A discussion of TikTok's disregard of UK and US child data policies

Dr. Clifford Fisher
Olivia Hodge
Lydia Barber
Purdue University, USA

Keywords

COPPA Violations, Child Privacy Policies, Data Collection, TikTok Security, UK Data Protection

Children are among the most vulnerable members of society, necessitating strong protections, especially regarding their online presence. Although laws have been enacted to safeguard their physical well-being, many online companies, including TikTok, have failed to ensure proper handling of children's data. TikTok, a popular social media platform, has been repeatedly flagged for security risks, including inadequate parental consent, unreasonable data collection, and unauthorized data transference. This paper examines these discrepancies within TikTok's data privacy practices concerning US and UK regulations, with a focus on the Children's Online Privacy Protection Act (COPPA) and the UK General Data Protection Regulation (GDPR).

This research follows a comparative analysis of regulatory frameworks that highlights TikTok's repeated failures of compliance, while discussing the broader implications for online child data protection. A comprehensive review of TikTok's practices offers insights into how companies can improve their compliance with child data protection laws while highlighting the importance of regulatory enforcement.

Corresponding author: Olivia G Hodge
Email address for the corresponding author: ohodge@purdue.edu
The first submission received: 24th April 2024
Revised submission received: 14th August 2024
Accepted: 25th August 2024

Introduction

Today's children are growing up in a society dominated by technology. As a result, online services and applications have an added responsibility to regulate how data from children is collected and protected. The mass increase in children using technology and social media has coined a new term in the 21st century, the "iPad kid" (Leiby). A term that goes beyond "digital native," iPad kids describe the children who have direct access to digital media as young as two years old. Due to children's high level of vulnerability, the idea of increasing legal protections for children is nothing new. Laws such as prohibiting alcohol consumption, establishing a legal driving age, and preventing child abuse all have the goal of protecting children. With nearly one-third of children between the ages of 7 and 9 using social media, it is more important than ever for social media platforms and online services to comply with standards set by regulatory agencies and provide a secure experience for child users (Searing, 2021).

Online data collection has become a significant marketing tool used by companies. Collecting demographic and behavioral data allows companies to specifically target individuals in a personalized way (Froehlich, 2023). With nearly 91 percent of consumers more likely to purchase a product or service when ad targeting is used (Rouse, 2017), online data is rapidly becoming a currency in commerce (Evans, 2018). As this form of currency continues to develop, several problems have arisen with collecting demographic and personalized data of children under thirteen.

During the COVID-19 pandemic, children were forced to rely on technology often provided by the schools to complete their work remotely. As children used online services to assist in learning math, reading, and other subject material, it was revealed that these online services were also collecting data from students and sending the data to third parties to be further analyzed without parental consent (Harwell, 2022). These educational services shared the data with advertising companies like Google and Facebook to find ways of targeting children with personalized advertisements across platforms. For instance, the educational platform named "Schoology" was discovered to have a code within the app that would "extract a unique identifier from the student's phone" to be later used to track the students across platforms (*Online Tools for Teaching & Learning*, n.d.). As data becomes a sought-after resource for companies, concerns involving children's data online have surfaced from not only educational sites but popular social media companies as well (Harwell, 2022).

TikTok, a popular social media platform run by the Chinese company ByteDance Ltd., has become a significant point of interest to online privacy regulators. In May 2023, the social media company was fined £12.7 million by the United Kingdom's (UK) data protection agency, the Information Commissioner's Office (ICO). The original notice of intent was released in September 2022, accusing TikTok of violating the UK General Data Protection Regulation (UK GDPR). The breaches discussed included collecting data from child users without proper parental consent, collecting and misusing particular category data, and failing to provide clear and easy-to-understand data policy information. While TikTok was not found guilty of misusing special category data, the company was found guilty of collecting child user data without proper consent, failure to provide a clear understanding of their privacy policy, and failure to ensure safe and lawful data processing for their UK users (*Ico fines TikTok £12.7 million for misusing children's Data*, 2023).

