Evaluating Cost, Privacy, and Data

Matthew Checrallah, Caroline Sonnett, & Jacob Desgres

Hypothes.is Social Annotation

This chapter is annotated every year as part of an undergraduate/graduate class on Teaching and Learning with Technology. To turn off the highlighted text, click on the "eye" icon in the top right corner of the browser screen.

Introduction

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? Have you ever signed up for an online course (e.g., Coursera, WGU, Udacity) without realizing they are tracking and sharing your data, including recording your mouse and keystrokes?

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 Markup: This Private Equity Firm Is Amassing Companies That Collect Data on America's Children

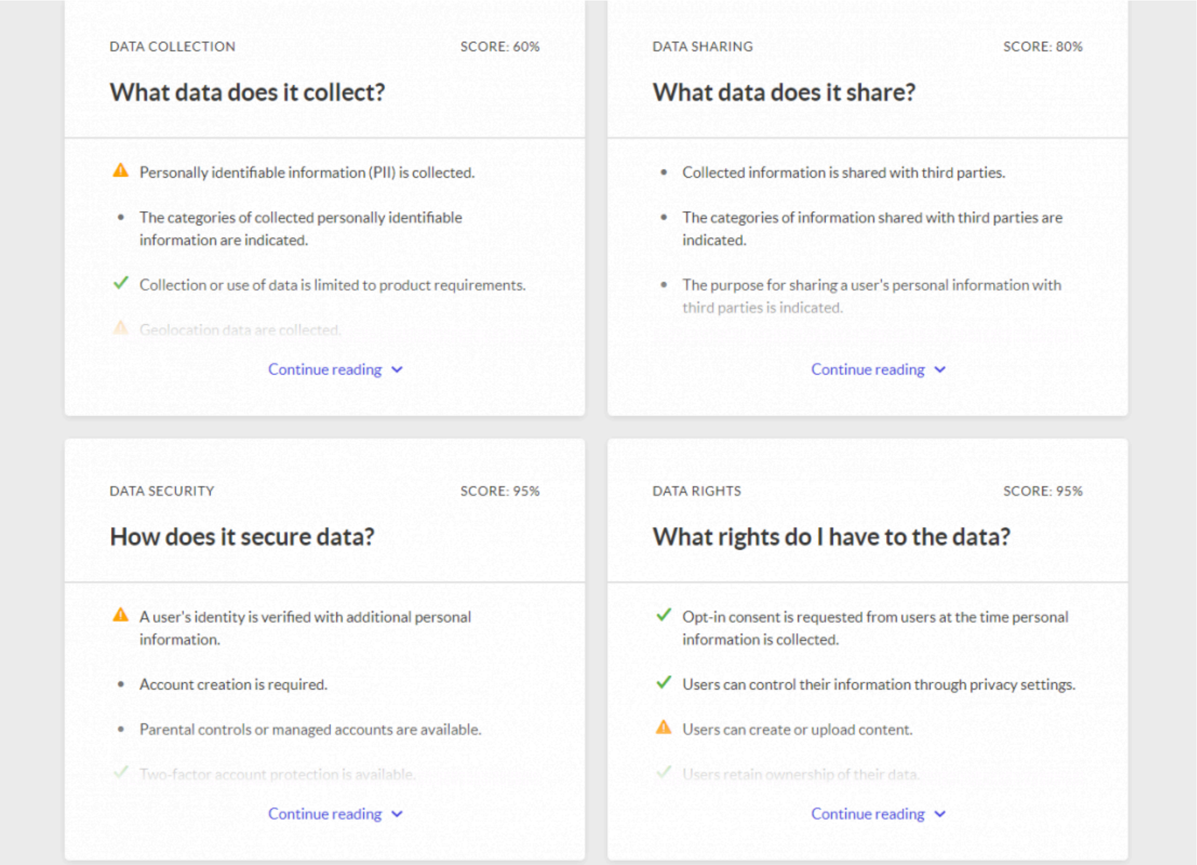
"We found that the companies, collectively, gather everything from basic demographic information—entered automatically when a student enrolls in school—to data about students' citizenship status, religious affiliation, school disciplinary records, medical diagnoses, what speed they read and type at, the full text of answers they give on tests, the pictures they draw for assignments, whether they live in a two-parent household, whether they've used drugs, been the victim of a crime, or expressed interest in LGBTQ+ groups, among hundreds of other data points" (Feathers, 2022, para. 11).

