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

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. This outline and corresponding panel discussion address considerations for determining when these privacy laws apply, and outline practical tips for how companies that market to children can address their privacy obligations.

I. **Brief COPPA Overview Focused on Ed Tech**

- **COPPA’s principal goal** is to enable parents to make informed choices about how and when their children’s personally identifiable information (PII) is collected and used.

- The statute and regulation apply to **commercial operators** of online services who must provide notice and obtain verifiable parental consent before children’s PII collection; it does not 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 Attorneys General 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.

II. **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 is 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.

III. **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 COPPA FAQ:** 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 information 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 do not 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?

  o These and others are the types of considerations to work through when evaluating the educational vs. other purposes of the proposed Ed Tech usage in the educational environment.

• **Consent**

  o Who at the school can provide consent in lieu of parents?

  o **FTC COPPA FAQ:** The FTC recommends that, as a best practice, schools or school districts be the decision-maker, rather than teachers, and institute a procedure to formalize that process. The FTC also recommends as a best practice that the school provide parents with notice of the Ed Tech services for which the school has provided consented on behalf of parents, and make the Ed Tech service’s privacy notices available, including, for example, through Acceptable Use Policies for Internet use (AUPs) that is posted on a school website or sent to parents at the start of the school year.

  o Often questions arise concerning the scope of such consent. For example, does the consent extend to more than one app/service? Is the consent valid when the app/service is subsequently updated? What are most Ed Tech companies doing to obtain sufficient consent?

• **Third-Party Tracking**

  o How to address third-party tracking on vendors’ online Ed Tech services (analytics or advertising) if it is embedded into the sites and services?

  o **FTC COPPA 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.”

  o 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.

  o 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? Further, Ed Tech should carefully consider what trends and consumer expectations may evolve with the implementation of GDPR processes by many global companies, including with respect to their U.S. based practices.

IV. Looking Ahead: Crystal Ball Predictions in the Privacy/Ed Tech Space

  • 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 current data practices are likely to be more closely scrutinized by schools, parents, and regulators, which may extend to litigation and regulatory enforcement (FTC, State AGs, private litigants) that move the goal posts for compliance.

  • GDPR compliance may also increase emphasis on robust privacy practices and the 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.

V. Best Practices

  • For Ed Tech, it is 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 these into the compliance program:

    o **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, and factor those potential changes into the ever-evolving “privacy by design” of the services.

    o **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.

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

    o **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.
I represent large and small technology clients, helping them apply legal obligations nimbly to their marketing and data practices, and defending them in government investigations with mindfulness on efficiency and results that support innovation.

Alysa Hutnik delivers comprehensive expertise in all areas of privacy, data security and advertising law. Her experience ranges from strategic consumer protection oriented due diligence and compliance counseling to defending clients in FTC and state attorneys general investigations and competitor disputes. Much of Alysa’s practice is focused in the digital and mobile space in particular, including cloud, mobile payment, calling/texting practices and data-focused services.

Ranked as a leading practitioner in the Privacy & Data Security area by Chambers USA, Chambers Global and Law360, Alysa has received accolades for the dedicated and responsive service she provides to clients. The US Legal 500 notes that Alysa provides “excellent, fast, efficient advice” regarding data privacy matters. In 2013, Alysa was one of just three attorneys under 40 practicing in the area of privacy and consumer protection law to be recognized as a “Rising Star” by Law360.

Highly responsive to her clients’ needs, Alysa consistently delivers practical ideas and written deliverables in clear, effective language. An ardent team player and reliable solution-builder, Alysa is both a fierce advocate when needed, while consensus-driven when it benefits her client’s position. Alysa’s ability to prioritize, particularly when it comes to problem-solving, is grounded in listening to each client’s needs, while safeguarding their position. Clients and colleagues alike appreciate Alysa’s support in identifying and addressing “red flags” before serious problems can ensue.

Alysa is a frequent speaker at conferences around the country, as well as on national television news regarding legal privacy and technology-related developments, including appearances on Fox Business News.
and Al Jazeera America. She is a past chair of the ABA’s privacy and information security committee (section of antitrust law), the co-chair of the section’s 2011 Consumer Protection Conference, and served as editor-in-chief of the ABA’s Data Security Handbook, a practical guide for data security legal practitioners.

Prior to joining the firm, Alysa was a federal clerk for the Honorable Joseph R. Goodwin, United States District Judge, Southern District of West Virginia.

Experience

Providing practical legal advice on compliance with privacy, information security and marketing laws and best practices. This include compliance with federal and state laws throughout the U.S., as well as international laws such as the General Data Protection Regulation (GDPR). These efforts also include strategic advice applicable to the enterprise, and advertising and marketing practices; “privacy by design” efforts in developing software, apps and platforms; mobile payment compliance; and designing compliance programs to mitigate third-party liability exposure (whether from customers, affiliates, franchisees, independent dealers or service providers).