This is not the first time that ByteDance Ltd. has gotten into trouble with its social media platforms. In 2019, ByteDance Ltd.'s predecessor to TikTok, Muscial.ly, was also accused of mishandling the data of its child users. Musical.ly settled a $5.7 million fine from the Federal Trade Commission (FTC) for its non-compliance with online children's privacy laws in the US (Singer, 2022). The social media app was accused of failing to seek parental consent before collecting children's data, such as names, email addresses, and other personal information, while aware of the significant presence of child users on their platform. The 2019 lawsuit resulted in the most important monetary settlement in a case involving the violation of the US Children's Online Privacy Protection Act (COPPA) (Ritchie, J.N. & A., Jayanti, S.F.-T, et al., 2022). In July 2020, more than a third of the total daily TikTok users in the US were reported as 14 or younger (Zhong, 2022). With such a large age demographic of underage users on the social media platform, there is an increasing sense of urgency for regulatory agencies to investigate TikTok's child data protection practices.

Research Methods

This discussion follows a comparative analysis in differentiating the United States' and United Kingdom's data regulation frameworks. The regulation analysis focuses on the Children's Online Privacy Protection Act (COPPA) in the US and the General Data Protection Regulation (GDPR) in the UK, giving special attention to how these are designed to protect children's online data. Data collected from legal case studies, regulatory documents, and academic papers were used to identify and compare the enforcement actions taken against TikTok in both countries. The evaluation of these sources aims to expose gaps of compliance and shine a light on future regulatory efforts.

Part I. Data Privacy Laws in the UK and the US

I. UK Data Protection Policies

The United Kingdom's data privacy laws are designed to build and expand off one another. The foundation of these data protection laws is the Data Protection Act of 2018 (DPA 2018). The DPA 2018 establishes grounds for the Privacy and Electronic Communications Regulations of 2003 (PECR), the UK General Data Protection Regulation (UK GDPR), and several other statutes, such as the Children's Code. The Data Protection Act of 2018 (DPA 2018) is the UK's primary data protection law. While initially put into effect by the European Union, the DPA 2018 has since been amended to best fit the UK's status outside the EU, creating a three-segmented system for UK citizen's data protection (*About this code, n.d.)*.

The first segment addresses the general processing system, highlighting the integration of the UK GDPR. The second segment discusses law enforcement data processing and the third regulates intelligence services processing. In addition to this segmented system, the DPA 2018 established the Information Commissioner's Office (ICO), defining its roles and function as the UK's data protection watchdog. Out of the three segments discussed, the first is most applicable in this context due to the UK GDPR's direct impact on company data policies (*About this code, n.d.)*.

The GDPR, first established by the European Union, became globally known as the gold standard for data protection. When Brexit occurred in 2020, UK data regulation was created to meet the same standards as the EU and maintain a sense of familiarity. To ensure that the free flow of personal data could continue from the EU to the UK, the EU performed an adequacy test on the UK GDPR and was deemed acceptable (*About this code, n.d.)*. The UK GDPR defines the responsibilities of data processors and data controllers. Data processors are those within a company or organization processing an individual's data. Controllers determine the purpose and means of personal data processing. The UK GDPR also establishes seven fundamental data protection principles for companies to abide by when processing consumer data: lawfulness, purpose limitation, data minimization, what is adequate and relevant, accuracy, storage limitation, integrity and confidentiality, and accountability (*About this code, n.d.*).

These principles represent the spirit of the legislation of the UK GDPR. Companies that comply with these principles are better set up for success in following ethical data protection practices. Any companies and organizations in or outside of the UK that offer goods and services to UK consumers are held to the UK GDPR principles and regulations (*About this code, n.d.)*.

The UK GDPR gives an explicit command for companies to take additional care in the collection of children's data. Recital 38 of the UK GDPR states, "Children merit specific protection about their data, as they may be less aware of the risks, consequences, and safeguards concerned and their rights about the processing of personal data. Such protection should, in particular, apply to the use of personal data of children for marketing or creating personality or user profiles and the collection of personal data about children when using services offered directly to a child…" (*About this code, n.d.)*.

In 1989, the UN Convention on the Rights of the Child defined children under the UK GDPR as anyone below the age of eighteen. "Childhood is separate from adulthood and lasts until 18; it is a special protected time, in which children must be allowed to grow, learn, play, develop and flourish with dignity" (UNICEF). Throughout the internet, children are constantly tracked and observed without their consent or their parent's knowledge. "By the time a child reaches 13, online advertising firms hold an average of 72 million data points about them" (Fowler, 2023). Information about children, such as their moods, the times they eat and sleep, and even the status of their relationships, are logged and recorded. The ICO describes this continual data logging as children being "datafied." The world is rapidly advancing in technology. Rather than hide children from the internet, the UK GDPR encourages children to access and learn how to navigate the internet with appropriate safeguards (*About this code, n.d.*).