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

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.



DATA COLLECTION SCORE: 60%

What data does it collect?

⚠ Personally identifiable information (PII) is collected.

• The categories of collected personally identifiable information are indicated.

✓ Collection or use of data is limited to product requirements.

⚠ Geolocation data are collected.

Continue reading

DATA SHARING SCORE: 80%

What data does it share?

• Collected information is shared with third parties.

• The categories of information shared with third parties are indicated.

• The purpose for sharing a user's personal information with third parties is indicated.

Continue reading

DATA SECURITY SCORE: 95%

How does it secure data?

⚠ A user's identity is verified with additional personal information.

• Account creation is required.

• Parental controls or managed accounts are available.

✓ Two-factor account protection is available.

Continue reading

DATA RIGHTS SCORE: 95%

What rights do I have to the data?

✓ Opt-in consent is requested from users at the time personal information is collected.

✓ Users can control their information through privacy settings.

⚠ Users can create or upload content.

✓ Users retain ownership of their data.

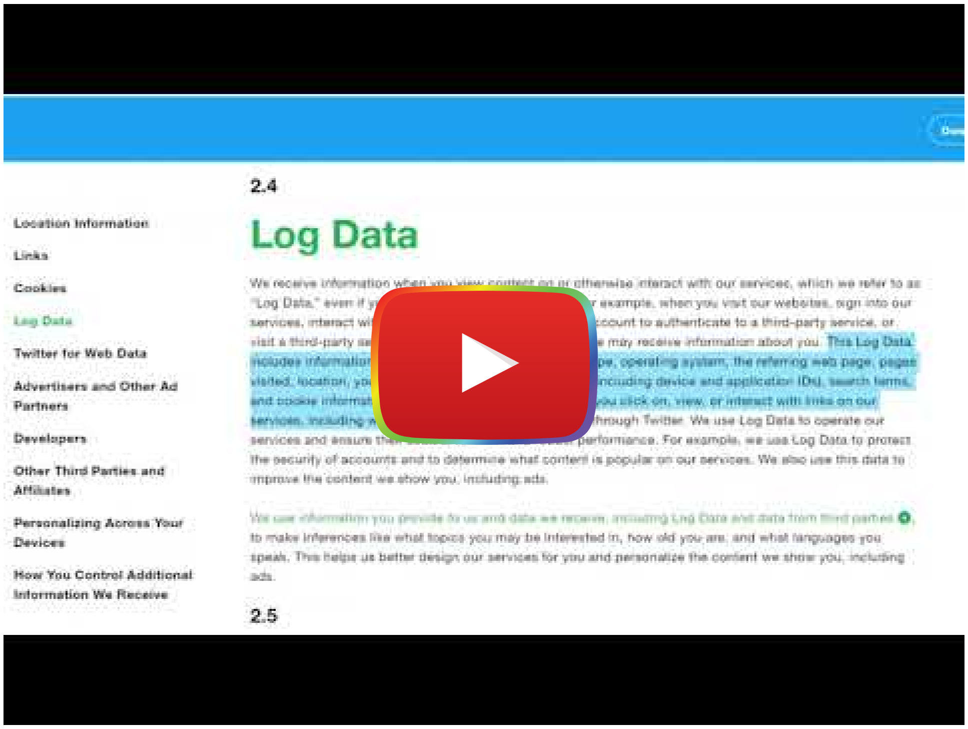
Continue reading

The Common Sense Media organization created an evaluation tool to help you assess the privacy of digital tools and apps, including what data is collected and shared, how data is secured, and what data rights you have. Learn more here: Common Sense Privacy Program.

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 problematic when the third-party company gives away too much information. 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 (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 the Twitter Privacy Policy Overview video embedded below and you'll discover that Twitter even collects and analyzes "private" direct messages with other users.



