Cybersecurity Law Report
An Acuris company

cslawreport.com

June 19, 2019

COPPA

Kids, Privacy & Legal Compliance

By Peter S. Hyun and Duane Pozza, *Wiley Rein*

It is estimated that every day more than 2,500 apps are added to the Apple App Store, and more than 1,300 to the Google Play Store. These staggering figures reflect a virtual marketplace where app developers are under significant pressure to be the first to market, to "disrupt" industries and/or to be the first to innovate a new market. However, rushing to market without first devoting time and resources to legal compliance can pose significant business risk for companies down the road. One area where it is important to ensure compliance early on is the protection of children's privacy.

See "COPPA Compliance Lessons Following Musical.ly's $5.7 Million FTC Settlement" (Mar. 20, 2019).

The Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA), enacted in 1998, requires online service providers that direct services to children (under age 13) and collect personal information from children to protect children's data, provide a clear privacy notice to users and parents and get parental consent before collecting certain information from kids.

While COPPA vests broad regulatory and enforcement authority with the FTC, COPPA also affords State Attorneys General with authority to enforce COPPA. Both the FTC and State Attorneys General across the country have been extremely active in enforcing COPPA in recent years, particularly in the wake of data breaches and sweeping new privacy laws in the European Union and California.

See CSLR's three-part series analyzing early GDPR enforcement: "Portugal and Germany" (Jan. 23, 2019); "U.K. and Austria" (Jan. 30, 2019), "France" (Feb. 6, 2019); and "CCPA Priorities: Turning Legislation Prep Into a Program Shift" (Jun. 5, 2019).

Recent COPPA Enforcement Actions

Several months ago, the New York Attorney General's office reached a $5-million settlement with a large online media company to resolve allegations that the company's online advertising business was unlawfully targeting display ads on websites it knew were directed at children. New York and other states have brought a variety of enforcement actions against online companies over the past decade.

The FTC has also been active in COPPA enforcement. Earlier this month, three online dating apps were removed from Apple's App Store and the Google Play store after the FTC alleged those apps allowed children to access them in violation of COPPA. Not only did the FTC issue a warning letter to the apps, but it also issued a consumer alert for parents regarding the dating apps.

These stern consumer alerts followed a series of notable FTC COPPA settlements with website operators under various provisions in COPPA. In April, the FTC settled a COPPA case against a dress-up games website that included allegations under the data security provision of COPPA. That provision requires operators to take reasonable steps to safeguard consumer data. The vulnerabilities on the website allowed hackers to breach the platform, putting millions of consumers' data at risk.

The FTC also resolved another COPPA investigation – the largest ever – with a prominent video social networking app with over 200 million users. The $5.7-million settlement resolved allegations that the video app illegally collected personal information from children and failed to seek parental consent before collecting kids' private information.

The dress-up website settlement and video app settlement also involved coordination with the Consumer Protection section of the U.S. Department of Justice. In the video app settlement, for example, the Justice Department and the FTC jointly filed a federal court consent decree that bound the company to comply with COPPA going forward, and take down all videos made by children under the age of 13. This type of coordination between the FTC and the Justice Department is not uncommon.

See also "Lessons From FTC 2018 Privacy and Data Security Update: Financial Privacy, COPPA and International Enforcement" (May 1, 2019).

COPPA Reforms and Policymakers

Not only do government enforcers have COPPA squarely on their radar but policymakers do as well. In the Internet of Things era, and with the ubiquitous nature of online services and activity, much has been made about efforts to update the 20+ year old COPPA law to match technological advancements.

Recently, Senators Ed Markey (D-MA) and Josh Hawley (R-MO) have pressed for changes to COPPA to extend even greater data privacy protections to children. The bipartisan duo recently introduced a bill that would update COPPA to require that online companies create an erase button for parents to remove all of their child's data from a service.

These types of policy proposals follow a sweeping change that the FTC undertook at the end of 2012 with respect to how the Commission defined critical terms within COPPA. The FTC modified, for example, key definitions such as what comprised "personal information" and "website or online service directed to children," and also revised notice requirements and consent mechanisms under the statute. The updates were made because of calls to stay current "amidst whirlwind technological change."