In addition to the UK GDPR, the Children's Code was implemented as an additional safeguard. The Children's Code, established under section 125 of the DPA 2018, provides specific guidelines for companies to follow as well as practical methods of compliance. The applied standards of this statute always work to prioritize the best interests of the child. Companies under this statute's regulation include online service providers or any company or organization that processes consumer information through apps, programs, websites, games, or community environments (*Introduction to the Children's Code*, n.d.).

The Children's Code compels companies to maintain a risk-based approach in multiple facets. To start, the Children's Code requires that online service providers must undergo a Data Protection Impact Assessment (DPIA). DPIAs evaluate the data protection risks involved for children using the provided service to mitigate risks early on (2. *Data Protection Impact Assessments*, n.d.). Additionally, online service providers are to activate 'high privacy' settings as the default for their sites. This involves selecting 'off' for default profiling and geolocation settings. Companies should not encourage children to use their sites to alter these settings to gain additional personal data or work around their data privacy protection. Any settings, parental controls, or online tools provided by the online service must be transparently stated. This code is not exclusive to children's content either. Due to the risk of a child accessing an app on an adult's phone without proper observation, the Children's Code applies to all online service providers (*Introduction to the Children's Code*, n.d.).

II. US Data Protection Laws

The United States adheres to a different regulation setup than the UK does. While the UK builds off the DPA 2018 for data protection within three different segments-- companies, intelligence agencies, and their government-- the United States focuses on protection from the government. The Privacy Act of 1974 is the central privacy policy the federal government follows, which is quite limited. The only regulation it provides describes how the federal government handles data from US citizens, not the way companies are to treat US consumer data. It is left to the states to implement data protection policies further.

While the US does have data protection laws in place for companies and institutions to follow, they are nowhere near as extensive as the UK's. The Federal Trade Commission Act of 1914 (FTC) is a federal statute that prevents businesses from exploiting their consumers via deception and misrepresentation. Other regulations imposed through the FTC Act, such as Gramm-Leach-Bliley, the Fair Credit Reporting Act (FCRA), the Health Insurance Portability and Accountability Act (HIPAA), and the Family Educational Rights and Privacy Act (FERPA), all cover significantly narrowed and limited areas of data protection. The sole exception in this field of legislation is the Children's Online Privacy Protection Act (COPPA) (Ritchie, J.N. & A., Jayanti, S.F.-T et al., 2022).

Acting similarly to the UK's Children's Code, COPPA builds off the FTCA and imposes regulation against unfair and deceptive practices with data collected from child users. This act defines child users as children aged thirteen years and under. COPPA applies broadly to operators of commercial websites and online services, including mobile apps that collect and maintain personal information. The FTC establishes a broad application of this Act, applying to "any service available over the internet, or that connects to the internet or a wide-area network" (Ritchie, J.N. & A., Jayanti, S.F.-T et al., 2022). The goal of COPPA is to place data collection controls back into the hands of parents and guardians. Companies must be fully transparent with their data processing policies. Online service providers must provide full disclosure on their website to parents on what data is collected and the operator's use of their data. Companies must obtain parental consent for data collection. All data collection information should be easily accessible by parents and children in the operator's privacy policy (Ritchie, J.N. & A., Jayanti, S.F.-T et al., 2022).

In 2018, California passed the California Consumer Privacy Act of 2018 (CCPA) along with the CCPA regulations to act as leading guidelines. The CCPA grants California consumers the right to know what information is being collected about them, the right to delete cached information, to opt out of the sale or distribution of personal information, and the right to non-discrimination for exercising these rights. Most recently, a 2020 amendment known as Proposition 24, the CPRA, introduced additional consumer rights to correct inaccurate information and limit the use of their personal information. Both are still under processing (*California Consumer Privacy Act (CCPA)*, 2023).

These privacy rights require businesses to be incredibly transparent, giving required notices to the consumer. California consumers are provided with a "notice at collection" at or before the time data collection occurs. A notice at collection lists the personal information the business has gathered from its consumers and the intended purpose for that data. If the business is in the market to sell its consumer data, consumers are given a "Do Not Sell or Share" link. By selecting this link, consumers can "opt out" of the business selling and sharing their data. The same goes for children. Businesses are not allowed to sell the personal information of a child unless given explicit permission by "Opt-In" settings being selected (*California Consumer Privacy Act (CCPA)*, 2023).