Location Information

Links

Cookies

Log Data

Twitter for Web Data

Advertisers and Other Ad Partners

Developers

Other Third Parties and Affiliates

Personalizing Across Your Devices

How You Control Additional Information We Receive

2.4

Log Data

We receive information when you view content on or otherwise interact with our services, which we refer to as
"Log Data," even if y
r example, when you visit our websites, sign into our
services, interact wi
ccount to authenticate to a third-party service, or
visit a third-party se
e may receive information about you. This Log Data
includes information
pe, operating system, the referring web page, pages
visited, location, yo
ncluding device and application IDs, search terms,
and cookie informat
you click on, view, or interact with links on our
services, including w
hrough Twitter. We use Log Data to operate our
services and ensure the
performance. For example, we use Log Data to protect
the security of accounts and to determine what content is popular on our services. We also use this data to improve the content we show you, including ads.

We use information you provide to us and data we receive, including Log Data and data from third parties, to make inferences like what topics you may be interested in, how old you are, and what languages you speak. This helps us better design our services for you and personalize the content we show you, including ads.

2.5

Watch on YouTube

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.

How do you feel about giving up your data and privacy? Try out the Technoethics DigCiz tool "**Data, Privacy, and Identity Drag and Drop Cards**."

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

- Common Sense Privacy Evaluations
- Student Privacy Training for Educators
- 2018 State of Edtech Privacy Report
- Educator Toolkit for Teacher and Student Privacy
- Schools Do Not Have to Sacrifice Students' Privacy to Continue Schooling
- A Security Checklist for School-Provided Technology
- Protecting Student Privacy (U.S. Department of Education)

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).