Performing TCPA and related consumer protection due diligence on calling and texting practices and technology solutions, as well as assisting clients in developing and enhancing telemarketing and non-telemarketing calling/texting compliance programs under the TCPA, TSR and state laws.

Assisting clients in proactive efforts designed to prevent data breaches, as well as crisis response and legal obligations upon discovering a potential data breach.

Assisting clients (particularly cloud-based platforms and solution providers) in developing efficient processes for managing and negotiating responses to third-party subpoenas that comply with applicable privacy and other laws, and are not unduly burdensome to the company.

Defending clients in privacy, data security, and advertising and marketing practice-focused investigations by the Federal Trade Commission (FTC) and state attorneys general.

Defending clients in advertising and marketing disputes with customers and competitors, including before the National Advertising Division and the National Advertising Review Board, and class action litigation (alleging false advertising and unfair and deceptive practice claims) in state and federal courts.

Honors and Awards

Selected as one of Washingtonian Magazine’s 2017 “Top Lawyers” in cybersecurity.

Named as a “Rising Star” by Law360 in the area of Privacy and Consumer Protection Law, 2013.


Memberships and Associations
American Bar Association
International Association of Privacy Professionals (IAPP)
Professional Association for Customer Engagement (PACE)

Professional Activities
Alysa is the current Consumer Protection Officer of the American Bar Association (ABA) Antitrust Section. She also has served on the Council of the ABA Antitrust Section, past chair of the Antitrust Section’s Privacy and Information Security Committee, was the editor-in-chief of the Section’s Data Security Handbook, and a co-chair of its 2011 Consumer Protection Conference.

Publications


“Do’s and Don’ts for the Internet of Things: Lessons Learned from FTC Privacy and Security Enforcement,” Bloomberg BNA, June 1, 2016, co-author.


“Smart’ Ways To Avoid FTC Internet Of Things Scrutiny,” Law360, April 11, 2016, co-author.


“Dial M for Murderous Liability: Maximize TCPA Compliance to Minimize Potentially Devastating Consequences,” Metropolitan Corporate Counsel, October 19, 2015, co-author.

“Another Privacy Victory For Video Service Providers,” Law360, October 5, 2015, co-author.

“Stay Tuned for Details: 5 Tips Online Streaming Services Need to Know About the Video Privacy Protection Act,” InsideCounsel, August 25, 2015.


“FTC Publishes Internet of Things Report,” The Metropolitan Corporate Counsel, February 13, 2015, co-author.
“Life’s a Breach: Make a New Year's Resolution to be Prepared,” InsideCounsel, January 7, 2015, co-author.


“Mobile Enforcement Continues To Be APPealing To FTC,” Law360, April 17, 2014, co-author.


“FCC Opens The Door To Vicarious Liability For Third-Party Telemarketing Under Certain Conditions,” The Metropolitan Corporate Counsel, July/August 2013, co-author.

“Practical Privacy Takeaways From FTC’s Deal With HTC,” Law360, March 4, 2013, co-author.


“Children’s Data (USA),” DataGuidance, February 11, 2013, co-author.


“FTC Issues Final Amendment to the Children’s Online Privacy Protection Rule (COPPA): A Detailed Look at What Has Changed,” The Metropolitan Corporate Counsel, February 2013, co-author.

“California Credit Card Privacy Litigation Continues Apace,” E-Finance & Payments Law & Policy, December 2012, co-author.


“State Agency Notice Requirements for Data Breaches Chart,” PLC Law Department, July 2012, co-author.


“Early 2009 Shows Active FTC Data Security Enforcement: No Room For Lax Safeguards,” Metropolitan Corporate Counsel, March 2009.


“State Agency Notice Requirements for Data Breaches Chart,” *PLC Law Department*, February 2010, co-author.


“Product Placement and Brand Integration Strategies: Managing the Risks of Regulatory Uncertainty,” *ABA*


**Speaking Engagements**


“Beyond NAIC and DOI: How other laws, enforcement agencies and consumer complaints can influence your advertising practices,” 17th Annual IAdCA Conference, Austin, TX, April 4, 2018.


“Regulatory Enforcement: Updates from North America and the EU,” IAPP Privacy Academy, San Jose, CA, September 19, 2014.


“Privacy in the Cloud—Will It Float?” 61st Spring Meeting of the ABA Section on Antitrust Law, Washington, D.C., April 11, 2013.


“Determining the FTC’s Seminal Ability to Pair Traditional Regulations with Emerging Internet, Mobile and Wireless Communications Technologies,” ACI’s 2nd Annual Regulatory Summit for Advertisers and Marketers, Washington, D.C., June 17, 2008.


“Goldilocks and the Three Privacy Bears: Is There Too Much, Too Little or Just the Right Amount of Privacy Law?,” Moderator, ABA Section of Antitrust Law Teleconference, October 25, 2006.