California sets a new standard for states in keeping companies focused on the consumer's best interests at heart. Not only does the policy give a clear explanation of how, what, and why data is being collected, but it also gives consumers a chance to opt out. Like the GDPR, California residents can know that this policy applies to them regardless of where they are (*California Consumer Privacy Act (CCPA)*, 2023). The CCPA is one of the first attempts within the US to combat the gains a company receives from using consumer data. Several states followed suit as a result.

Part II. TikTok's Policies Regarding Data Collection

TikTok provides separate privacy policies for UK users and US users. While similar in content, the privacy policy for UK users has many more specifics than the US policy to meet UK GDPR guidelines. For example, the UK privacy policy dedicates a section to discussing the importance of classifying "legitimate interests" for UK TikTok user data. This follows the ICO's requirement for online privacy policies to state their legitimate interests in processing users' data, being specific about the purpose and intended outcome of said processing. Because this is not a requirement under US data protection regulation, TikTok's Privacy Policy for their US users is much vaguer with its language.

Similar to the differences between the US and UK user policies, TikTok provides a separate privacy policy for its child users. TikTok states that the company "is committed to protecting children's privacy" (*About: TikTok - real short videos,* n.d.). The social media platform claims it collects minimal information from children when they register for an account, including their username, password, and birthday. However, in the following sentence of the privacy policy, TikTok states that information from the child's device, such as IP address, web browser version, country-level location, video watches, time in the app, and general usage information, may be obtained (*About: TikTok - real short videos,* n.d.).

This is a significant wound in TikTok's legal skin that may fester over time. In addition to the unclear and somewhat manipulative wording, the children's privacy policy is also incredibly vague in describing how data from child users will be used, shared, and retained. For example, TikTok clearly states that data will not be sold or shared with third parties but will share child user data with their corporate group and undefined "service providers" (*About: TikTok - real short videos,* n.d.).

In both the "Data Security" and "Retention and the Sharing Data" sections of the privacy policy, TikTok continues to use unspecific phrasing to define their purpose for data collection, such as: "provide and support our services," "as necessary for service providers/corporate group to support internal operations," "to fulfill the purpose for which the information was collected" (*About: TikTok - real short*

videos, n.d.). Vague wording and a lack of transparency is a red flag for regulation enforcers like the ICO and goes against policies outlined in both the Children's Code and COPPA.

Part III. TikTok's Violations of Data Policies

I. Violations of COPPA in the US

TikTok has had multiple lawsuits related to child data collection over the past ten years. In 2019 the app Musical.ly, now known as TikTok, was under fire for violating COPPA under multiple counts. From 2014 to 2016, Muscial.ly failed to provide appropriate parental consent and controls (Ritchie, J.N. & A., Jayanti, S.F.-T et al., 2022). The proposed order of civil penalties for *United States of America v. Musical.ly* states, "The Complaint charges that Defendants violated the COPPA Rule and the FTC Act by failing to post a privacy policy on its online service providing clear, understandable, and complete notice of its information practices; failing to provide direct notice of its information practices to parents; failing to obtain verifiable parental consent before collecting, using, and disclosing personal information from children; failing to delete personal information at the request of parents; and retaining personal information longer than reasonably necessary to fulfill the purpose for which the information was collected." Musical.ly paid $5.7 million to settle FTC allegations and was ordered to delete all the stored personal information of these users unless otherwise directed by a parent or guardian (Ritchie, J.N. & A., Jayanti, S.F.-T, et al., 2022).

Musical.ly operators were aware of the number of children using the app, displaying a blatant disregard for COPPA. The FTC did not plan to let Musical.ly off the hook with only a fine, either. After acknowledging the order, Musical.ly was required to submit a compliance report a year later. The report holds similar criteria to DPIAs and Safe Harbor program applications, including, but not limited to, detailed descriptions of the activities of the business, showing the company is upholding the compliance of the order, copies of each new privacy policy notice posted on their website or service, copies of transparent statements describing data collection for obtaining parental consent and each type of data collected from children and the need for said data (Ritchie, J.N. & A., Jayanti, S.F.-T et al., 2022).