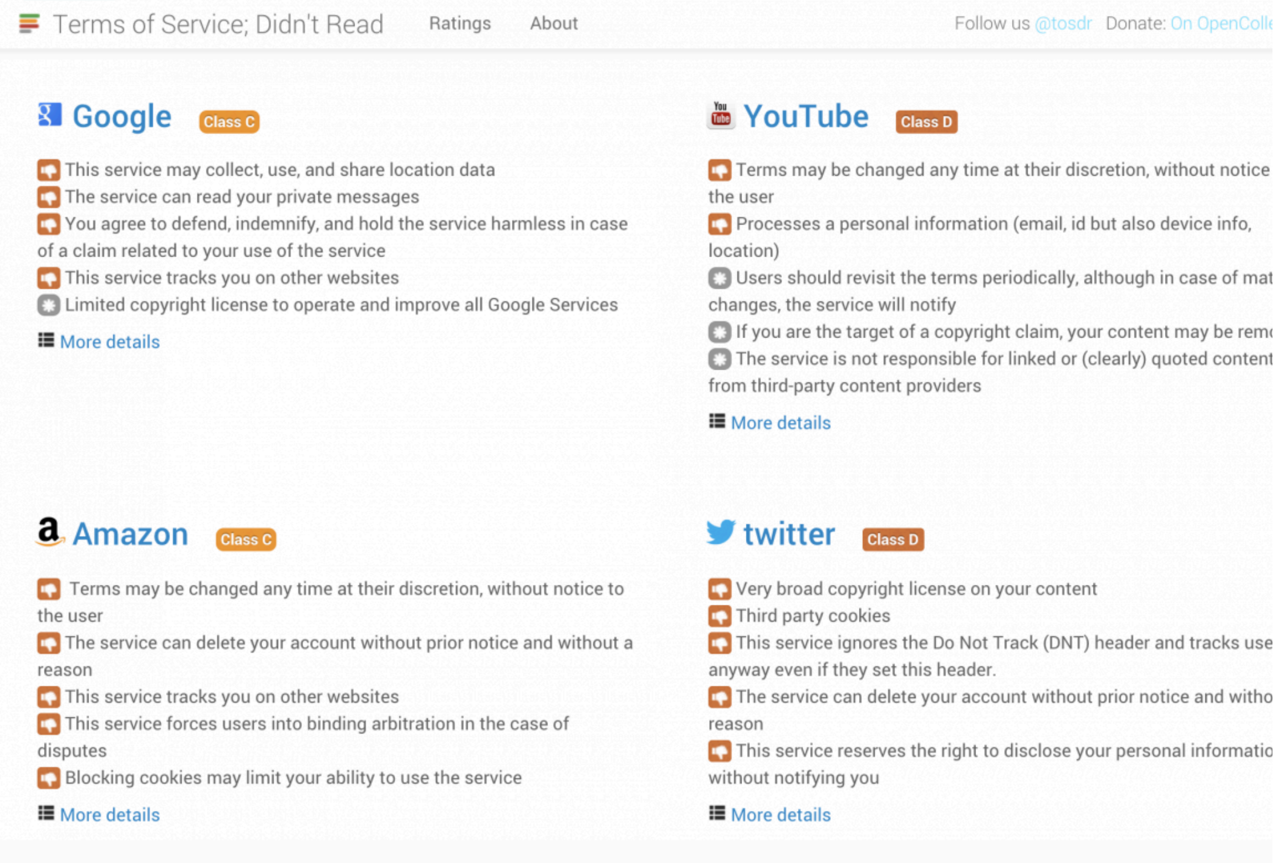
Visualizing Terms of Service

According to LePan (2020), "Even the shortest terms and conditions for popular online services are a few thousand words long. 97% of people in the 18-34 age group agree to conditions without reading them" (para. 1). LePan's article features an **infographic displaying the length of each TOS for 14 popular apps**, with Instagram at the shortest read time of 9 minutes and 42 seconds and Microsoft's TOS at more than an hour of read time (15,260 words).

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 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 OpenColle

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 the user
- Processes a personal information (email, id but also device info, location)
- Users should revisit the terms periodically, although in case of mat changes, the service will notify
- If you are the target of a copyright claim, your content may be rem
- 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 use anyway even if they set this header.
- The service can delete your account without prior notice and witho reason
- This service reserves the right to disclose your personal informatio 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)

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**
   - Start by watching "How to read privacy policies like a lawyer"
   - 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?

The Markup: What Does It Actually Mean When a Company Says, 'We Do Not Sell Your Data'?

"The next time you look at a privacy policy, which few people ever really do, don't just focus on whether or not the company says it sells your data. That's not necessarily the best way to assess how your information is traveling and being used. And even if a privacy policy says that it doesn't share private information beyond company walls, the data collected can still be used for purposes you might feel uncomfortable with, like training internal algorithms and machine learning models. (See Facebook's use of one billion pictures from Instagram, which it owns, to improve its image recognition capability.) Consumers should look for deletion and retention policies instead" (Ng, 2021, para. 38-40).

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://www.donotsell.org/

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.

The Washington Post: Remote learning apps shared children’s data at a ‘dizzying scale’

"School districts and public authorities that had recommended the tools, Han wrote, had 'offloaded the true costs of providing education online onto children, who were forced to **pay for their learning with their fundamental rights to privacy**.'" (Harwell, 2022, para. 17).

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 four 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**.

The New York Times: 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” (Thompson & Warzel, 2019, para. 7).

Placed at the Scene of a Crime due to 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).

The Markup: Your Location Is a Universal Identifier

"We wanted to develop a statistical approach to quantify what it would take, on average, to identify someone from an anonymous location dataset, and we were able to show that **four data points of approximate place and time of where someone was was enough**, in a data set of 1.5 million people, to uniquely identify someone 95 percent of the time" (Angwin, 2022, para. 13).

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 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, be shared with local authorities and increase interactions between police and students from traditionally marginalized backgrounds, 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.

The74: Survey Reveals Extent that Cops Surveil Students Online — in School and at Home

"The tools, offered by a handful of tech companies, can sift through students’ social media posts, follow their digital movements in real-time and scan files on school-issued laptops — from classroom assignments to journal entries — in search of warning signs. Educators say the tools help them identify youth who are struggling and get them the mental health care they need at a time when youth depression and anxiety are spiraling. But the survey suggests an alternate reality: Instead of getting help, many **students are being punished** for breaking school rules. And in some cases, survey results suggest, **students are being subjected to discrimination**" (Keierleber, 2022, para. 44).

Education Week: Using Student Data to Identify Future Criminals: A Privacy Debacle

"Experts on data privacy and student security are calling for investigations and parents are expressing alarm after a news report last week revealed that a county police department in Florida uses sensitive data from the local school district to keep a secret list of middle and high school students it deems as potential future criminals" (Lieberman, 2020, para. 1).

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).