Additionally, just weeks ago, the Chinese government, through its top internet regulator (the Cyberspace Administration of China), released draft COPPA-like regulations applicable to online providers. The draft regulation would cover the collection of personal information relating to children under age 14. The draft shares many similarities with COPPA – including parental consent provisions and consumer disclosure provisions – but it also incorporates additional security requirements such as data breach notification requirements and encryption requirements. Undoubtedly, stakeholders will be carefully attentive to the final implementation of the regulation in China.

How Can You Achieve COPPA Compliance?

With COPPA compliance being a hot issue for regulators, enforcers and policymakers, it is incumbent on all online companies – including app developers – to incorporate an appropriate COPPA/privacy compliance strategy into its business plan early on.

Indeed, before a product or service is launched, it is essential to have at least a baseline understanding of how to deal with future government risk and/or investigations in this area. Assessing that risk, however, can be difficult, given the complex policy and regulatory environment that many tech companies operate under, and given the nuances that each product or service possesses on its own.

Taking a proactive approach early on to issue-spot legal risk and COPPA compliance before deploying a new product or service can help minimize potential violations and the cascade of troubles that can follow. Ensuring compliance at the beginning of the development process can also help preserve a compliance culture that can serve the company well long into its future.

The FTC has a helpful six-step compliance plan for COPPA, and the following are additional considerations to think through when putting together a plan for COPPA compliance in the context of a broader assessment of privacy, cybersecurity and data governance risks.

See "Focus on Children's Privacy by FTC and Plaintiffs Calls for Prioritizing COPPA" (Sep. 13, 2017).

Create a Risk-Management Plan

As a general matter, every business must assess data-related risks and prioritize them to determine how it will manage risk events as they arise. When thinking through a COPPA risk-management plan, consider that it encompasses sensitive private data of children and, thus, risk in this area goes beyond legal risk to include, among other things, reputational risk and political risk. Therefore, developing a plan to identify areas in which children's data may be gathered and COPPA obligations may be triggered, assess compliance obligations, and manage risks related to such data is of utmost importance.

Conduct an Internal Review of Your Product

Not only should the business have a clear view of the legal COPPA requirements (through help with outside counsel or otherwise), but early on, when a company is designing its product or service, the company should evaluate whether and how it may be used by children under the

age of 13. If, in fact, it may be used by children, conducting an internal review can help the company clearly determine what kind of data it collects, as well as how that data is used, stored, shared, and accessed, and whether any changes should be made for COPPA compliance purposes. Commonly, companies will create and analyze data flow maps to help understand these points. And, at a minimum, where companies have actual knowledge of customers' ages under 13, companies must pay close attention to ensure they are satisfying all applicable COPPA requirements.

Develop Clear and Consistent Privacy Policies

It is important that your consumer-facing privacy policy corresponds with privacy and data security policies and procedures that apply internally across the company, across all components and sectors. In other words, policies should not just apply to IT departments, but across the organization. Policies should also include designated personnel to train and enforce on data governance policies.

Secure Data

Companies should be mindful of securing their own data, particularly where the data may be accessed or provided to a third party. Companies should carefully review data security provisions in third-party contracts, and in doing so, implement contractual commitments to ensure compliance with COPPA, the company's privacy and data security policies and other legal obligations that may apply.
Given the regulatory and enforcement environment on issues of privacy and data security, companies should strongly consider COPPA compliance early on in their product or service life cycle and take steps to avoid COPPA-related headaches down the road.

See CSLR's two-part series on how to maintain effective and secure long-term vendor relationships: "Understanding the Risks" (Jun. 20, 2018); "Addressing the Issues" (Jun. 27, 2018).

Peter S. Hyun, a partner at Wiley Rein LLP, represents individuals and entities in government enforcement actions, congressional investigations and State Attorneys General investigations. He is a former Assistant U.S. Attorney in the Eastern District of Virginia's U.S. Attorney's Office, Assistant Attorney General in the New York Attorney General's office and Chief Counsel to U.S. Senator Dianne Feinstein on the U.S. Senate Committee on the Judiciary.

Duane C. Pozza, a partner at Wiley Rein LLP, counsels on tech regulation, consumer protection and FTC enforcement. He advises clients on key legal issues, advocacy positions and regulatory compliance involving consumer uses of developing technology. Prior to joining Wiley Rein, Pozza was an Assistant Director in the Division of Financial Practices at the FTC's Bureau of Consumer Protection, where he led consumer protection efforts in financial technology and other sectors, and supervised investigations and enforcement actions involving consumer protection issues on technology platforms.