Alana Robinson
Week 3 Privacy Terms

Classcraft vs Class Dojo
Both Classcraft and ClassDojo are digital behavior management tools as well as engagement classroom tools. I use both tools with my students as part of the mandated school-wide Positive Behavior Intervention and Supports (PBIS) and to reinforce core competencies in social and emotional learning (SEL). Classcraft is for middle and high school students and ClassDojo is for elementary students. Both tools serve as a communication platform that helps teachers encourage students in class and engage parents and other teachers. Class Dojo is also used as a communication and messaging app for parents. Each app lists its privacy policy on its website. Both delete student, teacher, parent data after 12 months of inactive use.

Classcraft:
Althoguh Classcraft has taken the Student Privacy Pledge (2020) and they are FERPA (in USA), COPPA (in USA) and GDPR (in E.U.) compliant, they collect a ton of data. Here's what they collect: student first and last name, email, student ID assigned by district and app, student app username and passwords, student curriculum progression known as quests and student assignments, student use of avatar and pet system, powers system discussion, app messaging to teachers, student conduct or behavioral data, grade level and class name, application use statistics. The information is collected from the user or through cookies and is maintained and used within the school environment. The collected data is never used for marketing or disclosed to third parties. They do not sell student personal information or use or disclose student information for behavioral targeting of advertisements to students. They also do not retain student personal information beyond the time period required to support the authorized education or school purposes. What I question is that they conduct "periodic risk/vulnerability assessments and data privacy and security compliance audits". What is defined as periodic and would this be once a year or every three years? With these periodic audits do they share the results with their customers? Yet, it is a great form of transparency that they disclose they conduct vulnerability tests and that cybersecurity is embedded in their business model, at least it is presented that way on paper.

ClassDojo:
ClassDojo collects the first and last names of teachers, parents, students, school leaders, and logged-in users. The data is collected directly from the user from their website or mobile app or when a user fills out surveys or through their customer service email. The information is used to send an SMS message to invite a (potentially) non-logged-in user to ClassDojo for support or a survey or to let a ClassDojo team member contact the individual. The data is shared with Sendgrid in the U.S to help the company send friendlier emails. The information is stored on AWS (Amazon Web Service) servers in the U.S. and MLab in the U.S and back-ups are in the exact locations (AWS/MLab in the U.S.) and Zendesk in the U.S. and SurveyMonkey in the U.S. ClassDojo.