II. Violations of the UK GDPR and the Children's Code in the UK

In May of 2023, TikTok was issued a £12.7 million fine by the ICO for violating the UK GDPR from May 2018 to July 2020. The violations that were addressed involved TikTok's failure to obtain parental consent for children's data, failure to ensure lawful and transparent data processing, and failure to "do enough" to verify the ages of their users. It was approximated in 2020 that over 1 million children under thirteen were using TikTok's platform, even with TikTok's age restrictions in place. Regarding TikTok's privacy policy, the social media platform failed to describe what user data was collected, used, and shared for in an easy-to-understand manner (*Ico fines TikTok £12.7 million for misusing children's Data*).

John Edwards, the ICO commissioner, shared his view on the severity of the situation, "As a consequence, an estimated one million children under the age of thirteen were inappropriately granted access to the platform, with TikTok collecting and using their data. That means that their data may have been used to track them and profile them, potentially delivering harmful, inappropriate content at their very next scroll" (*Ico fines TikTok £12.7 million for misusing children's Data*).

Outside of children's data protection regulations, TikTok has been served with multiple fines and class action lawsuits for violating consumer data protection laws. Ongoing instances involve the EU, the state of California, the state of Indiana, the state of Montana, and more (Singer, 2022). In addition to these lawsuits, TikTok's choice of data processing and vague terms has led multiple countries to outright ban the app on government-issued devices.

Part IV. Recommendations for Compliance and Best Practices

I. Ensuring Compliance with the UK GDPR and Children's Code

The Children's Code, while being an additional regulation, should be seen as a tool for companies to use rather than a hindrance. By strictly following the code and framing a company's software around its regulations, compliance with the GDPR is also improved, as many principles overlap.

For companies seeking to comply with the UK GDPR and the Children's Code, child safety and data protection should be at the forefront of product design. This may seem like an overwhelming task, but the Information Commissioner's Office assists companies to succeed by providing clear direction and multiple failsafe tools for companies to use. Section 123 of the Data Protection Act of 2018 requires the ICO to produce a code for companies and online service providers to abide by, as well as provide Data Protection Impact Assessments (*About this code*, *n.d.)*. Data Protection Impact Assessments (DPIAs) identify areas of high data risk within a project and assist in minimizing the risk (*2. Data Protection Impact Assessments*, n.d.).

Data processing is categorized as high risk if a data breach could endanger the health or safety of an individual. Data Processing Impact Assessments are legally required for all UK companies whose services are categorized as high-risk regarding data. In addition to high-risk data processing, the ICO requires DPIAs if a company or online service provider intends to use innovative technology, process biometric data, use profiling or special category data, process genetic data, match or combine data from other sources, collect data from a third-party source, or when targeting online services directly to children (*2. Data Protection Impact Assessments*, n.d.). Companies that do not fall under the high-risk category do not have to send their DPIAs to the ICO for review. To build up trust with parents and guardians of young consumers, the ICO recommends companies publish their DPIAs on their home web pages to show their prioritization of compliance with data collection regulations (*FAQs on the 15 standards of the children's code*, n.d.).

II. The US COPPA Safe Harbor Program

Like DPIAs, online service providers in the United States can use the COPPA Safe Harbor Program. This program allows companies and organizations to submit self-proposed regulatory guidelines that appeal to COPPA's standards to gain FTC approval. Companies that offer applications and are approved can work forward on developing their software quickly, knowing that the most critical standards have been met. Applications for this program must contain the online service provider's business model, a rundown of the tools used to collect and maintain consumer data, and an outline that aligns the proposed guidelines with corresponding COPPA rules (Ritchie, J.N. & A., Jayanti, S.F.-T, et al., 2023).

Once submitted, the protections provided by the self-proposed guidelines will be assessed and compared to the rules set forth by COPPA. The FTC approves applications that offer the same, or better, amount of protection for a consumer's data than COPPA does. The proposed guidelines must contain appropriate disciplines to be enacted for online service operators who are not compliant. This program provides companies with an opportunity to start an online service with a solid legal footing. The FTC further encourages companies to maintain the best interests of a child user at the heart of their design by allowing companies that pursue approval to be given safe harbor treatment for 180 days. A company within this Safe Harbor window has a reduced amount of liability regarding data collection policies. As the issues within a proposed policy are worked out, Safe Harbor acts as a buffer against penalties and fines from the FTC (Ritchie, J.N. & A., Jayanti, S.F.-T, et al., 2023).

