Panel Description:

Children's Privacy: Interpreting COPPA and Ed Tech In A Data-Driven Era

The Children's Online Privacy Protection Act (COPPA) is simple to learn, but often difficult to apply in practice. In addition to COPPA, there are other federal and state requirements relevant to children’s data and online interactions, including in the educational setting and with educational technology tools, that merit additional compliance considerations. Our panel will discuss considerations for determining when these privacy laws apply, and practical tips for how companies that market to children can address their privacy obligations. The panel discussion will include:

- Discussion of COPPA and recent updates.
- War Stories: Where COPPA and Ed Tech meet the real world.
- Mobile devices and tools used by children.
- Where do federal and state privacy enforcers go from here?

*****

1. Brief COPPA Overview Focused on Ed Tech

- COPPA Focus on allowing parents to make informed choices about how and when their children’s PII is collected and used

- Applies to commercial operators of online services who must provide notice and obtain verifiable parental consent before childrens’ PII collection; doesn’t apply to public schools or non-profits

- Potential reach: Online sites and connected/smart services/products – directed to children or if operator has actual knowledge collecting kids information even if on general audience site/service

- PII Scope: Update to COPPA includes screen name, persistent identifiers, geolocation information, in addition to other identifiers

- Civil Penalties (currently can be up to $41,484/violation). FTC and State AGs can enforce

- School Exception: Operators can get consent from schools (in lieu of the parents) if the PII is solely for the benefit and use of the school, and specific to the educational context – i.e., not for a commercial purpose
2. Highlights of State Law/Guidance

- **Student Online Personal Information Protection Act (SOPIPA)** - Focus on online apps/services for K-12 purposes

- Intent is to provide clear rules to help ensure student information not exploited for commercial purposes by ed tech and others

- Became effective in 2016 in California and New Hampshire; many other states followed with similar legislation

- Restrictions against targeted advertising to kids, creating “profiles” on students except for K-12 purposes, selling student information, and disclosing covered information

- Requires reasonable security and deleting the children’s PII upon request

- Can share student information only with educational researchers or educational agencies performing a school function

- Can use de-identified and aggregated data to develop and improve services

3. Real World COPPA/Ed Tech Challenges

- How to determine if the service/app is strictly educational? How to demonstrate to the school that it is
  
  o FTC FAQs: consider what information will be collected, how will it be used, and will any children’s (under 13) be used or shared for commercial purposes unrelated to education? Are schools allowed to review the collected student info? Can schools request deletion of the student info? If it does involve such student info and schools don’t have such rights, schools can’t grant consent on behalf of parents.

  o What about company Ts&Cs if they require school to obtain parental verifiable consent, and put burden on school to maintain such proof of consent?

  o What if schools don’t sufficiently obtain verifiable parental consent? Who bears the risk of enforcement?

  o How do we square that with the state SOPIPA requirements, even if there is parental consent.

- Consent

  o Who at the school can provide consent in lieu of parents? Discussion of what the FTC has said, and in practice, what often happens.

  o Does consent extend to more than one app/service?
Validity of the consent when the app/service is subsequently updated.

What are most Ed Tech companies doing to obtain sufficient consent?

- Third-Party Tracking
  - How to address third-party tracking on vendors’ online Ed Tech services (analytics or advertising) if it’s embedded into the sites and services?
  - FTC FAQ: Operators are responsible for determining the “information-collection practices of every third party that can collect information” via their app, service, or site. FTC staff have added further that “generally speaking, an operator must disclose the existence of any third-party tracking services that are collecting personal information from children using the operator’s website or online service.”
  - FTC staff have also stated that operators that don’t adequately disclose third-party tracking activity that collects children’s PII cannot obtain informed consent from parents or schools.
  - Also consider, under SOPIPA, if that tracking is for advertising purposes, the implications for the vendor and school. What type of due diligence is reasonable?

4. Additional Application to Mobile Tech

- [We can fill in with some real world examples incorporating above/other scenarios]

5. Crystal Ball Predictions / Best Practices

- Following Facebook/Cambridge Analytica developments, there is likely to be increased scrutiny on data sharing practices, particularly as related to sensitive information or for sensitive purposes or involving vulnerable audiences.

- As a result, Ed Tech may get a closer look at current practices, which may involve examples of regulatory enforcement (FTC, State AGs, private litigants).

- GDPR compliance may also increase emphasis on robust privacy practices and ability to demonstrate privacy sophistication by Ed Tech industry.

- Participants should continue to closely watch this space at federal and state level for further updates/guidance.

Best Practices

- For Ed Tech, important to anticipate the issues discussed and have policies and procedures for how to address – both from a legal and reputational perspective.

- Consider stricter lessons under state laws and fold into your compliance program:
Legal Savvy: Determine if/when COPPA and State Student Privacy Laws apply and how; build the FAQ commentary into your internal business considerations.

Data Collection and Retention: Limit data collection to the types and categories of information necessary to accomplish the objectives of the Ed Tech service as outlined by the educational institution with whom you contract. Be transparent with students and describe data collection and data use practices, as well as data retention policies.

Data Use: Do not use any information acquired from your site or service for profiling students and/or targeted advertising.

Data Disclosure: Notify students of third party disclosures of covered information; specifically, the types of entities that receive covered information and the purpose for the disclosure. Apply the appropriate safeguards to protect covered information when sharing information with third parties.

Individual Control: Implement policies and procedures to permit student access and correction of covered information.

Data Security: Implement and maintain reasonable safeguards and practices to protect student information, including employee privacy and security training. Have an actionable plan in place for data breach incidents.

Transparency: Provide a conspicuous and plain language privacy policy that identifies a privacy contact who can address questions regarding privacy concerns.