ITCS 3688 Team FOXTROT Article

Team Foxtrot Members:
Elif Su
Henry Di Leo
Charles Morris
Jacob Sasser
Arnav Sareen

Reference:

Determann, L., Tam, J., & Denham, E. (2023, August 28). *Kids' and teens' online privacy and safety: 8 compliance considerations*. The International Association of Privacy Professionals (IAPP). Retrieved September 1, 2024, from https://iapp.org/news/a/kids-and-teens-online-privacy-and-safety-8-compliance-considerations

The Datafication of Children

Main purpose: — *Elif Su*

The main purpose of the article is to outline strategies to maintain legal compliance when dealing with data that belongs to minors highligthing the risks of exposure to harmful content with inadequate data protection. The article emphasizes the importance of parental guidance when it comes to using these platforms as minors while assigning the majority of the responsibility for data privacy to the companies. The article urges companies to take measures against underaged use and lists potential guidelines as well as algorithms that can be used to ensure data privacy for minors.

Key Question: — *Henry Di Leo*

While collecting data on users is beneficial for flourishing companies, there is an ethical responsibility to prioritize the safety of children. So, how can companies minimize the data they collect on children, while maximizing the security and privacy for children? The author acknowledges the balance needing to be achieved to make all parties satisfied, but there is a rightful and heavy priority on protecting children from harmful data practices. Throughout the article, there is a clear pattern that there is no single solution that could work in every situation, although we see that there are multiple strategies that can be implemented together for a company to achieve a desired outcome, like having “high privacy” as the default setting for children with included parental controls so children cannot give

away their privacy so easily. The author emphasizes that it is the responsibility of the company to use and maintain ethical and legal practices. As laws develop and users have more rights to protection, companies must adapt policies with the user in mind to minimize legal risks.

Author's Focus: — *Charles Morris*

The author is focused on protecting children's data and providing information about privacy for childrens data in the digital environment. They approach this from the angle of educating parents and offering parental guidelines to them to understand the digital risks their child may face. The article aims to convince parents that they must be more aware and proactive in monitoring and managing their child's online activities. It emphasizes the importance of safeguarding children's personal information and educating them on safe internet practices to protect their privacy.

Most important information: — *Jacob Sasser*

The most important information in this article is laws are being created and updated to help protect children from the dangerous aspects of the internet. By making companies abide by regulations that will keep children and their information safe from potential bad actors. Children under 13 can not consent to have their personal data sold, so COPPA and laws like it help protect children against that.

Main underlying ethical dilemma: — *Arnav Sareen*

As technology becomes further ingrained into the routines of everyday life, the implications of data privacy and children only become more and more essential. Young people often lack the broader world knowledge and experience to recognize malicious intent and their perceptions are often easily skewed. Thus, if companies are enabled to collect vast amounts of data about minors, then they may use this data to target one of the Internet's most vulnerable populations. Furthermore, unlike adults who may be able to opt out of particular data-gathering schemes or pursue litigation if their rights are violated, there is little awareness about how children can enjoy these same protections, and often any measures that can preserve their data privacy are behind convoluted and needlessly complex language. Finally, given that much of the Internet lies in an unfiltered, transparent environment, children are at particular risk for exposure to explicit or damaging content. In many cases, many online platforms promote this content to minors unknowingly as social media trends and algorithms are unable to differentiate between an appropriate and inappropriate audience.

Main implications: — *Jacob Sasser*

The main implication for society is that with these laws, children under 13 will now have better protection against bad actors online. This is a very good thing as children that young usually do not understand the implications behind what they are doing, so requiring parental consent to agree for your data to be sold is a good thing. With the coppa act, children can now have a much safer experience online.

Main conclusion: — *Elif Su*

The article concludes that the responsibility of monitoring data privacy for minors belongs to the companies and urges companies to practice the suggested ways to protect their data. Inadequate protection of data belonging to minors can not only result in legal consequences but it can severely damage the companies reputation.

Our Team's Thoughts:

Elif Su: I think it is really important to make sure that minors on the internet have access to privacy. I completely agree with the fact that the companies should take accountability when it comes to protecting minors on their platforms as parental guidance can be easily misguided or the parents may not be aware of the extent of the content a platform can offer. The strategies listed on the article seem perfectly reasonable and it can very well be beneficial to users other than minors.

Arnav Sareen: Given that just a few years ago, I was a minor using the Internet, this topic has a personal appeal; in many ways, all of us are victims are intrusive data violations, and our own personalities are being exploited. Most legislation concerning digital privacy and safety is severely lacking, and I wonder how we can provide a greater incentive to governments to enact more widespread protections for children. Many of us have spent years on the Internet at this point, much of that time coming as adolescents—how much data do these companies like Google and Meta really have on us?

Charles Morris: I believe that the focus on protecting children's data and educating parents about digital privacy is very important, but should be looked at in a broader context. One of the biggest concerns is the monetization of ads and the intentional addictive nature of nearly all online content, where its games, videos, or social media are targeted at children. Companies spend billions of dollars annually to ensure their platform and ads maximize engagement at the expense of children. This should lead us to a broader discussion on the relationship between profit and safety. Furthermore, I believe that companies should be collaborating with parents to create the safest possible experience for children to inform parents as well as protect users from privacy risks and potentially unsafe interactions.

Henry Di Leo: I am delighted to see a topic like data privacy for children be taken seriously among legislature but I feel like we are nowhere close to where we need to be. As a kid it was the simplest thing to set my birth year to a couple years before I was born to be able to access things I wanted to access. With the self verification there is nothing stopping me from lying without thinking about data risk, because realistically most children would not consider it. The general public has very little knowledge

on how data collection works, what data companies can access, and where that data goes. Growing up with technology I can say that even now, I am clueless as to what happens to data I put on the internet, willingly or unknowingly. Parents are not informed enough to understand what data is at risk for themselves and the same applies for their children.

Jacob Sasser: It is extremely important that children can be safe from predators online. I have been on the internet for my whole life, and the coppa act helped protect me from bad actors online, when I was a child using the internet, I did not even know what data collection was. Thanks to the coppa act, I was not subject to having my data sold when I was using the internet as a child.

Our Team's Questions:

What are some ways we can all benefit from the strategies suggested by the article? — ***Elif Su***
Should websites such as betting platforms or particular social media sites require people to prove their age before being allowed to access them? — ***Arnav Sareen***
How can we inform parents of potential privacy and security risks for their children when they create their kids account? — ***Charles Morris***
What can be done about the data of children that has already been collected before/after restrictive laws were passed? — ***Henry Di Leo***
How can we create a better way for allowing parents to consent to their child's data being used? — ***Jacob Sasser***