COPPA, and edtech providers should take notice. EdSurge. Retrieved from <https://edtechbooks.org/-qvD>

McDowell, M. (2019, September 27). Reviewing end-user license agreements: CISA. Retrieved from the Cybersecurity and Infrastructure Security Agency website: <https://edtechbooks.org/-jAk>

Parent Coalition for Student Privacy & Badass Teachers Association. (2019, October). Educator toolkit for teacher and student privacy. Retrieved from the Access 4 Learning Community website: https://www.a4l.org/resource/resmgr/files/sdpc-publicdocs/PCSP_BATS-Educator-Toolkit.pdf

Pegarella, S. (2016, October 23). Examples of user agreements. TermsFeed. Retrieved from <https://edtechbooks.org/-LaLV>

Privacy. In The Merriam-Webster.com Dictionary. Retrieved January 28, 2020, from <https://edtechbooks.org/-ypn>

UMass Amherst. (2020). Data classification at UMass Amherst. Retrieved from

Teaching with Digital Tools and Apps

<https://edtechbooks.org/-wKSi>

U.S. Department of Education. (2018, March 1). Family Educational Rights and Privacy Act (FERPA). Retrieved from <https://edtechbooks.org/-hSCi>

Valentino-Devries, J., Singer, N., Keller, M. H., & Krolik, A. (2018, December 10). Your apps know where you were last night, and they're not keeping it secret. The New York Times. Retrieved from <https://edtechbooks.org/-hPNd>

Book Author Information

Torrey Trust



Torrey Trust, Ph.D. is an Associate Professor of Learning Technology in the Department of Teacher Education and Curriculum Studies in the College of Education at the University of Massachusetts Amherst, where she is the co-coordinator of the [Learning, Media and Technology master's degree program](https://www.umass.edu/education/programs/stem/masters) [https://www.umass.edu/education/programs/stem/masters]. Her research, teaching, and leadership/service focus on how technology can support teachers in designing contexts that enhance student learning. Specifically, Dr. Trust studies educators' professional growth through digitally-enhanced professional learning networks (PLNs), the influence of social media on teaching and learning, how makerspaces and 3D printing facilitate new learning experiences, and the design and use of open educational resources in college and graduate level courses.

www.torreytrust.com [http://www.torreytrust.com]



Trust, T. (2020). *Teaching with Digital Tools and Apps* (1st ed.). EdTech Books.
Retrieved from <https://edtechbooks.org/digitaltoolsapps>



CC BY-NC-SA: This book is released under a CC BY-NC-SA license, which means that you are free to do with it as you please as long as you (1) properly attribute it, (2) do not use it for commercial gain, and (3) share any subsequent books under the same or a similar license.