If an online service provider is found to violate COPPA, all use of children's data must be stopped. Operators should review all aspects of data collection, storage, and use. Begin by analyzing privacy policies, methods of data collection, transparent communication with child and parent users, as well as

data security. Seek consulting with an FTC-approved COPPA Safe Harbor Program organization such as the Children's Advertising Review Unit (CARU), the Entertainment Software Rating Board (ESRB), iKeepSafe, kidSAFE, Privacy Vaults Online, Inc., and TRUSTe. Penalties for violating COPPA may involve fines up to $50,120 per violation and are calculated based on the severity and frequency of the violations (Ritchie, J.N. & A., Jayanti, S.F.-T, et al., 2023).

Part V. Discussion

I. The Need for Strengthened Data Protection in the US

When the US FTC Act and COPPA were established, the internet was not as prominent as it is today. The legislation, on its own, is not equipped to handle the protection of consumer's data to the extent in which the internet exists today. However, the UK has kept current, implementing policies as the internet has expanded and continued. Data protection is not merely a static concern but an ever-evolving challenge that must adapt to the rapid advancements in digital technology. The ongoing evolution calls for a deeper analysis of the implications and potential trajectories of data protection laws, especially about safeguarding our most vulnerable citizens - children.

The patchwork of state-dependent data protection policies in the United States presents a fragmented landscape. To combat this, the US should adopt a unified and comprehensive policy approach at the state or federal level, similar to the UK's GDPR. As it stands, the US system, with its reliance on individual state policies, faces significant challenges in providing a coherent data protection strategy. In contrast, the UK's proactive stance not only strengthens protection for children's data but coordinates with the broader mandates of the GDPR, enhancing overall data governance.

Emulating the UK's data privacy model offers multiple benefits to the US. It would streamline state regulations, leaving a singular reference point for companies and consumers. This uniformity is especially pertinent given the cross-state nature of digital services. Current individual state legislation, such as California's Consumer Privacy Act (CCPA), though commendable, does not fully address the trans-state challenges of digital data flows. A federal standard, informed by the same components that make up UK regulation, would not only safeguard the rights of American citizens but also elevate the US's standing in global data protection.

II. Insights into Research Limitations

This paper acknowledges certain limitations reflective of the developing and evolving state of data protection legislation. The assessments of the UK's GDPR and Children's Code alongside the US's COPPA framework are bounded by the assumption that the principles and practices established in these legislations can be universally applied. However, cultural, social, and political differences between regions will necessitate distinct approaches to data protection. The UK model, while robust, may not be able to transfer to the US context without proper modifications. These assumptions are based solely on the interpretation of legislation aimed at safeguarding children's privacy. They do not take the broader societal or economic implications of these regulations into account. In light of these limitations, ongoing research and dialogue are necessary to evolve data privacy policies as technology advances and societal values change.

III. Conclusion

The UK GDPR and Children's Code have set a standard that emphasizes the importance of child safety and data protection from the start of a product's design. Compliance with these regulations is not only a legal obligation but a fundamental aspect of ethical practice, which plays a crucial role in building user trust and establishing a foundation for the sustainable growth of digital services.

This paper advocates for a call to action for proactive engagement with data privacy legislation, particularly in the United States. While the US COPPA Safe Harbor Program provides a framework for companies to adhere to, there is a clear need for strengthened and unified data protection laws that reflect the digital landscape and anticipate future technological advancements. California has played a leading role in the US, signaling a path forward, suggesting that both state and federal levels could benefit from adopting the principles embodied in the UK's approach.

It is not enough to respond to privacy concerns as they arise; there must be a forward-thinking, proactive stance that anticipates the challenges and prepares for the complexities of a digital future. Policymakers, industry leaders, and stakeholders must consider the long-term implications of data privacy and work collaboratively toward comprehensive legislation that safeguards the rights and well-being of children online. By doing so, the digital world will not only be a space for innovation and growth but also a secure environment that fosters the potential of every user.

References

Data Protection Impact Assessments (no date) *ICO*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/2-data-protection-impact-assessments/ (Accessed: 04 October 2023).

About this code (no date) *ICO*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/about-this-code/ (Accessed: 04 October 2023).

