Know the Law

The Family Educational Rights and Privacy Act (FERPA):

FERPA, or the Family Educational Rights and Privacy Act, is a federal law that protects the privacy of student education records. EdTech developers need to be aware of FERPA requirements to ensure that they are not violating students' privacy rights. Here are some key points from FERPA for EdTech developers:

- FERPA applies to all educational institutions that receive federal funding, including K-12 schools and colleges and universities.
- FERPA protects the privacy of students' education records, which include any records that are directly related to a student and maintained by an educational institution or a party acting on behalf of the institution.
- EdTech developers must obtain written consent from parents or eligible students (those who are 18 or older) before collecting, using, or disclosing any personally identifiable information from education records.
- Personally identifiable information includes, but is not limited to, student names, addresses, Social Security numbers, and grades.
- EdTech developers must ensure that any third-party service providers they use to process education records also comply with FERPA requirements.
- EdTech developers must implement reasonable security measures to protect education records from unauthorized access or disclosure.
- EdTech developers must provide parents and eligible students with access to their education records and the opportunity to request that any inaccurate or misleading information in the records be corrected.

To comply with FERPA requirements, EdTech developers can take the following steps:

- Obtain written consent from parents or eligible students before collecting, using, or disclosing any personally identifiable information from education records. This can be done through a consent form or a terms of service agreement.
- Implement reasonable security measures to protect education records from unauthorized access or disclosure. This can include using encryption, firewalls, and access controls to safeguard data.
- Only collect the minimum amount of personally identifiable information necessary to provide the service. For example, if an EdTech app only needs students' names and grades, it should not collect any additional information such as addresses or Social Security numbers.
- Ensure that any third-party service providers used to process education records also comply with FERPA requirements. This can be done through a contract that includes specific provisions related to FERPA compliance.
- Provide parents and eligible students with access to their education records and the opportunity to request corrections. This can be done through a user interface that allows users to view and edit their information.

It is important for EdTech developers to understand FERPA requirements and take steps to comply with them to protect students' privacy rights. Failure to comply with FERPA can result in serious consequences, including loss of federal funding and legal action.

The Protection of Pupil Rights Amendment (PPRA):

PPRA stands for the Protection of Pupil Rights Amendment, which is a federal law that governs the use of surveys, assessments, and evaluations in schools that receive federal funding. EdTech developers are required to comply with PPRA when creating products that are used in schools that receive federal funding. Here are some key points to keep in mind when developing EdTech products in compliance with PPRA:

- Obtain written consent from parents or guardians before collecting personal information from students, such as demographic information or survey responses.
- Ensure that any surveys or assessments used in the product are age-appropriate and do not ask for information that could be used to identify individual students.
- Provide parents or guardians with access to the surveys or assessments used in the product, as well as any personal information collected from their child.
- Allow parents or guardians to opt their child out of participating in the surveys or assessments used in the product.

Overall, EdTech developers should prioritize accessibility and compliance with federal laws like PPRA when creating products for use in schools. By following best practices and being aware of platform limitations, developers can create products that are usable and accessible for all students, while also protecting their privacy and rights.

The Children’s Online Privacy Protection Act (COPPA):

COPPA (Children's Online Privacy Protection Act) is a federal law that applies to commercial "operators" of websites, apps, or other online services that knowingly collect information from children under age 13. If you are an EdTech developer, it's important to understand COPPA's key points to ensure that your products are compliant with the law. Here are some important takeaways for EdTech developers regarding COPPA:

- COPPA requires EdTech providers to obtain verifiable parental consent before collecting any personal information from children under 13.
- Schools act as intermediaries between vendors and students to obtain parental consent when using educational technologies that collect COPPA-protected personal information.

- EdTech providers are prohibited from using such information for any commercial purpose, including marketing and advertising unrelated to the provision of the school-requested online service.
- EdTech providers must not retain personal information collected from a child longer than reasonably necessary to fulfill the purpose for which it was collected.
- EdTech providers must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.
- COPPA rules forbid EdTech providers from conditioning participation in any activity on a child disclosing more information than is reasonably necessary to participate.

It's important to note that EdTech providers that have viewed data gleaned from students engaged in online learning as a form of commercial asset, akin to online data about adults, need to rethink their approach or potentially end up in the FTC's enforcement crosshairs.

To comply with COPPA, EdTech providers must obtain verifiable parental consent, limit the use of personal information to the provision of the school-requested online service, and implement reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. Additionally, EdTech providers should avoid retaining personal information longer than reasonably necessary and should not require students to submit to unnecessary data collection in order to do their schoolwork.

It's important for EdTech providers to understand COPPA's requirements and limitations on the collection, use, disclosure, and retention of personal information about children. As the FTC has put EdTech companies on notice of COPPA compliance investigations, it's crucial for EdTech providers to comply with COPPA to avoid enforcement actions and protect the privacy of children's personal information.