CHILDREN'S PRIVACY:

INTERPRETING COPPA AND ED TECH IN A DATA-DRIVEN ERA

APRIL 26, 2018

ALYSA Z. HUTNIK
Partner
Kelley Drye & Warren LLP

RYAN BROWN
Corporate Counsel for Global Operations
Rosetta Stone Ltd.
Children's Privacy In A Data-Driven Era
COPPA Overview

- Allow 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 children’s 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 the operator has actual knowledge collecting kids information even if on general audience site/service
COPPA Overview

• 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
State Ed Tech Laws

- **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
State Ed Tech Laws

- Student Online Personal Information Protection Act (SOPIPA) (Cont.)
  - 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
Real World Privacy Challenges
Crystal Ball Predictions

- Facebook
- GDPR
- Cambridge Analytica
Best Practices

• **Legal Savvy:**
  • Determine if/when COPPA and State Student Privacy Laws apply and how
  • Build the FAQ commentary into your internal business considerations
  • Consider forward-looking privacy trends, such as GDPR and more robust industry standards
  • Factor those potential changes into the ever-evolving “privacy by design” of the services
Best Practices

• **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 schools, students, and parents and describe data collection and data use practices, as well as data retention policies

• **Data Use:**
  - Avoid use of information acquired from your Ed Tech site or service for profiling students and targeted advertising
Best Practices (cont’d)

• **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
Best Practices (cont’d)

• **Data Security:**
  - Implement and maintain reasonable safeguards and practices to protect student information, including employee privacy and security training
  - Have an action 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
  - Ensure that the privacy-designated contact is responsive and knowledgeable in addressing issues raised