About: Tiktok - real short videos (no date) *TikTok*. Available at: https://www.tiktok.com/about?lang=en (Accessed: 30 September 2023).

California Consumer Privacy Act (CCPA) (2023) *State of California - Department of Justice - Office of the Attorney General*. Available at: https://www.oag.ca.gov/privacy/ccpa#sectionb (Accessed: 04 October 2023).

Evans, M. (2018) *Why data is the most important currency in commerce today*, *Forbes*. Available at: https://www.forbes.com/sites/michelleevans1/2018/03/12/why-data-is-the-most-important-currency-used-in-commerce-today/ (Accessed: 30 September 2023).

FAQs on the 15 standards of the children's code (no date) *ICO*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/faqs-on-the-15-standards-of-the-children-s-code/ (Accessed: 04 October 2023).

Fowler, G. (2023) *Your kids' apps are spying on them*, *The Washington Post*. Available at: https://www.washingtonpost.com/technology/2022/06/09/apps-kids-privacy/ (Accessed: 04 October 2023).

Froehlich, N. (2023) *Council post: The truth in user privacy and targeted ads*, *Forbes*. Available at: https://www.forbes.com/sites/forbestechcouncil/2022/02/24/the-truth-in-user-privacy-and-targeted-ads/?sh=51b0c4a+d355e (Accessed: 30 September 2023).

Harwell, D. (2022) *Remote learning apps shared children's data at a 'dizzying scale,' The Washington Post*. Available at: https://www.washingtonpost.com/technology/2022/05/24/remote-school-app-tracking-privacy/ (Accessed: 30 September 2023).

Ico fines TikTok £12.7 million for misusing children's Data (2023) *ICO*. Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/ (Accessed: 04 October 2023).

Introduction to the children's code (no date) *ICO*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/ (Accessed: 04 October 2023).

Leiby, M. (2022) *'iPad kids' and the future of early childhood development*, *Spartan Shield*. Available at: https://spartanshield.org/31970/opinion/ipad-kids-and-the-future-of-early-childhood-development/ (Accessed: 30 September 2023).

Online tools for teaching & learning (no date) *Online Tools for Teaching Learning*. Available at: https://blogs.umass.edu/onlinetools/community-centered-tools/schoology/ (Accessed: 30 September 2023).

Ritchie, J.N.& A. and Jayanti, S.F.-T., and A. (2022) *Video social networking app Musical.ly agree to settle FTC allegations violating children's privacy law*, *Federal Trade Commission*. Available at: https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy (Accessed: 04 October 2023).

Ritchie, J.N.& A. and Staff in the Bureau of Competition & Office of Technology (2023) *Complying with COPPA: Frequently asked questions*, *Federal Trade Commission*. Available at: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (Accessed: 30 September 2023).

Rouse, M. (2017) *Ad targeting*, *TECHOPEDIA*. Available at: https://www.techopedia.com/definition/30295/ad-targeting (Accessed: 30 September 2023).

Searing, L. (2021) *One-third of children ages 7 to 9 use social media apps, study says*, *The Washington Post*. Available at: https://www.washingtonpost.com/health/social-media-young-kids/2021/11/19/3130ce5a-488a-11ec-95dc-5f2a96e00fa3_story.html (Accessed: 30 September 2023).

Singer, N. (2022) *Tiktok may face $29 million fine for failing to protect children's privacy*, *The New York Times*. Available at: https://www.nytimes.com/2022/09/26/technology/tiktok-children-privacy-fine-uk.html#:~:text=Natasha%20Singer %2C%20a%20technology%20reporter, children's%20online%20privacy%20since%202012. &text=TikTok%2C%20t he%20popular%20video%2Dsharing, privacy%20in%20the%20United%20Kingdom. (Accessed: 30 September 2023).

Vittorio, A. and Witley, S. (2022) *Tiktok Faces 'pile-on' pressure from states after Indiana sues*, *Bloomberg Law*. Available at: https://news.bloomberglaw.com/privacy-and-data-security/tiktok-faces-pile-on-pressure-from-states-after-indiana-sues (Accessed: 30 September 2023).

Zhong, R. and Frenkel, S. (2020) *A third of TikTok's U.S. users may be 14 or under, raising safety questions*, *The New York Times*. Available at: https://www.nytimes.com/2020/08/14/technology/tiktok-underage-users-ftc.html (Accessed: 03 October 2023).