The New York Times: You’re Tracked Everywhere You Go Online. Use This Guide to Fight Back

"A lot of the tracking systems out there make it easier for law enforcement to gather data without warrants,” he said. “A lot of trackers sell data directly to law enforcement and to Immigrations and Customs Enforcement. I think the bottom line is that it’s creepy at best. It enables manipulative advertising and political messaging in ways that make it a lot easier for the messengers to be unaccountable. It enables discriminatory advertising without a lot of accountability, and in the worst cases it can put real people in real danger" (Bennett Cyphers as cited in Herrera, 2019, para. 15).

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.

Digital Tools & Apps That Focus on Privacy

While the extent to which data is collected, shared, sold, and used varies quite a bit from tool to tool, there are several tools that either do not collect a lot of information (to support users' privacy) or have privacy policies that are designed with students' privacy rights in mind. Here are a few examples*:

- **Code.org**
    - Common Sense Education Privacy Rating: 96%.
    - Online Tools for Teaching & Learning Site Evaluation: N/A.
    - Details: Collection or use of data is limited to product requirements.
- **Data Basic.io**
    - Common Sense Education Privacy Rating: N/A.
    - Online Tools for Teaching & Learning Site Evaluation: 5 Stars.
    - Details: "The Data Basic website stores information uploaded only for the amount of time it takes users to analyze the data, and then it deletes it. The aggregate results shown on the website (metadata) are kept for 60 days, and then are deleted."
- **Formative**
    - Common Sense Education Privacy Rating: 93%.
    - Online Tools for Teaching & Learning Site Evaluation: 5 Stars.
    - Details: Collection or use of data is limited to product requirements. Users can control how their data is displayed. Privacy policy states: "We strive to adhere to U.S. federal, certain state, and certain international regulations. This includes (but may not be limited to) FERPA, COPPA, GDPR, and California AB 1584."
- **Pencil Code**
    - Common Sense Education Privacy Rating: N/A.
    - Online Tools for Teaching & Learning Site Evaluation: 5 Stars.
    - Details: "Pencil Code does not collect personally identifiable information, and our Terms of Service expressly prohibit posting personally identifiable information."
- **PhET Simulations**
    - Common Sense Education Privacy Rating: 22% (this rating is for the University of Colorado's privacy policy and not the PhET simulations privacy settings).
    - Online Tools for Teaching & Learning Site Evaluation: 5 Stars.
    - Details: "In connection with your use of the PhET Simulations Android app, NO personally identifiable information is collected by the CU PhET team. The PhET Simulations Android app is meant to provide educational simulations to a wide audience. As we strive to collect the minimum amount of information needed to advance our educational mission, we have determined that there is no need for the collection of personal data within this app."
- **Remind**
    - Common Sense Education Privacy Rating: 94%
    - Online Tools for Teaching & Learning Site Evaluation: 5 Stars
    - Details: Abides by GDPR. Awarded the iKeepSafe COPPA Safe Harbor Seal.

This list is not meant to be an exhaustive list of digital tools and apps that seek to protect users' privacy. There are several tools that have recently changed their privacy policies to be more protective of users' privacy and to abide by privacy laws, such as the GDPR and CCPA. Therefore, it is important to continually (at least once a year) check the privacy policies of digital tools and apps that you use for teaching and learning for any changes or updates.

*This list was curated by Ana Paula Dornelles Schantz.

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

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 (FERPA)

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?).

Learn more about FERPA from the U.S. Department of Education: Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices.

Remote Learning Tip

If you record or take a screenshot of a class virtual meeting that displays students' images and/or personally identifiable information, this becomes an educational record protected under FERPA and must be stored and used in a way that protects the students' privacy (see FERPA Faculty/Staff FAQs by Rice University).

Note: Sharing a screenshot of your 4th grade class Zoom session (featuring student names and images) on Twitter is a FERPA violation because you are sharing an educational record without students' or parents/guardians' permission. Learn more: The 3 Biggest Remote Teaching Concerns We Need to Solve Now.

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 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 and the U.S. state comprehensive privacy law comparison website.

