

Common Sense Media to Grade EdTech Company Privacy Practices

March 15, 2016

Last week, Common Sense Media ("CSM") announced that it is undertaking an ambitious initiative to evaluate and grade the student data privacy practices of EdTech companies that provide products, apps, or services for use in K-12 classrooms. CSM's announcement indicates that they have established a working group of approximately 40 US public school districts, including a core group of populous districts such as New York City Department of Education, Fairfax County (VA), Denver Public Schools and Chicago Public Schools. In consultation with these districts, CSM intends to develop the go-to resource for evaluating EdTech privacy practices.

What do we know?

Not much yet. CSM reviewers will use a set of yet-to-be-published principles to assess the data privacy and security practices and policies of selected companies. Note that, unlike another non-governmental initiative – the Student Privacy Pledge – CSM is not making this assessment voluntary and companies will not have the opportunity to opt-out of the review or grading by CSM.

CSM states that it will provide companies with internal feedback prior to publication to allow them an opportunity to respond to any questions or concerns, although the impact of any such response will be entirely at CSM's discretion.

CSM expects to release a draft of the guide they will use to assess privacy practices in late March 2016 and anticipates releasing a final version of the guide in early April. While CSM is not formally seeking comments from EdTech companies on the guide, we believe that this process requires close monitoring and that such companies should have a voice in the process.

CSM stated that the principles it will use to assess "compliance" will be based largely on applicable federal laws (such as the Family Educational Rights and Privacy Act, or FERPA, the Children's Online Privacy Protection Act, or COPPA, and Federal Trade Commission statutes). However, the principles will also incorporate Department of Education guidance (likely including its Model Terms of Service), and industry "best practices."

CSM notes that it will not apply the principles rigidly; rather, the grade a company receives will be based on a qualitative assessment that will take into account both the sensitivity of the data collected and CSM's judgment about the necessity of the information to be collected. Thus, a company that CSM judges to lack necessity for certain information it collects could receive a lower grade even if its data use, disclosure, and security policies meet or exceed those of a company CSM judges to have sufficient necessity for the same information.

What will this mean for my company?

It is difficult to say at the moment what impact CSM's plans will have on EdTech companies. We know that school districts and states have become increasingly concerned with student data privacy in recent years. In the absence of a uniform national standard (beyond the outdated FERPA), states – starting with California – have taken the lead in updating and enhancing student data privacy laws. The results have been mixed and the patchwork set of laws increasingly created obstacles for EdTech companies, especially emerging companies. In the absence of any substantial federal legislation on the horizon, a consensus set of reasonable principles could be welcome news.

However, companies may be skeptical that this initiative will create such a reasonable consensus that will address legitimate interests for the privacy of students without unnecessarily undermining the valuable

educational prospects for data-driven products and services.

The ultimate success of this initiative can't be predicted at this time; however, companies should closely monitor developments and may wish to seek an active role in this discussion. School districts are looking for a user-friendly guide to address concerns about privacy and the use of third party products and services in the classroom. This grading system would seem to provide a tantalizingly simple approach to overwhelmed administrators and teachers. But in order to be valuable, the system needs to be not only simple but also useful and fair. Companies could help achieve such goals by proactively joining this conversation.

What should I do now?

- Make sure your Privacy Policy and Terms of Service are up-to-date and tailored to your specific needs. Having a Privacy Policy that you do not follow is worse than not having one.
- Consider consulting with a student data privacy expert to ensure that your Privacy Policy and Terms of Service comply with FERPA and COPPA along with applicable state laws. Don't forget about the Department of Education's Model Terms of Service.
- Dust off (or create) a comprehensive data security policy. Ensure that your policies address physical, technical, and administrative aspects of data security and that the level of security employed is commensurate with the sensitivity of the data you collect. Make sure you have a breach response plan.
- Stay tuned. When it comes to this initiative, the devil will be in the details. We will continue to monitor developments and will assist clients to respond appropriately.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our [legal notices](#).

Key Contacts

Jay Vaughan Washington, DC	jvaughan@cooley.com +1 202 776 2031
--------------------------------------	---

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.