

from one's geo-location and engagement with content to contents of emails and the full set of websites someone has visited online.

There are early indications that these types of commercial surveillance practices are beginning to invade ed tech, creating the risk that students will be profiled and targeted—and that their sensitive information could be exposed as part of a data breach.

The “notice and consent” approach to privacy can be particularly inadequate in contexts where people lack real choice or alternatives. For example, a parent who is uncomfortable signing up their child for expansive tracking and data collection may do so anyway if it is the only way their child can do their schoolwork.

Fortunately, though COPPA is often thought of as a “notice and consent” regime, the law also provides *substantive* limits on what data can be collected and how it can be used and retained. In other words, ed tech providers and other companies covered by COPPA are prohibited from engaging in the types of surveillance and monetization that have taken hold across other digital services.

B. Use Limitations

Second, there are limits on how ed tech companies can use the data that they collect on children. A school's ability to consent on behalf of parents is limited to data collected in the context of educational services.⁶ This means that for ed tech companies operating based on authorization from a school district or school, the children's data they collect cannot end up as part of any score, algorithm, profile, or database that is used for targeted advertising or any other commercial use.

In other words: children's data should not be fodder for A/B testing, should not be plugged into supposedly "anonymous" or "aggregate" audience models, and should not be extracted and used to develop new products. Children's use of learning games should not be used to enhance engagement for future users, and children should not be subjected to targeted advertisements just to do their schoolwork.⁷ Although many of these practices are commonplace in the big data ecosystem, they have no place in our schools, and, where they are forbidden by COPPA, the FTC intends to vigorously enforce those prohibitions.

C. Retention Limitations

Third, COPPA-covered companies must retain such information "only as long as is reasonably necessary to fulfill" that purpose.⁸ This means that companies, once they collect a child's data, cannot hang onto it for speculative future uses. The Commission's recent enforcement action against Kurbo highlights the importance of this provision. Specifically, the Commission alleged that Kurbo, now a subsidiary of the company formerly known as Weight Watchers ~~RWD, WWRQ~~, retained children's data indefinitely, without regard to whether it was necessary. The FTC's settlement requires WW to delete children's information that was unlawfully collected, as well as any derivative work product, such as models or algorithms.⁹

D. Security Requirements

Fourth, if an ed tech provider must collect data and must retain it, the COPPA Rule also requires

III. Next Steps

The Policy Statement underscores the importance of safeguarding children’s privacy in today’s digital economy.

COPPA is a critical tool in the FTC’s toolbox, one that we will use vigorously. But it can only go so far, especially given the dramatic changes in how firms collect, use, and monetize children’s data. I understand that Congress is considering what legislative updates might be necessary to adapt COPPA to modern market realities—and I very much welcome these efforts.

At the FTC, we are considering ways to strengthen our rules and expand their protections more broadly. The COPPA Rule was last updated in 2013, and another Rule review was initiated in 2019. I look forward to reviewing the record as we determine next steps for strengthening protections online.

IV. Conclusion

The collection, use, and retention limitations of COPPA place notable restrictions on how digital companies operate in our schools. Though widespread tracking, surveillance, and expansive use of data across contexts have become increasingly common practices across the broader economy, this Policy Statement makes clear that COPPA forbids companies from wholesale extending these practices into the context of schools and learning.¹¹ We intend to vigorously enforce these restrictions in order to protect children online.

¹¹ I am grateful to the Bureau of Consumer Protection’s Peder Magee, Jim Trilling, Mark Eichorn and Kristin Cohen for their work on this statement, as well as for their efforts enforcing COPPA, issuing rules, and developing guidance relating to children’s online privacy. Thank you also to Josephine Liu, Rich Gold, and Liz Tucci in our Office of General Counsel for their input, and June Chang, Lesley Fair, and Jennifer Leach in DCBE for getting the word out.