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://www.youtube.com/watch?v=VlYjtWg4Thw

American Bar Association. (n.d.). Customer information and privacy. Retrieved from https://www.google.com/url?q=https://www.americanbar.org/groups/business_law/migrated/safeselling/privacy/&sa=D&ust=1585001184609000

Cambridge Public Schools. (2019). Student data privacy. Retrieved from https://www.google.com/url?q=https://www.cpsd.us/cms/&sa=D&ust=1585001184609000

Cipriani, J. (2016, July 12). Pokemon Go can see everything in your Google account. Here's how to stop it. CNET. Retrieved from https://www.google.com/url?q=https://www.cnet.com/how-to/pokemon-go-google-account-access/&sa=D&ust=1585001184610000

Common Sense. (2020). Ask companies not to sell your data. Retrieved from https://www.google.com/url?q=https://www.donotsell.org/&sa=D&ust=1585001184610000

Farrar, L. (2018, March 13). Protecting students' online privacy in the classroom. KQED Education. Retrieved from https://www.google.com/url?q=https://ww2.kqed.org/education/2017/11/15/protecting-students-online-privacy-in-the-classroom/&sa=D&ust=1585001184610000

Federal Communications Commission. (2019, June 10). E-rate: Universal service program for schools and libraries. Retrieved from https://www.google.com/url?q=https://www.fcc.gov/consumers/guides/universal-service-program-schools-and-libraries-e-rate&sa=D&ust=1585001184611000universal-service-program-schools-and-libraries-e-rate

Federal Communications Commission. (2019, June 12). Children's Internet Protection Act (CIPA). Retrieved from https://www.google.com/url?q=https://www.fcc.gov/consumers/guides/childrens-internet-protection-act&sa=D&ust=1585001184611000

Gallagher, K., Magid, L., & Pruitt, K. (2019). The educator's guide to student data privacy. Connect Safely. Retrieved from https://www.google.com/url?q=http://www.connectsafely.org/eduprivacy/&sa=D&ust=1585001184612000

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://www.google.com/url?q=https://thenextweb.com/insights/2018/12/11/all-those-free-apps-on-your-phone-are-tracking-your-location-and-selling-your-data/&sa=D&ust=1585001184612000

Gussis, G. G. (2018). Software license agreements checklist. Retrieved from https://www.google.com/url?q=https://www.gussislaw.com/software-license-agreements/&sa=D&ust=1585001184612000/

Klein, A. (2020). Cyber attacks on schools tripled in 2019, report finds. Education Week. Retrieved from https://www.google.com/url?q=http://blogs.edweek.org/edweek/DigitalEducation/2020/03/cyber_attacks_on_schools_tripl.html&sa=D&ust=1585001184613000

Mamaysky, I. (2019, October 8). The FTC has its sights on COPPA, and edtech providers should take notice. EdSurge. Retrieved from https://www.google.com/url?q=https://www.edsurge.com/news/2019-10-08-the-ftc-has-its-sights-on-coppa-and-edtech-providers-should-take-notice&sa=D&ust=1585001184613000

McDowell, M. (2019, September 27). Reviewing end-user license agreements: CISA. Retrieved from the Cybersecurity and Infrastructure Security Agency website: https://www.google.com/url?q=https://www.us-cert.gov/ncas/tips/ST05-005&sa=D&ust=1585001184613000

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.google.com/url?q=https://cdn.ymaws.com/www.a4l.org/resource/resmgr/files/sdpc-publicdocs/PCSP_BATS-Educator-Toolkit.pdf&sa=D&ust=1585001184614000 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://www.google.com/url?q=https://www.termsfeed.com/blog/examples-user-agreements/&sa=D&ust=1585001184614000

Privacy. In The Merriam-Webster.com Dictionary. Retrieved January 28, 2020, from https://www.google.com/url?q=https://www.merriam-webster.com/dictionary/privacy&sa=D&ust=1585001184615000

UMass Amherst. (2020). Data classification at UMass Amherst. Retrieved from https://www.google.com/url?q=https://www.umass.edu/it/support/security/data-classification-umass-amherst&sa=D&ust=1585001184615000

U.S. Department of Education. (2018, March 1). Family Educational Rights and Privacy Act (FERPA). Retrieved from https://www.google.com/url?q=https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html&sa=D&ust=1585001184615000

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://www.google.com/url?q=https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html&sa=D&ust=1585001184616000